The London School of Economics and Political Science

Interpreting a Major Event Organization's Efforts to Reliably Manage Information Security Risks: the Case of the Athens 2004 Olympics

Despena Elizabeth Afxentiadis

A thesis submitted to the Department of Management
(Information Systems and Innovation Group)

of the London School of Economics and Political Science
for the degree of Doctor of Philosophy

London, January 2010

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

Declaration

I certify that the thesis I have presented for examination for the MPhil/PhD degree of the London School of Economics and Political Science is solely my own work other than where I have clearly indicated that it is the work of others (in which case the extent of any work carried out jointly by me and any other person is clearly identified in it).

Disclaimer

I certify that any opinion expressed in the presented thesis is to be considered the researcher's interpretation of events and findings, not the opinion of the organizations involved in the Athens 2004 Summer Olympics event.

Abstract

The implementation of mega projects and events is increasingly becoming part of corporate and governmental reality in an effort to create global and frictionless operations and infrastructures that result into a new mobility that has been labelled as 'the most powerful and coveted stratifying factor in contemporary society'. The successful implementation of such mega projects and events usually relies on the *highly reliable* operations of technological infrastructures and the *secure*, yet flexible, management of information resources across a number of partnering organizations. However, the past performance of mega projects and events has been greatly criticised for inefficiency, lack of decision-making transparency and an overall lack of diligence with regards to the true nature and extent of associated risks. A need has been identified to investigate more thoroughly the mechanisms employed to manage and communicate risks across a number of vertical and horizontal project and event management dimensions. The objective would be to capture know-how and lessons learned from past experiences in order to support more successful, future mega-project implementations.

The aim of this research is to increase understanding of the risk issues and concerns in the management of information systems security (ISS) in a major events context, in an effort to deliver highly reliable IS operations. The study is conducted by reviewing the analysis, design, management and risk communication processes of ISS in the Athens 2004 Olympic Games event. The research methodology adopts an *interpretive* mode of inquiry, where the management of ISS is longitudinally evaluated in terms of the organizational scope, context and culture, the expectations and motivations of different actors, the meanings assigned to various ISS risk signals and events, and the related patterns of behaviour and organizational actions and controls. The theoretical foundation that informs the collection and analysis of data is that of the Social Amplification of Risk Framework (SARF), which suggests that the experience of risk is determined by the direct physical consequences of a risk/risk event and the interaction of psychological, social, institutional and cultural processes.

Findings from the case study under investigation indicate that a major event demonstrates high levels of operational and functional interdependence and complexity, directly or indirectly affecting ISS management efforts, decisions and communications. Principles of high reliability and mindful management can indeed improve overall ISS performance and management of risk, yet the structural and cultural aspects of a major event project will amplify/attenuate risk perceptions and constrain the effectiveness of such controls. Therefore, there is a need to improve understanding of such factors, incorporating this into risk evaluation, management and communication practices.

In conclusion, this study shows that the management of IS security and integrity in an environment of great organizational reliability demands requires the appreciation of structural/functional interdependencies and cultural interactions. By sustaining mindful and reflexive processes and structures of risk communication and interpretation, ISS assurance and governance practices will allow organizations to demonstrate that they can reliably anticipate and contain ISS risks.

Acknowledgments

Along this journey several people have supported me, giving me the key to open new doors, lighting the way to new directions, or standing by me.

I would like to take this opportunity to thank them all for making this possible. It's been an adventure.

Thank you, to...

Dr James Backhouse (LSE) for enthusiastically encouraging me to commence and complete this journey.

Dr Shirin Madon (LSE) for always being approachable, providing me with advice and words of warm encouragement.

Mr Philippe Verveer (IOC) and Mr Spyros Kapralos (ATHOC) for giving me the opportunity to enter the world of Olympic dream-weaving.

Dayle. You have been the most unexpected gift. You showed me the way, you raised the bar, and you trusted me. I will always be grateful.

My dear friends Maro and Luna for their endless support and love. You were always there for me throughout this journey - I cannot thank you enough. Your love has made me believe in myself.

My special Geo, for keeping me sane and making me smile. You are my sunshine.

My dear, patient Theo, for supporting *my* choices, for loving me, for holding me. Throughout this journey I've needed you more than anything or anyone else. Our future is here. Now. I can't wait!

Finally, I'd like to dedicate this to...

... my mother, for never doubting my choices and decisions.

... my father, for believing in and creating a better future.

You are both my core. Your personal choices and actions have shown me that any achievement of magnitude requires one to push boundaries, to evolve, to dream, to plan, and to work hard. For that, and your love, I will always be thankful.

List of Abbreviations

A	a risk 'anticipation' strategy and control that aims to prevent errors from happening, and prepare for errors prior to their realization
A2004	Athens 2004 Summer Olympic Games
AAR	After Action Review
ACL(s)	Access Control List(s)
Admin-IS	the IS supporting the A2004 Games administrative and preparation activities by ATHOC and its partners
AOB	the Athens 2004 Olympic Broadcasting organization (i.e. the host broadcaster of the Athens 2004 Olympic Games)
ATHOC	Athens 2004 Olympic Committee
BIOS	Basic Input/Output System (the BIOS sets the machine hardware into a known state so that software can be loaded, executed, and given control of the PC)
C	a risk 'containment' strategy and control that focuses on limiting the impact of an error and recovering operations after the error has materialised
C.I.A.	the core principles of ISS, namely Confidentiality, Integrity and Availability
EMBOK	Event Management Body of Knowledge: a three dimensional description of the knowledge and skills essential to create, develop and deliver an event project
Games-IS	The A2004 IS solution aimed to capture and report every moment of the event's action, communicating this to the world via a number of media
Games-ISS	the Athens 2004 Summer Olympics ISS project and infrastructure that supported the secure operation of the Games-time IS
GMS	Games Management System
HERO	Hierarchical Epistemology and Realist Ontology
HRO	Highly Reliable Organization
IBC	the International Broadcasting Centre
IDS	Information Diffusion System
IF	the International Sport Federations

IOC	International Olympic Committee
IRGC	International Risk Governance Council
IS	Information System(s)
ISS	Information Systems Security
IS(S)	IS and ISS
K-Lock	Kensington lock
KOEP	a A2004 consortium of five Greek IT companies, providing ATHOC with IT hardware, software and skilled personnel
Masterplan	the project management framework provided by the IOC to ATHOC in order for the latter to manage and monitor the deliverables of the TOP sponsors
METER	the contractual agreement between the IOC and SchlumbergerSema that specified the IT services to be sponsored by the TOP IT sponsor along with the Olympic promotional opportunities and privileges that it would benefit from
NOC	the National Olympic Committees
NSF	the National Sport Federations
OBS	the Olympic Broadcasting Services SA (i.e. OBS supplies all services relating to the establishment and management of the Host Broadcasting function of the Games)
OC	'Organizational Culture' controls of high reliability
OCOG	the temporary Organizing Committees for the Olympic Games
OD	'Organizational Design' controls of high reliability
OGKS	the Olympic Games Knowledge Services SA (i.e. the OGKS supports the IOC in the transfer of knowledge and expertise from one OCOG to another)
OM	'Operations Management' controls of high reliability
OTE	the Hellenic Telecommunications Organization
OVR	On-Venue-Results system (part of the Games-IS Results system)
PMBOK	Project Management Body of Knowledge: a PMI process-based project management guide and an internationally recognized standard that provides fundamentals of project management as they apply to a wide range of projects

PRINCE-2	An OGC project management method, covering the management, control and organization of a project. It has become a de facto standard for project management in the UK, while it has also spread outside the country.
SARF	the Social Amplification of Risk Framework
SIM	a Security Information Management solution which aggregates and cross-correlates data to identify ISS trends and attacks
SL2002	Salt Lake 2002 Winter Olympic Games
SLA	Service Level Agreement
T&S	Timing and Scoring system (part of the Games-IS Results system)
TEs	Test Events
TE-1	the first round of Test Events (in August 2003)
TE-2	the second round of Test Events (October 2003 to January 2004)
TE-3	the third round of Test Events (February to May 2004)
TE-4	the fourth round of Test Events (in June 2004)
Third Parties	A2004 Olympic broadcasters
TOC	the Technology Operations Centre
TOC-SEC	the 'Event-time' ISS expert team operating from the Technology Operations Centre (TOC)
TOC-NET	the 'Event-time' Games-network expert team operating from the Technology Operations Centre (TOC)
TOP	The Olympic Partners
TRs	Technical Rehearsals
TR-1	the first round of Technical Rehearsals (in April 2004)
TR-2	the second round of Technical Rehearsals (in June 2004)
TSA(s)	Technology Secure Areas: restricted/controlled-access areas across the Olympic venues and headquarters where Games-IS devices were located
Venue(s)	A2004 Olympic Games competition venues
VITM	Venue IT Manager
VLAN	Virtual Local Area Network

Contents

List of Figures

List of Tables

1. Introduction

1.1 Research background and orientation

The need of contemporary organizations to handle their information assets reliably has been long acknowledged, as well as the significance of information systems security (ISS) practices in ensuring inter- and intra-organizational communications integrity.

In more recent years, however, as corporations and governmental organizations expand their global and socio-economic reach and interconnectivity, a number of high-visibility ISS incidents have been witnessed. These have taken place across organizations and governments of varying IS infrastructure maturity, size, function and performance, leading to a global attention towards means to regulate and standardize information handling practices.

As a result, corporations and governments have not only introduced the issue of ISS into their strategic agendas, but have also allocated increasing resources to its management[1], while identifying a need for organizational structures of ISS accountability.

Yet, ISS spending can be costly, while the realized benefits are often elusively defined and accounted for. As such, there has been an increased appreciation and utilization of risk management practices with respect to ISS, as this is "a process that helps organizations in balancing operational necessities and economic costs associated with IT-based systems", while justifying risk management decisions both internally and externally. "The overall mission of risk management is to enable an organization to handle information adequately" (Dhillon, 2007:157), and this implies a number of issues.

Firstly, the notion of an 'adequate' level of risk handling suggests that there is an '*acceptable*' level of ISS risk that will be defined according to an organization's mission and priorities. Therefore, risk mitigation solutions must be customized according to each organization's needs. In addition, the above definition of 'ISS risk management' suggests that this is a *process* of assessment, evaluation, and prioritization, which aims to determine the nature and extent of uncertainty, and thus identify means to control it. In addition, in times when regulatory legitimacy of

[1] I.e. Yoran (2009) and Moscaritolo (2009).

ISS operations requires decision-making transparency and consistency, risk management processes also imply the need for structures of accountability.

Therefore, despite the apparently deterministic nature of risk management practices, these involve an inherently subjective and interpretive process, which will be also determined by the context within which it is applied.

Meanwhile, extensive literature[2] indicates that with an increased organizational reliance on IS infrastructures, certain organizational structures will be more prone to errors, accidents and disasters than others. In fact, research indicates that such organizations often have to operate under a very low, if not zero, tolerance for failure[3]. Thus, increasing numbers of organizations have to demonstrate such highly reliable operations.

As such, after an extensive review of related literature[4], the researcher has identified a crucial need to investigate organizations and their IS infrastructures that are required to deliver 'highly reliable' and secure IS operations, while operating under conditions of considerable uncertainty, budgetary and time constraints. Therefore, the initial drive of this study is to increase understanding with regards to issues of ISS risk management in organizational environments that are prone to accident, yet have a low risk tolerance level.

1.2 The research problem and focus

'Highly reliable organizations' (HROs) are defined by a number of organizational theorists[5] as those organizations that succeed in avoiding major errors and disasters, despite the fact that they operate under conditions where 'normal accidents'[6] can be expected. What drives such exemplary performance is the fact that HROs cannot afford to fail, since the impact of an operational failure would have disastrous

[2] E.g. Perrow, 1984, 1992; Vaughan, 1996, 1999.

[3] I.e. Weick and Sutcliffe, 2007.

[4] The literature reviewed for the purposes of this study is further presented in Chapter 2.

[5] E.g. Roberts, 1989, 1990a, 1990b; Weick, 1987.

[6] A 'normal accident' is an unanticipated interaction of multiple failures in a complex system. This complexity can either be technological or organizational, and often has elements of both (i.e. Perrow, 1984).

outcomes for the legitimacy and survival of the organization, as well as detrimental impacts for a wide number of stakeholders and the public.

Weick and Sutcliffe (2007), in fact, suggest that as corporations and governments become highly interconnected global entities, there is an increasing need for organizations of all kinds to operate under conditions of 'high reliability', namely under a low, if not zero, tolerance for failure. The cost could otherwise be too great.

Extending this argument in the field of ISS management, the same could be applied here. As organizations reach out to even wider, diverse and interconnected markets, they are required to demonstrate that they are *reliable* guardians of corporate and private information.

Therefore, from a 'rational'[7] viewpoint organizational endeavours that involve too great an uncertainty and too great a negative impact in case of failure should not be pursued. Yet, research and practice demonstrate that this is often not the case.

The researcher suggests that the reasons for this phenomenon partly lie with what sociologist Zygmunt Bauman (1998) has labelled as 'the Great War of Independence from Space', and IT and business 'guru' Bill Gates has called 'frictionless capitalism' (Taylor, 1998). The phenomenon refers to the emergence of mega (IS) infrastructure projects that result in a new socioeconomic mobility, and determine the new 'politics of distance' (Bauman, 1998).

As is later demonstrated in Chapter 2 of this study, mega projects and events[8] are increasing in number and significance, since they are "central to the new politics of distance because infrastructure is increasingly being built as megaprojects" (Flyvbjerg et al., 2003:3). Meanwhile their success is so important to their sponsors that firms and even governments can collapse when they fail (Merrow, 1988). Yet, mega projects and events are inherently risky in nature and usually demonstrate poor performance, leading to the identification of the 'megaproject performance paradox' (Flyvbjerg et al., 2003).

---

[7] The term 'rational' in the context of decision making and risk management refers to a utility-focused viewpoint, where decisions are made based on cost versus benefit, or risk versus benefit considerations.

[8] Mega infrastructure projects are defined as projects that are great in scale and impact, which primarily aim for increased *connectivity*, whether that is via physical construction, technological or other means (i.e. Flyvbjerg et al., 2003). Mega *events & meetings*, which aim to increase connectivity, human interaction and exchange of ideas, are also considered to be an increasingly significant subcategory of mega-projects (i.e. Silvers, 2008).

As more researchers and practitioners point to the above problem, they have also identified a need to consider consistently factors that challenge the successful performance and delivery of mega project and event organizations. Researchers[9] have pointed towards the urgent need to identify the methodologies, approaches and processes that will ensure highly reliable operations of megaproject organizations. Yet, it seems that initiatives that will explore and investigate the scoping, delivery and economic and socio-political impact of such ambitious and risky endeavours "are still in their very early days" (Silvers, 2008: xviii, 11). Any efforts to understand and standardize the practices of mega projects/events require both localized and sector-specific pools of expertise as well as integrated, government and industry-wide, coordination and commitment.

In response to such an identified need, a number of efforts have been made to map, categorize and standardize the phases and functional areas of projects and events. These have led to project management frameworks, methodologies and best practices such as PMBOK, PRINCE-2 and EMBOK[10].

Throughout all of these approaches, the secure yet flexible management of project and event information is considered a key administrative functional area. From the information generated and utilised during the preparation phase of an event/project, to the information generated and distributed during the operational end-phase of the project, information remains one of the most critical project assets. It represents the business's intelligence, memory, evidentiary and historical records (Silvers, 2008). Project information is an asset that needs to be securely managed, speedily and accurately communicated, regularly monitored and updated, and reliably maintained.

However, despite, such identified criticality of ISS management practices within a mega project/event context, no research seems to have been conducted in this area. Given that mega projects and events have only recently received researchers' attention, the risk management practices required in order to deliver reliable and secure IS operations have not been considered in depth.

[9] I.e. Flyvbjerg et al. (2003) and Silvers (2008).

[10] I.e. list of abbreviations above.

Hence, the aim of this research becomes more focused. Its objective is to *understand*[11] ISS risk management practices in a major project/event context, where stakes and risks are both very high. As argued above, the researcher agrees with the view that risk management is an interpretive process whose outcomes will be determined by both the physical impact of the risk as well as the processes involved in the organizational encounter with that very risk[12]. Therefore, in order to understand the ISS risk management practices of a major project/event organization, the researcher reviews the processes of ISS risk analysis, design, management and communication in the Athens 2004 (A2004) Olympic Games, and explores the underlying causes and the related patterns of behaviour. Eventually, the researcher aims to understand how ISS management practices, risk perceptions and behaviours evolve and affect a mega event's capacity to deliver highly reliable IS operations.

Given that organizational encounters with risk involve a dynamic, ongoing process of risk attention, sense-making and re-organization[13], where risk perceptions and actions evolve and *change over time*, the researcher has opted for an interpretive, longitudinal case-study approach. Early involvement in the case-study environment and the utilization of a number of research methods have supported a layered data collection and analysis method, favouring the need for a rich, in-depth understanding of the organizational context, ISS actions, behaviours and outcomes.

1.3 Organization of the study

In order to capture and present the rationale and methods of this research, as well as the associated findings and insights with regards to the ISS management practices and behaviours in a mega event organization that needs to deliver highly reliable IS operations, the researcher has organized her study in the following sections:

[11] 'As explained in section 3.2.2 of this study, the notion of '*understanding*' refers to Weber's (1962, 1968) 'Verstehen', where research focuses on the meaning and values of acting persons in order to arrive at a causal explanation of the course and effects of social action.

[12] The concept of 'organizational encounters with risk' is introduced by Hutter and Power (2005b). It refers to an ongoing process of organizational risk attention, sense-making and re-organization. This concept is explored further in Chapter 5.

[13] I.e. Hutter and Power, 2005b.

After the research orientation, focus and problem is identified in Chapter 1, the literature reviewed for the purposes of this study is considered in Chapter 2. As stated in the above paragraphs, the research orientation was the reason to investigate existing literature across a number of disciplines, ranging from organizational theories to risk/hazard management theories, ISS management and project/event management approaches. The reviewed literature is, thus, summarized and grouped in research themes and research gaps, directions and foundations to this study's research problem are identified.

The implicit argument is that while ISS scholars have increasingly considered the behavioural and social aspects of risk management practices, there is still considerable space for inter-disciplinary investigations that will promote the utilization of integrative theoretical and methodological frameworks. Such frameworks should stress the multiple dimensions to an organizational encounter with ISS risk, the significance of context and communication, and the ongoing, learning process involved in the delivery of highly reliable ISS operations.

Chapter 3 of this thesis sketches out the methodology of this research. It identifies the ontological and epistemological assumptions of this study, and points to the associated implications with regards to the applied theoretical perspective. The conceptual framework that guides the empirical analysis, namely the Social Amplification of Risk Framework (SARF), is presented here. In addition, a contextual mode of inquiry is proposed, stressing the need for an investigation into the contextual issues of organizational actions, meaning structures, and the way these change over time. Finally, the research design is presented in Chapter 3.

The empirical work of this research is covered in Chapter 4. The structural context of the organization and event project under study is presented here. The main focus of the research findings is on the interpretation of the ISS management implications related to the delivery of a highly reliable IS within a particular context. The empirical findings are analysed in a chronologically linear fashion, representing the various case-study project phases. The conceptual framework utilised for the data analysis is the SARF. Emergent issues are also presented here.

The key issues and study insights are presented in Chapter 5. This is done in light of the theoretical and philosophical assumptions set out in Chapters 2 and 3. Discussion revolves around the three key themes that 'organizational encounters with risk' define, namely those of risk attention, sense-making and re-organization. The key issues and lessons learned presented are always closely correlated with the

organizational context - that of a major event - and the organizational mission - that of highly reliable IS(S) operations.

Finally Chapter 6 concludes the discussion generated in the previous chapters, recapitulating key ideas in relation to the nature of ISS, its management and associated risk communications, as well as the implications of a major-event, highly-reliable organizational context. The main contributions and limitations of this study are presented. Any methodological or theoretical concerns related to advancing our understanding of ISS management practices are underlined. Finally, future research directions are suggested.

2. Literature Review

2.1 Introduction: the research problem and literature review directions

As indicated in the introductory chapter of this study, the initial drive of this research was to *understand* the ISS management issues and challenges faced by contemporary organizations that operate in an inherently risky environment, while having a low risk tolerance level. In an effort to do so, literature across disciplines was considered that covered topics of ISS and risk management, accident/error and hazard management. In addition, organization theories that relate to the conditions necessary to deliver highly reliable organizations and IS infrastructures, as well as the obstacles to such a performance, were also considered.

The literature review pointed towards a number of industries that demonstrate a paradoxical performance, namely an increased recognition of the high - often unknown - risk conditions, which however do not hinder organizations from pursuing such endeavours that often result in major disasters. One such industry, which has been inadequately explored, is that of mega (infrastructure) projects and events.

Given that the literature review also pointed towards the need to investigate risk management practices and failures/accidents within their particular organizational and contextual settings, the risk management methodologies applied in the mega project/ event industry were also investigated in more detail.

Therefore, the research problem became more focused around the ISS risk management practices applied in a major-event organization of high reliability requirements. This was achieved after an extended body of literature was reviewed across a number of practices, while the very findings and observations made during the lengthy data collection phase of this study triggered further investigation into existing schools of thought and practice across a range of subjects.

As such, it is vital that the literature reviewed for the purposes of this research is presented here, as this will greatly justify the research focus, as well as the choice of theoretical & methodological directions.

Although the subjects reviewed range across a variety of topics, three main themes were identified, namely:

(a) Information systems security (ISS) risk management;

(b) Technology risk and hazard management; and

(c) Mega project and event management.

The section below of this study is structured along those thematic lines. At the end of the literature review chapter, a justification is provided with regards to the chosen research topic, as well as the choice of conducting this research across disciplines, and 'bridging' knowledge and insightful conclusions from various areas of expertise.

2.2 Information systems security (ISS): managing information integrity

2.2.1. The demand for and evolution of the ISS discipline

The definition of ISS has evolved over time, reflecting new knowledge and changing research, market and legislative demands. Traditionally, ISS has been defined as "the preservation of confidentiality, integrity and availability" (ISO/IEC 17799, 2000) and linked to the concept of 'computer security' (i.e. Whitman and Mattord, 2005).

Contrasting the traditional definition to the more recent one of 'information (systems) security', Baskerville (1992) notes that there are two significant evolutions. Firstly, 'information security' introduces the concept of 'information', which has meaning and brings strategic aspects to information security, while information resides in both electronic and manual forms. Secondly, 'information security' introduces a human component via the inclusion of not only manual systems, but also human processors. This human component highlights the behavioural aspects of information security, such as motivation, cognition, and the interplay of the system with the organization.

The more recent and expanded in scope notion of 'ISS' points to the current inadequacy of the C.I.A. definition. The C.I.A. approach provides a solid technical starting point, but fails to address the organizational and ethical issues faced when dealing with knowledge workers, who can easily compromise proprietary information

(Dhillon and Backhouse, 2001). Employee access to information is increasingly pervasive throughout organizations as the breadth of technology increases[14].

Wenger (2006) suggests that the flattening of organizational structures has had ramifications from a security standpoint. "As organizations become leaner and fitter using technology to reduce layers of management, they run the risk of removing the controls and checks which former supervisory and managerial positions would have applied" (UK Audit Commission, 1994:12). The injudicious distribution of too much organizational knowledge can result in unwanted accountability for those exposed to it (Schultze and Leidner, 2002), as well as greater security risks for the organization.

Given such a new organizational and technological context, the need to expand the definition of 'ISS' has been increasingly acknowledged by researchers, practitioners, and legislators. In addition to the C.I.A. aspects of information security, Dhillon and Backhouse (2000) have proposed adding responsibility, integrity of organizational members, trust, and ethical norms and behaviour. These additional principles are commonly referred to as R.I.T.E. and stress the human component and behavioural aspects of information security.[15]

Meanwhile, recent legislation such as the Sarbanes-Oxley Act and HIPAA has recognized the strategic value of information and the need to expand officially the scope of information security[16]. Such legislation is in fact stressing the need for accountability that adequate controls are in place to protect information from both intentional and unintentional, external and internal threats.

In addition, as accountability demands increase and spending in ISS needs to be justified, organizations require a means to measure the effectiveness of security efforts (Anderson, 2003). The significance of ISS metrics and risk management practices is increasing along with the overall need to take a strategic, business-driven approach to information security. Trust is implied by way of reasonable assurance and accountability, while ethics are implicitly captured in the necessary behaviours required for the realization of organizations' desired outcomes (Spears, 2006a).

---

[14] I.e. Spears, 2006a; Dhillon and Backhouse, 2001; and Cooper, 1999.

[15] According to Rindfleisch (1997) ethical norms can deter insecure practices of trusted personnel, while they can direct behaviour in unforeseen contexts where formal rules do not exist (Dhillon and Backhouse, 2000).

[16] I.e. Geffert, 2004; Spears and Cole, 2006.

ISS is, therefore, defined as "the practice of protecting organizational information of value from both intentional and unintentional acts that adversely affect its safety and providing reasonable assurance of this protection via adequate controls and accountability" (Spears, 2006a:6). Respectively, the goal of ISS is to mitigate the risks to an organization's information assets to a level that is acceptable to management (Pattinson and Anderson, 2006a).

In parallel to the evolution of the 'ISS' definition, the very approaches and focus of ISS research and practice have evolved. D'Arcy and Hovav (2006) identify three ISS approaches to date, namely the technical, financial/economic and behavioural ones.

With regards to the ***technical orientation*** to ISS, "each major technological advance in computing raises new security threats that require new security solutions, and technology moves faster than the rate at which such solutions can be developed" (Gasser, 1998: 8). As such, according to Dhillon and Backhouse (2001) most of the ISS research has been on the formal automated part of an information system. The associated literature views information security as a technical issue that can be effectively managed by selecting appropriate hardware and software components and designing an architecture to protect the information assets of an organization (Dutta and Roy, 2003).

The main body of work focuses on the development of technological ISS solutions[17], while technical ISS researchers have been concerned with ways to incorporate security into the design of information systems[18]. A related stream of technical ISS research has examined risk analysis methods for the design of security information systems. Dhillon and Backhouse (2001) have suggested that the use of risk analysis methods can make information systems more secure if security controls are developed and implemented within information systems in a logical and sequential manner.

[17] Research on the development of technological ISS solutions focuses on topics such as restricting information access to authorised parties (e.g. Irakleous et al., 2002; Osborn et al., 2000), securely transmitting information (e.g. Lou and Liu, 2002), and securely and accurately storing information, and timely retrieving information (e.g. Post and Kagan, 1998). A number of researchers have also focused on the technical details of various threats to information systems, such as viruses (e.g. Cohen, 1984; Bagchi and Udo, 2003), and worms (e.g. Spafford, 1989; Panko, 2003; Chen, 2003).

[18] E.g. Conway et al., 1972; Wang and Wang, 2003; Furnell, 2005; Payne, 2002.

Finally, more recently, researchers have been proposing taxonomies for information security technologies, addressing network, host and application security from both a proactive and reactive perspective (Venter and Eloff, 2003). According to Wenger (2006: 3) "the fact that researchers are building such taxonomies indicates that this area of the field is starting to mature".

The ***financial/economic orientation*** to ISS covers a growing body of ISS literature that explores the financial and economic aspects of ISS, covering topics such as information security investment decision-making[19], the financial impact of security breaches[20], and economic analyses of security threats and associated technological solutions[21].

Finally, ***behavioural information security*** is defined as "the complexes of human action that influence the availability, confidentiality and integrity of information systems" (Stanton et al., 2004: 1388). It has been driven by studies that indicate that technological countermeasures alone do not provide adequate security of information resources. Increasing numbers of researchers now agree that the success of information security depends in part upon the effective behaviour of the individuals involved in its use (D'Arcy and Hovav, 2005).

Depending on the particular focus of behavioural ISS research, it can be distinguished into two approaches, namely the socio-technical and socio-organizational approach (Wenger, 2006).

The first addresses ISS beyond a purely technical perspective, viewing the 'user' as more than simply an abstract entity pursuing a specific information asset, but as a member of the broader organization. Therefore, this approach considers organizational aspects of security, but focuses on the technologies used to address them.

The socio-organizational approach takes a 'softer' view (Checkland, 1981) and emphasizes user participation in information security development, thus increasing user motivation to practice security. Organizational and social issues are considered as important, if not more important, than technological issues (i.e. Wenger, 2006). By adopting this perspective it is that Dhillon and Backhouse (2000) have suggested

[19] E.g. Gordon and Loeb, 2002; Cavusoglu et al. 2004.

[20] E.g. Ettredge and Richardson, 2003; Hovac and D'Arcy, 2003 and 2005; Yayla and Hu, 2005.

[21] E.g. Gopal and Sanders, 1997; Cavusoglu et al. 2005.

the implementation of principle-based approaches to information security. This would include the above mentioned R.I.T.E., thus helping to bridge the gap between a narrow IT and a more socio-organizational perspective of ISS.

Therefore, behavioural research focuses on ways to predict and increase ISS compliance[22], measure the impact of security breach countermeasures on general IS misuse behaviours[23], as well as on an individual level[24].

A variety of theories and evaluation techniques are applied in this domain, which have been criticised of suggesting solutions that are more descriptive than prescriptive in nature[25]. In addition, such behavioural theories tend to focus on the malicious activities that compromise information security, and often neglect the accidental, behavioural events.

Furthermore, researchers[26] suggest that results in behavioural ISS research are often inconclusive, partly because individual and situational differences moderate the impact of various countermeasures, thus suggesting a need to contextualize any behavioural findings and associate solutions.

The use of theoretical frameworks that focus more on the contextual, organizational, social and cultural concerns surrounding ISS behaviours has been suggested[27]. Therefore, approaches that have otherwise been widely used in Information Systems (IS) research such as 'institutional' and 'structuration' theory have been more recently suggested for the ISS field (Li, 2006).

Overall, as the multi-dimensional complexities of ISS are being realized, there is increasing recognition that the approaches and orientations of related research need

---

[22] E.g. Thomson and von Solms, 1998; Stanton et al., 2004 and 2005; Magklaras and Furnell, 2005.

[23] E.g. Straub, 1990; Kankanhalli et al., 2003; Wiant, 2003.

[24] E.g. D'Arcy and Hovav, 2005; Gopal and Sanders, 1997; Foltz, 2000; Harrington, 1996; Lee et al., 2004.

[25] Some of the theories applied in the study of behavioural ISS include the following: (a) General Deterrence Theory (Theoharidou et al., 2005; Straub and Welke, 1998; Parker, 1998); (b) Theory of Reasoned Action (Mishra and Harris, 2006); (c) Theory of Planned Behaviour (Mishra and Harris, 2006); (d) Social Bond Theory (Theoharidou et al., 2005; Hirschi (1969) and (e) Social Learning Theory (Theoharidou et al., 2005).

[26] I.e. D'Arcy and Hovav,2006; Long Li, 2006.

[27] I.e. Long Li, 2006; Dhillon, 2007.

to be integrated[28]. D'Arcy and Hovav (2006) suggest that the interplay between the financial, organizational, best-practices, behavioural, regulatory, technological, and industry dimensions of ISS needs to be considered.

2.2.2. The ISS risk management discipline and practices

Apart from the evident evolution in the way computer and information systems security are perceived, and the greater recognition of the added value of integrative approaches, a further dimension to ISS research has been highlighted - that of ISS 'risk'.

Organizational drivers for ISS risk management

The current demand for increased use of risk management methodologies applied in the field of information systems security (ISS) is supported by the very goal that ISS has evolved into aiming for; namely a balance between security risk and investments in their countermeasures (Pattinson and Anderson, 2006).

There is a growing organizational incentive to invest in ISS risk management controls as financial losses from ISS breaches are increasing[29].The inter- and intra-organizational dependencies with regards to ISS are more widely recognized, and both organizations and legislators are acknowledging what ISS scholars have always stated about the 'weakest link' of a security infrastructure. "One weak link in the organization compromises all other divisions. One unprotected division endangers all of the other divisions in the firm even if they have all invested in security" (Kunreuther and Heal, 2005: 196).

The implication of 'interdependent security' is of course that "the economic incentive for any division in an organization to invest in risk-reduction measures depends on how it expects the other divisions to behave in this respect" (Kunreuther and Heal, 2005: 190).

Therefore, although investing in ISS is becoming increasingly critical, it is not a straight-forward decision. ISS investments need to be proportionate not only to the associated ISS risk, but also to the actions taken throughout the organization. ISS

[28] I.e. Pattinson and Anderson, 2006; Jain, 2006; Smith et al., 2006.

[29] I.e. Gordon et al., 2005; Whitman, 2003.

risks need to be measured and prioritized, while countermeasures' efficiency needs to be coordinated and monitored.

External drivers for ISS risk management

Further to the financial concerns from within organizations, there are also a number of external and industry factors driving ISS towards a risk-management approach.

Whether from increased exposure to ISS threats and the associated media coverage, or the increased availability of ISS standards and best practices[30], organizations are becoming more aware of the criticality of ISS investments with regards to the integrity of their operations and information handling.

In addition, following a series of massive organizational failures - both by corporations and governments - to monitor risks associated with the handling of sensitive information, legislators and regulators are increasingly demanding that information management becomes an issue of corporate and governmental accountability which is closely and transparently managed and monitored[31] (Jones and Ashenden, 2005).

Therefore, as regulation is becoming tighter and markets are becoming increasingly aware of the need to align ISS to strategic organizational goals, ISS compliance and governance are becoming issues that, more than ever before, require top management support and involvement (Jain, 2006).

However, the use of ISS standards and legislations to guide the information security efforts of organizations is not necessarily adequate or simple. Standards are often simplified when used (Shedden et al., 2006), while their effective application requires a great deal of expertise on the part of the assessor regarding risk and risk assessments (Halliday et al., 1996). In addition, standards still suffer from the problem of subjectivity, not only with regards to their interpretation, but also in relation to their translation within an organizational context (Lichtenstein, 1996).

Similarly, the use of legislation to address ISS risks is positive in the sense that it encourages responsibility and accountability, including the documentation of controls and the implementation of audit trails (Spears, 2006a). Nonetheless, legislation

[30] Information Security is addressed by a series of standards and best practices, such as the ISO-27001 & 2, ISO-17799, BS-7799, and the NIST standards.

[31] Such legislative demands include initiatives like the Sarbanes-Oxley Act, HIPPA, Basel-2, Gramms-Leach-Bliley Act, Data Protection Act, and Solvency-2.

suffers the same, if not more, problems than standards have with regards to their ISS utilization. Legislation can be subjective, often vague, and compliance to it is difficult to measure. Most importantly, however, legislation does not address the issues of 'taking care' of ISS problems.

There is, thus, a need to have specific measures for information security (Jain, 2006). There is a need for research on the ways to manage ISS risk and increase individual information security accountability via effective training, awareness and flexible governance structures (Mellor and Noyes, 2006).

The evolution of the ISS risk management discipline

Having established above the evolving need of the ISS discipline to adopt a risk management approach to information security (Shedden et al., 2006: 1), it is worth considering the research that has been conducted in this particular ISS field.

To begin with, 'information security risk management' is defined as

> "the process that helps in balancing operational necessities and economic costs associated with IT-based systems. The overall mission of ISS risk management is to enable an organization to adequately handle information. There are three essential components of risk management: risk assessment, risk mitigation, and risk evaluation" (Dhillon, 2007: 157).

Similarly, and to an extent in parallel, to the greater ISS discipline, ISS risk management has evolved over time in both its focus and application. According to Jones and Ashenden (2005) ISS risk management can be distinguished into four phases.

The first phase is that of risk management efforts focusing on individual IT systems and their implementation, paying scant attention to the risk associated with the people using this, or the processes that underpinned the operation.

As systems became interconnected, it was recognized that attention needed to be paid to the points of connection and now risk assessments focused on the risks exposed by connecting systems together.

The third phase of ISS risk management is identified as the one where information risks on the project level were considered. This was a significant step ahead as the people and processes that surrounded the system were now considered.

The final stage of evolution for risk assessment is for it to be seen as an enterprise-wide issue, often covering all aspects of operational risk in an effort to comply with corporate governance requirements.

ISS risk management research needs to expand further

Although this evolution of the ISS risk management discipline seems positive, there still remain several challenges. Liebenberg and Hoyt (2003) argue that within organizations there has been a paucity of research in ISS enterprise risk management which needs to be amended. Jones and Ashenden (2005) and Spears (2006a) agree and suggest that the discipline needs to broaden further, avoiding the tendency to focus primarily on the technical aspects of ISS. Indeed, addressing the behaviour of individuals and organizations as a more effective means to reducing information risk is picking up ground, while at the same time the related challenge is being increasingly appreciated.

Smith et al, (2006:2) agree with the significance of the behavioural aspects of information security and proceed to stress that

> "organizations need to translate their security framework into an organization culture that is by its very nature more security-aware. While the technical solutions are critically important, their efficient use depends on the extent to which employees are not only trained in using these solutions effectively, but also motivated and willing to perform these functions [...] Effective security isn't one person's job or responsibility; it is the aggregate concern of all employees, and such a concern must be reflected in corporate culture".

However, creating a culture of internal vigilance where every organizational member understands their role in securing the organization's infrastructure remains a difficult matter to tackle. Risk assessment and management practices need to be flexible and adaptive to their context. They need to be insightful and mindful of their audience, which is diverse and increasingly concerned with the ways in which an ISS risk assessment can contribute and is aligned to the business strategy.

As such, consideration of 'softer' aspects of ISS risk has been increasingly proposed, including the examination of the socio-psychological aspects of ISS risk (Pattinson and Anderson, 2006a). Some of the psychological phenomena that have been considered

in the ISS risk management field are risk homeostasis, risk perception, cognitive style, and social inhibition[32].

Although it is only very recently that such research efforts have commenced, it is clear that these have to continue since they can improve the understanding and management of employees' motivations and behaviours with regards to information security (Pattinson and Anderson, 2006a).

Finally, with regards to expanding ISS research, it has been suggested that in today's world an information security approach requires "a total risk management approach which considers security risk controls across three levels, namely that of policies, programs, and technical and access controls" (Jain, 2006: 11).

ISS risk management methodologies

Although the aim of ISS risk management is to secure organizational systems and processes, what is underpinning it is primarily to build trust. A trust that extends "across a broad community so that it encompasses not only the organization itself but goes beyond its boundaries to customers, partners, shareholders, and regulators" (Jones and Ashenden, 2005:244).

In an effort to do so, a number of risk management methodologies have been developed, which have been mostly derived from the Security Development Life Cycle (Jain, 2006) and are commonly used in conjunction with some form of ISS standards, baseline guidelines or principles.

As stated above, any risk management process and associated model has three main stages, namely risk assessment, mitigation, and evaluation (Dhillon, 2007). These imply a series of pro-active - and ideally regularly revised - plans, which should be implemented from the early stages of an IS solution (Jones and Ashenden, 2005). Such plans can guide the collection of risk information; the scope and frequency of risk assessments; the treatment of risk; and the tracking of risks, as well as the changes in the business.

---

[32] For more references on '*risk homeostasis*' see: Wilde, 1994; Filley, 1999; Pattinson and Anderson, 2006a and 2006b. References on '*risk perception*' include Heimer, 1988; Bener, 2000; Otway, 1980; Lippa, 1994; Pattinson and Anderson, 2006a. References on the '*cognitive style*' include Witkin et al, 1977; Ausburn and Ausburn, 1978; Pattinson and Anderson, 2006a. Finally, '*social inhibition*' references include Latane and Darley, 1969; Pattinson and Anderson, 2006a.

In addition to the proactive identification and mitigation of risks, there are a number of methodologies that focus on the management of incidents or disasters in the immediate, short- and long-term time frames respectively. Such Incident Management, Disaster Recovery, and Business Continuity methodologies include their respective plans, which focus on the incident reactive controls in place that will contain and manage ISS failures and operational disruptions[33].

However, as Jones and Ashenden (2005) point out, ISS risk assessment and management methodologies seem to address the pro-active and re-active matters separately, omitting their interdependencies. Thus, they support a holistic ISS risk management methodology, where proactively understanding the organizational context, preparing for the associated risks, and learning from incidents and mistakes, form a greater symbiotic cycle.

One further criticism of such ISS risk management methodologies is similar to the one highlighted above with regards to the use of ISS standards. Despite the above structured approach to dealing with ISS risk, it is widely accepted that such methodologies often do not cover how to go about conducting these assessment and management efforts (Shedden et al., 2006).

Finally, Jones and Ashenden (2005) identify time, resource and budget constraints as factors that may complicate ISS risk decision making and implementation. They also identify political and reputational considerations that may complicate the risk management processes, and add that "it may be easier to impose risk management techniques downstream in the value chain but harder to achieve upstream" (Jones and Ashenden, 2005: 9, 188).

The 'art' of managing ISS risks - required skills

Hence, the process of ISS risk management is a complex one, despite the implied simplicity by the associated methodologies and frameworks. As Jones and Ashenden (2005:25) argue, the management of ISS risks is an 'art' rather than a science.

> "The risk manager needs a broad set of skills and thought processes to be successful. [...] She/he needs to understand risk dependencies between information assets, different technology implementations, different stakeholder groups within the organization, and the different environments in which the organization operates".

[33] I.e. Spencer, 2006; Jones and Ashenden, 2005.

ISS risk management needs to 'bridge' thinking and skills across disciplines and boundaries. It needs to be aligned to the organizational structure, and therefore the ISS risk manager must understand the context and the implications of technology in business terms. "Information security risk managers need a certain amount of business knowledge, coupled with technical understanding and good communication skills" (Jones and Ashenden, 2005:26).

In addition, ISS risk managers/experts need to be able to utilize both qualitative and quantitative risk analysis methods, while acknowledging the limitations of both these approaches[34]. They also need to be familiar with ISS risk assessment methodologies[35], and incorporate both ISS audits and assessments as part of their risk identification and monitoring efforts (Fagnot and Stanton, 2006).

Finally, ISS risk managers must be appreciative of the organizational ISS culture, and identify the best means to communicate ISS risk messages to the end-users, IT specialists, Board members, or other third parties.

The 'soft' aspects of ISS controls

This more holistic approach to information security risk has raised attention to several 'softer' aspects of ISS and their impact and dynamic interaction with 'harder', more technical aspects[36].

As indicated earlier, the human component and behavioural aspects of ISS have been increasingly appreciated[37] and a number of human factors that have the potential to impact upon an organization's ISS has been identified (Pattinson and Anderson, 2007). Some of these include: (a) the organizational structure and risk culture; (b) the individual propensity to take risks; (c) the individual/group perception of risks; (d) familiarity with the risk communication; (e) age, gender, position in the organization; (f) the amount of education and training; (g) the individual cognitive style; and (h) experience.

---

[34] For more information on the quantitative and qualitative risk analysis methods see Jones and Ashenden, 2005:215-218.

[35] I.e. NIST, 2000.

[36] I.e. Dhillon and Backhouse, 1994; Dhillon, 2007.

[37] I.e. Spears, 2006a; Pattinson and Anderson, 2005; Schneier, 2000 and 2004; Pincus, 2005; Heiser, 2005.

Similarly, the communication of ISS risks and controls and the contextual surrounding of these have been increasingly indicated as crucial factors to the effectiveness of any ISS risk management efforts.

In addition, some research is being conducted in the area of ISS risk perceptions, although this field remains immature. Efforts are being made to bridge work done in the ISS and risk perception fields. The 'framing' of ISS messages is considered to be a significant tool in the management or risk perceptions, requiring further exploration[38].

ISS risk communication is also considered to be a means to improving levels of organizational trust in ISS controls and controllers. Spears (2006a:6) identifies trust in the ISS context to imply "reasonable assurance and accountability", while Jones and Ashenden (2005:245) describe it as "a predisposition to expose oneself to a security risk". As part of the RITE-principles of ISS, Dhillon (2007:322) defines trust as assurance that other organizational members will act in accordance with organizational norms and accepted patterns of behaviour. Regardless of the exact definition of trust in ISS, the linkage between trust, governance, and compliance are increasingly stressed as an important factor in an organization's ability to demonstrate integrity and value for its stakeholders.

Trust has been also linked to organizational structures of accountability, responsibility and ethics, which in total form the context of any ISS risk and control. This organizational context that captures "the totality of patterns of behaviour that come together to ensure protection of organizational information resources" is known as the 'security culture' of an organization (Dhillon, 2007:221).

Having identified organizations as agents of risk generation, management and control, efforts have been made to map organizations' security culture, and define what a robust security culture is, thus providing guiding principles to its development[39].

[38] I.e. Dhillon, 2007; Pattinson and Anderson, 2005 and 2007.

[39] E.g. Smith et al., 2006; Wenger, 2006. In addition, Dhillon (2007) argues that culture can be studied by analysing the communication processes of an organization. He, thus, suggests using Hall's (1959) 'Web of Culture'[39] in order to map the ways in which different cultural streams interact with each other, and the patterns of behaviour they lead to.

Futhermore, in an effort to deal with ISS insider threats[40], suggestions have been made that organizations need to take into consideration the employees and their 'psychological contract'[41] and proactively deal with any potential behavioural ISS problems (Wenger, 2006). Smith et al. (2006:3) suggest that

> "several prerequisites must be met for maintaining an efficacious security culture, including decent, regularly paid wages and a stable working environment. The workforce must have the skills, knowledge and motivation to do their jobs in accordance with best practices".

In addition, ISS awareness and training have been identified as key methods to internalize ISS into the organizational culture (Wenger, 2006; Smith et al., 2006). ISS researchers suggest that ISS awareness and training should stress that ISS is every employee's responsibility, supporting individual accountability and ownership of security. Making employees understand the consequences of their individual actions can transform them from passive learners to active ones (Mellor and Noyes, 2006). Having established that legacy ISS training practices are ineffective (Bradford, 2003; Desman, 2003), increasing research is carried out in this area in order to provide guidelines that will turn organizations' largest security liability - its personnel - to its largest asset (Mellor and Noyes, 2006).

Some of the guidelines found across the related research suggest that ISS training should be organized, with clear goals and stages, as well as interactive and where possible certified and evaluated. Moreover, it should take place across all ISS domains, while ISS trainers must be appropriately skilled[42].

A further means to improve ISS awareness and behavioural practice is through learning from incidents (Spencer, 2006). However, as Spagnoletti (2006:2) argues, this is a challenging activity since preventing and investigating incidents is a complex task in itself.

---

[40] Research and statistics have repeatedly indicated that one of the most significant ISS threats for organizations is their employees and 'trusted' partners (i.e. Spears, 2006a; Dhillon, 2001).

[41] The 'psychological contract' is defined by Wenger (2006:1) as "the employees' beliefs about the mutual obligations between themselves and the organization. It extends beyond the specifics that may be outlined in employment contracts [...] and includes expectations for continued employment, advancement opportunities, and work environment".

[42] I.e. the NIST SP 800-16 standard, and Pfefer (2003).

> "Computer incidents are a significant example of 'drift'[43] and are strongly related to the context in which they take place. In this sense, the design of appropriate ISS Management Systems can take a very large advantage from the deep understanding of single incidents performed by case studies".

These can improve management's ability to make decisions about investments on security preventing measures at the technical, formal and informal levels.

Hence, Spagnoletti (2006) proceeds with the utilization of the Theory of Crime Prevention and Situational Crime Prevention[44] to investigate and reduce ISS incidents. Some of the findings of this case-study research indicate (a) the unpredictability of human behaviour; (b) the significance of improvisation in the context of emerging circumstances; (c) the need for interpretive frameworks to investigate incidents; and (d) that in-depth case-studies of incidents can represent a valuable source of information to design systems and to increase the awareness of people.

Finally, as part of the heightened attention towards the 'softer' aspects of ISS and the management of associated risks, the increased levels of proactive user participation in the risk identification and assessment processes have been put forward[45].

2.2.3. Future and further ISS research

Overall, ISS literature and research have evolved significantly over the past decades, in order to meet the changing organizational, market, and threat-profile demands. There has been an increasing recognition of the interdependencies of ISS, as well as its multiple dimensions, thus stressing the need to take more holistic approaches to ISS decision-making and controls. In addition, there has been an increased consideration of more structured ways to address and manage ISS risks.

---

[43] I.e.Ciborra et al (2000).

[44] The 'Theory of Crime Prevention' and 'Situational Crime Prevention' is based on the idea that crime results partly from the opportunities presented by the physical environment. This being the case it should be possible to alter the physical environment so that crime is less likely to occur. Thus, they refer to a preventive approach that relies upon reducing opportunities for crime.

[45] I.e. Spears (2006b) and Suh and Han (2003).

Holistic ISS models and ISS risk management methodologies have, therefore, helped towards the identification and creation of ISS risk and control typographies and guidelines. Nevertheless, there are several areas of both the ISS and ISS-risk disciplines that need to mature further. Among others, some of the themes identified include the following:

There is a need to investigate further the informal, behavioural aspects of ISS within specific contexts. Such research should cover matters of effective ISS communications and better understanding of end-users' risk perceptions and decision-making processes, thus leading to greater compliance levels. Research conducted in other disciplines, such as psychology, sociology, and anthropology, should be utilised to that direction[46].

Furthermore, a need has been identified to investigate means to create an effective security culture that is integrated with the work culture and organizational structure[47], including better recruitment and personnel management methods that will enhance any efforts to create an organizational security culture[48]. Similarly, the importance of effective stakeholder involvement in the ISS decision-making process has been acknowledged[49].

In addition, researchers have pointed out the benefits of integrating research across the various ISS levels, aiming to develop an enterprise-wide, total risk management approach. ISS risk methodologies should facilitate for the multi-dimensional aspects of ISS throughout all their stages[50].

Finally, researchers have highlighted the need for theoretically founded methodologies in order to investigate ISS incidents[51].

---

[46] I.e. Pattinson and Anderson, 2005, 2006a, 2006b; Jain, 2006; Mishra and Harris, 2006.

[47] I.e. Smith et al., 2006; Spears, 2006b.

[48] I.e. Mishra and Harris, 2006.

[49] I.e. Jain, 2006; Mishra and Harris, 2006; Spears, 2006b.

[50] I.e. Jones and Ashenden, 2005; Jain, 2006; Mishra and Harris, 2006; D'Arcy and Hovav, 2006.

[51] I.e. Spagnoletti, 2006.

2.3 Risk and hazard management: managing uncertainty

As explored in section 2.2 of this study, the notion of risk and the value of risk management practices in the information systems security (ISS) field have been receiving increasing recognition. The need for holistic risk management and communication methodologies that are founded on solid theoretical underpinnings and will facilitate the improvement of ISS practices has been highlighted, yet inadequately explored.

'Risk', on the other hand, consists of a greater discipline of its own, with sizeable research and associated practices.

The purpose of this section is to consider the research and practices in the risk discipline, and thus appreciate the ways in which technological risk and hazard management have been approached. The researcher's view is that the ISS risk management field can benefit from the cross-disciplinary investigation of concepts of technological uncertainty, risk and hazard.

2.3.1. The history and evolution of approaches to risk

"While the idea of risk management can be traced to ancient times [...] and while risk has been an essential underpinning to investment and insurance practices for centuries, the systematic application of risk to evaluate the technologies and products of high modernism is a child of the late 20th century" (Jaeger et al., 2001:9).

According to Jaeger et al. (2001) in common usage 'risk' has a wide range of connotations. Despite however usage variation, there are unifying features that ground the meaning of risk. All conceptions of risk presuppose a distinction between predetermination and possibility (Renn, 1992a). Risk implies both the possibility that an event or outcome can happen with the denial that either occurs with predetermined certainty. Risk thus necessarily implies uncertainty.

> "As a result, humans try to make causal connections between present actions and future outcomes, and they exercise agency in attempting to shape the causes of future outcomes. [...] However, not all uncertainty is risk. [...] A risk is present only to the extent that uncertainty involves some feature of the world that impacts human reality in some way. Risk, in human terms, only exists when humans have a stake in outcomes" (Jaeger et al., 2001:17).

Therefore, 'risk' is defined as "a situation or event in which something of human value has been put at stake and where the outcome is uncertain" (Rosa, 1998:16).

Such a definition leads to three associated questions with regards to (a) the scope of negative effects, (b) the conceptualization of uncertainty, and (c) the rule of aggregation for practical purposes. The perspectives adopted in order to respond to these three questions of any risk debate differ greatly, indicating the conceptual diversity and complexity in addressing risk. The focus and key references of each perspective are summarised in Appendix-A1.

A critical investigation of the various perspectives within the risk discipline indicates that despite the straightforwardness of technical and economic approaches, their narrowness is a virtue as much as it is a shortcoming (Merkhofer, 1984). Society is not only concerned with risk minimization (Douglas and Wildavsky, 1982). Context matters, and therefore a broader scope of undesirable effects needs to be adopted.

According to Fischhoff (1994) the social sciences perspectives on risk can help to identify public concerns associated with a source of risk, and explain the context of risk-taking situations. In addition, they can assist towards identifying cultural meanings and associations linked with special risk arenas. Sociological approaches to risk can also contribute to the design of procedures or policies that incorporate cultural values within the decision-making processes. Furthermore, they can assist with the design of programmes for participation in decision-making, and the performance evaluation of risk management controls.

Yet, social perspectives of risk can lead to varying advice from social scientists, while they do not offer a common denominator for measuring cultural or social acceptability (Kasperson, 2005a). Hence, Renn (2008) suggests that different risk situations may require different theoretical frameworks for their analyses, while it is crucial to initiate a discourse among the major parties involved in the decision-making process or affected by the decision outcomes. Participation is a requirement for rational decision-making in situations in which risks need to be evaluated (Jasanoff, 2004).

Thus, Renn (2008:45) stresses that a dual strategy is needed for risk management. The balancing of opportunities and hazards of modern technologies and other human activities "requires a plural, yet integrated, attempt to have technical and social sciences join forces to shape a humane future in line with best available knowledge and a consensus on social expectations".

2.3.2. 'Systemic risks' and the broadening of risk management

The emergence of 'systemic risks'

Beyond the social constructivism versus realism debate in the risk discipline, the changing scope and impact of contemporary risks has influenced the focus of the risk debate. The profound and rapid technological, economic and social changes that the modern world experiences today has lead to the emergence of a new concept of risks that have been labelled as 'systemic risks' (OECD, 2003). They are characterised by high complexity, uncertainty, ambiguity, and ripple effects[52]. Due to these characteristics, systemic risks are overextending established risk management and creating new, unsolved challenges for policy making in risk management (Klinke and Renn, 2006). Their negative effects are often pervasive, impacting fields beyond the obvious primary areas of harm. Therefore, "investigating systemic risks goes beyond the usual analysis of causes and consequences, and focuses instead on the interdependencies and spillovers between various clusters" (Renn and Klinke, 2004:41).

As such, systemic risks require that risk analysis and management become increasingly important fields to identify new, as yet unknown, risks and to devise methods for dealing with them efficiently. Data from different risk sources needs to be integrated within one analytical perspective, while a holistic approach must be taken with regards to hazard identification, risk assessment, concern assessment, tolerability/acceptability judgements and risk management. To handle systemic risks interdisciplinary and holistic mechanisms in governance across boundaries are required (Klinke and Renn, 2006; IRGC, 2007).

[52] The four major properties of systemic risks are defined by Klinke and Renn (2006) as follows: (a) *Complexity* refers to the difficulty of identifying and quantifying causal links between a multitude of potential candidates and specific adverse effects. (b) *Uncertainty* reduces the strength of confidence in the estimated cause and effect chain. (c) *Ambiguity* denotes the variability of (legitimate) interpretations based on identical observations or data assessments. High complexity and uncertainty favour the emergence of ambiguity, but there are also quite a few simple and almost certain risks that can cause controversy and thus ambiguity. (d) *Ripple Effects* indicate the secondary and tertiary consequences regarding time and space.

A broader perspective to risk management

In order to address these emerging systemic risks, scholars have stressed the need for risk managers not only to conduct risk evaluations based on systematic and experiential knowledge, but also act in situations of 'non-knowledge' or insufficient knowledge about potential outcomes of human actions or activities.

Therefore, across the various steps of a hazard/risk chain, risk management interventions can occur both preventatively and reactively (i.e. Fig. 2.1). In addition, risk management refers not only to the implementation of precautionary controls, but also to the evaluation and establishment of proactive structures of risk preparedness, resilience and robustness.

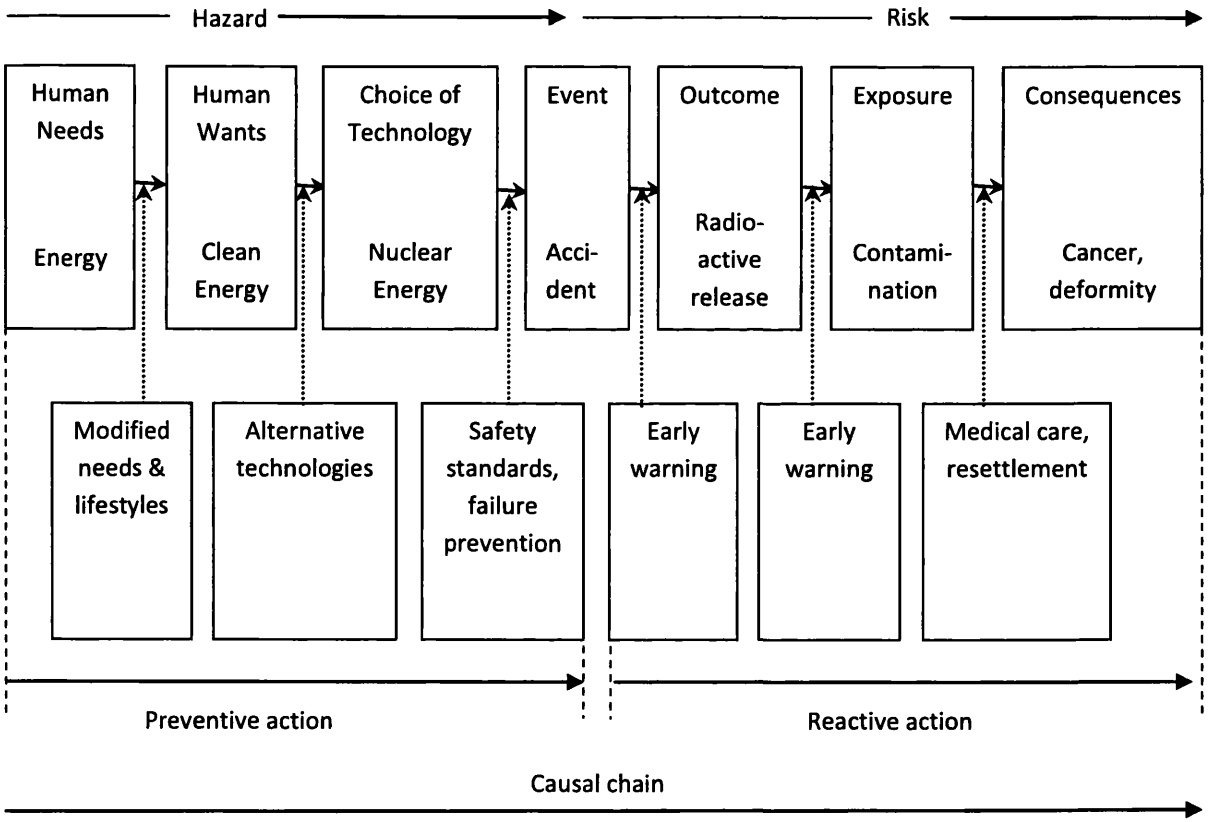


Figure 2.1: *Seven steps of a hazard/risk chain: the example of nuclear energy* (Source: adapted from Renn, 2008:7).

By recognizing this broader scope of risk management and the need for collaboration and coordinated efforts across a range of stakeholders, over the past decade the term 'governance' has experienced increasing popularity in the field of risk research.

'*Risk governance*' includes, but also extends beyond, the three conventionally recognized elements of risk handling, namely risk assessment, management and

communication. It requires consideration of the legal, institutional, social and economic contexts in which a risk is evaluated, and involvement of the actors and stakeholders who present them.

Risk governance is of particular importance in, but not restricted to, situations where there is no single authority to take a binding risk management decision. In addition, it not only includes a multifaceted, multi-actor risk process but also calls for the consideration of contextual factors such as institutional arrangements and political culture, including different perceptions of risk. Thus, a risk governance framework should also include concern assessment and explicit discussion of stakeholder participation (Renn, 2008). It should apply "the principles of good governance that include transparency, effectiveness and efficiency, accountability, strategic focus, sustainability, equity and fairness" (IRGC, 2007).

Therefore, the findings from the above review of risk theories (i.e. Appendix-A1) and the acknowledgement of the emerging systemic risks across areas of human activity encourage an *inclusive* model of risk governance[53]; a model that adopts a process-based approach to risk and considers both its physical and social dimensions (Renn, 2008).

2.3.3. Managing uncertainty: introducing contextualised risk governance

Risk governance - a process of interlinked phases

Supporting the utilization of an inclusive governance model, the International Risk Governance Council (IRGC) has suggested a framework that is in line with professional codices and risk governance legislation. This framework consists of four cyclical, iterative and interlinked consecutive phases, namely pre-assessment, appraisal, characterization/evaluation, and management. Risk communication is a process accompanying all these phases (Fig. 2.2).

[53] References relevant to the various models of risk governance include: Benz and Everlein, 1999; Lyall and Tait, 2004; Bunting et al., 2007; Millstone et al., 2004.

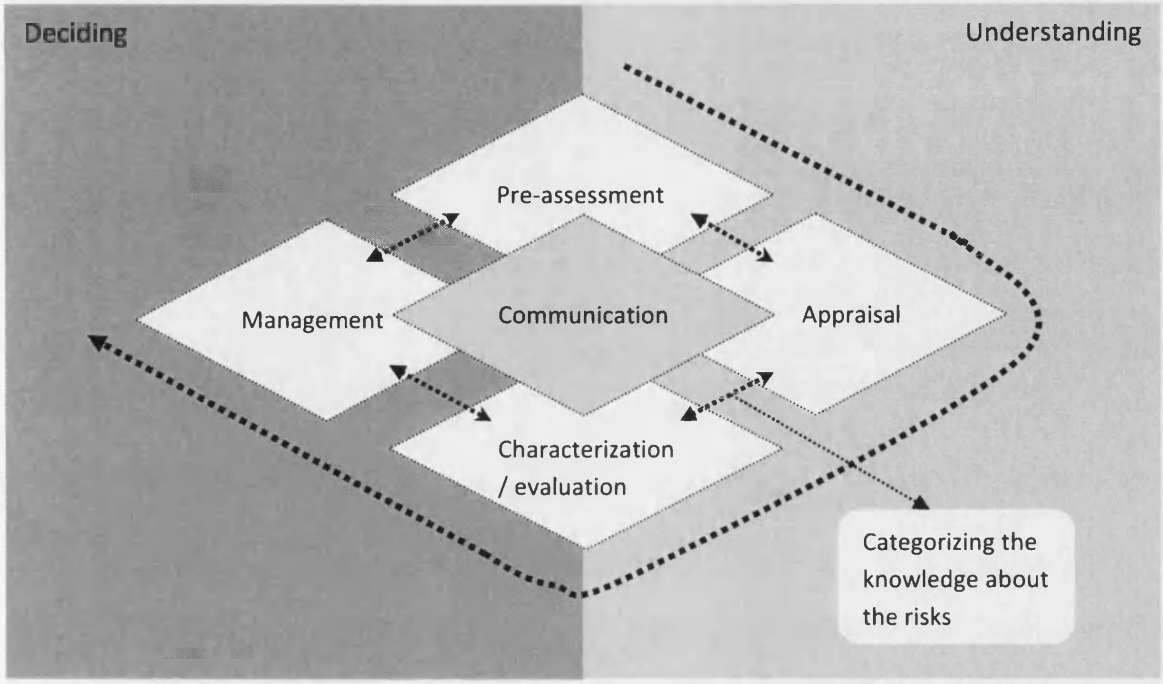


Figure 2.2: *The five elements of risk governance* (Source: adapted from IRGC, 2007:8)

Further to the two major phases of any risk handling framework, namely those of *risk appraisal* and *risk management*[54], the framework suggested by the IRGC (2005) also introduces the phases of *risk pre-assessment* and *characterization/ evaluation.*[55] The objective of such a design is to avoid the naïve separation of facts here and values there, while also escaping "the solipsism of post-modern relativity by honouring the analytical distinctions between the factual world and the world of values even if they clearly interact" (Renn, 2008:48).

The accomplishment is to move towards a more contextualised and holistic appreciation of risk governance processes and efforts, stressing the need to gain a thorough understanding of a risk and to develop options for dealing with it.

---

[54] *'Risk appraisal'* refers to the generation and collection of knowledge about a risk, while *'risk management'* refers to the decision-making about how to mitigate, control and otherwise manage a risk.

[55] According to the IRGC (2005), *'pre-assessment'* aims to capture both the variety of issues that stakeholders and society may associate with a certain risk as well as existing indicators, routines, and conventions that may prematurely narrow down what is going to be addressed as risk. *'Characterisation/evaluation'* aims to judge a risk's acceptability and/or tolerability.

Risk communication, participation & stakeholder involvement

The 'risk communication' element of the risk governance process is one that has received considerable attention over the last decade. In fact, it is a topic much broader than implied by the risk governance process.

The field of risk communication initially developed as a means of investigating how expert assessments could be best communicated to the public, thereby bridging the tension between expert judgements and public perceptions. In the course of time, this original objective has been modified and, some would argue, even reversed (Plough and Krimsky, 1987).

In more recent practices the objective of policy makers and risk experts is for risk communication to reflect the nature of the risks under consideration, their context and whether they arouse societal concern (Renn, 2008).

With relation to understanding the context of risk communication, Renn (2001) has identified three levels that must be addressed during a risk debate, namely (a) factual evidence and probabilities, (b) institutional performance, expertise and experience, and (c) conflicts about world views and value systems.

In turn, these three levels of risk correspond to the nature of the risk under question (Renn, 2007b). Utilizing the risk characterization model summarized in Appendix-A2, each type of risk - namely simple, complex, uncertain and ambiguous - maps onto a different risk level debate, thus requiring a different communication strategy.

In addition to identifying the objectives and associated strategies of risk communication, researchers[56] have offered a number of recommendations with regards to effectively communicating risk.

Moreover, researchers[57] have stressed the significance of *evaluating* risk communication efforts, referring to the need to scientifically assess the content, process and effects of an intervention according to defined criteria.

Finally, as the criticality of risk communication to the improvement of risk governance and the need for a mutual learning process have been established (Leiss, 1996), the importance of having stakeholders and public groups participate throughout the risk-handling process has been underlined.

---

[56] I.e. Breakwell, 2007; Renn, 2008; Löfstedt, 2005.

[57] I.e. Kasperson and Palmlund, 1989; Rohrmann, 1992; OECD, 2002.

However, risk participation and stakeholder involvement do not imply the inclusion of all public actors in all risk controversies. This would be inefficient and a waste of time and money (Renn, 2008, Löfstedt, 2003). The involvement process should be in proportion to the degree of public demand and conflict intensity. This will directly determine the potential benefits resulting from stakeholder and public involvement.

Therefore, the four classes of risk problems presented earlier - namely simple/linear, complex, uncertain, and ambiguous - support generic suggestions for participation. These have been summarised by (Renn, 2004b) and IRGC (2005) as in Appendix-A2.

Finally, researchers suggest that regardless of the type of risk problem and associated type of discourse and remedy, the design of participatory procedures, at any phase and at any level of intensity, should display the following features: transparency, competence, fairness, efficiency, clear mandate, diversity, and professionalism[58].

2.3.4. Managing the unexpected: hazards, accidents and errors

As examined in the paragraphs above, it has been suggested[59] that risk management strategies should vary according to the type of risk a group or organization is dealing with. Therefore, interventions to a hazard/risk chain can occur either/both preventatively and/or reactively (Fig. 2.1).

While simple risks can be routinely managed and assume that the risk management structures are in place to prevent a risk or successfully contain its impact, in the case of complex and uncertain risks matters are more complicated. They require organizational mechanisms that support information gathering, learning, and risk absorption to support either robustness or resilience.

Management of complex and uncertain risks implies management of the unexpected, of errors and accidents. It is, therefore, understandable that a considerable body of research has focused on the effective management of errors and accidents, an unavoidable part of organizational life. Therefore, the notion of risk management within an organizational context expands to cover also the notion of 'safety management'.

---

[58] I.e. Webler, 1995, 1999; Goldschmidt and Renn, 2006; Renn, 2004b, 2008.

[59] I.e. Renn, 2008, IRGC, 2005. Also see Appendix-A2.

> "Organizational encounters with risk and error are [...] a routine and systematic part of daily organizational life that only occasionally becomes visible to outsiders. [...] Unanticipated events that deviate from organizational expectations are so typical that they are 'routine non-conformity' - a regular by-product of the characteristics of the system itself. [...] Complex organizations that use or produce risky technologies may have encounters with risk daily" (Vaughan, 2005:33).

Yet, research has indicated that accidents have a history of early-warning signs that were either misinterpreted or ignored[60]. Every anomaly has a trajectory, during which it is subject to processes of definition, negotiation, and control. How anomalies are defined depends upon the occupational context and evaluation systems that have been developed to meet unexpected deviation in the work flow. A mistake or an anomaly is never defined in isolation, but is always relative to the local and institutional context of work[61].

Identifying, making sense of, and controlling an incident or accident[62] implies an organizational ability to synthesize and share incident information effectively, thus learning from it. However, it is not uncommon that incidents are only visible with the benefit of hindsight that comes from an accident[63]. This has raised debates with regards to the extent that an effective incident management system can prevent all accidents and disasters.

In studying risk of complex technologies and organizational structures, there have been two disparate theoretical approaches, namely the theory of normal accidents and the theory of high reliability:

The foundations of the **Normal Accident Theory** were laid by Perrow (1984) and further consolidated by the work of Sagan (1993). It asserts that accidents are a normal consequence of interactive complexity and close coupling of an organizational system.

---

[60] I.e. Turner, 1978; Turner and Pidgeon, 1997.

[61] I.e. Star and Gerson, 1987; Vaughan, 2005.

[62] An 'incident' is defined as an unexpected or unwanted change from normal system behaviour which causes or has the potential to cause a loss. An 'accident' is an incident in which a non-trivial loss occurs, while a 'disaster' is a very serious incident involving loss of life and/or extensive property damage (Cooke and Rohleder, 2006).

[63] I.e. Cooke and Rohleder, 2006; Vaughan, 2005.

The measure of '*interactive complexity*' is the number of ways in which components of the system can interact. It represents the number of variables in the system, the number of relationships between the variables and the number of feedback loops through which the variables interact. Typically, interactive complexity increases with the technology incorporated into the system.

Respectively, '*close coupling*' is measured by the speed at which a change in one variable cascades through the system to cause changes in other system variables. Close coupling represents tightness in the process, which is influenced by such things such as component redundancy, resource buffers/slack, and process flexibility.

The idea behind the Normal Accident Theory is that some of the system responses to change are unforeseen, are causes of incidents, and can potentially lead to catastrophes.

On the other hand, proponents of the **High Reliability Theory**[64] believe that while accidents may be normal, serious ones can be prevented by implementing certain organizational practices. In particular, Weick and Sutcliffe (2001) suggest that high-reliability organizations should implement business processes to instil 'mindfulness' qualities into the organization. These include preoccupation with failure, reluctance to simplify, sensitivity to operations, commitment to resilience, and deference to expertise. Meanwhile, Sagan (1993) supports that High Reliability Theory requires four essential elements to succeed: (a) high management priority on safety and reliability; (b) redundancy and backup for people and equipment; (c) decentralised organization with a strong culture and commitment to training; and (d) organizational learning through trial and error, supported by anticipation and simulation.

However, Sagan (1993), as a proponent of Normal Accident Theory, argues that the organizational learning required for the success of high-reliability theory will be restricted for several reasons, including the ambiguity about incident causation; the politicized environments in which incident investigation takes place; the human tendency to cover up mistakes; and the secrecy both within and between competing organizations.

[64] I.e. La Porte and Consolini, 1991; Roberts and Bea, 2001; Weick and Sutcliffe, 2001 and 2007.

Apart from the theoretical differences between the two approaches, there are also implications on the methodologies they use (Vaughan, 2005). Normal accident theorists study failure and emphasize that complex systems will inevitably fail. They tend to study incidents after the fact, concentrating on public failures with high costs. On the other hand, high reliability theorists study safe systems, emphasizing processes by linking them to successes. Rather than after-the-fact analysis, their research is done by locating themselves in an organization to interview and watch work practices and how risk is managed. Differences between the two approaches are quite significant. However, a number of more recent studies tend to blur the genres created by the dichotomy[65].

Of particular research interest is the work conducted by Cooke and Rohleder (2006), who agree that it is not natural for organizations to learn from safety incidents. Even if ad hoc learning is occurring it is not enough. Instead they promote the implementation of an effective and formal incident learning system. The 'Theory of Incident Learning' relies on the observation initially made by Turner (1978) that disasters have long *incubation periods* during which warning signals (or incidents) are not detected or are ignored. Thus, while the occurrence of incidents may be normal, an organization with an effective incident learning system can respond to these incidents to prevent serious accidents from occurring in the future. An organization implementing an effective and formal incident learning system may evolve into a high-reliability organization over time.

In addition to the incident learning system and process suggested by Cooke and Rohleder (2006), further research into organizational accident and error management indicates that errors and early warning signs remain not merely undetected, but often are misinterpreted[66]. The reason offered for this is the 'normalization of deviance'; a social psychological product of institutional and organizational forces. "Anomalies are not interpreted as warning signs but become acceptable, routine and taken-for-granted aspects of daily work. The trajectory of anomalies as they were identified and their risk measured and assessed, shows the importance of both the local organizational and institutional contexts of work" (Vaughan, 2005:34).

---

[65] I.e. Carroll and Perin, 1995; Weick, 1990; Roberts and Libuser, 1993; La Porte, 1994; Clarke, 1992 and 1993; Vaughan, 1996, 1999, 2002 and 2005; Schulman, 1993a; and Marcus, 1995.

[66] I.e. Vaughan, 1996; 1999; 2002; 2005.

It is, thus, concluded that learning from a disaster emerges as a complex, ambiguous process that is conditioned by culture and organizational and/or institutional context (Jasanoff, 2005). It is not easily forced into univocal, totalizing causal narratives, since perceptions vary and the boundary between factual and moral causes (i.e. responsibility versus blame) are dynamic. Whether an organization adopts a compliance or deterrence strategy, errors are a part of organizational life and learning from incidents is a continuous process, which needs to be effectively sustained.

2.4 Megaproject and event management: managing the unknown

Following a review of research conducted in both the ISS and broader risk disciplines, one common theme appears to dominate - the significance of context. Whether 'context' is perceived as the organizational, institutional, socio-economic or/and cultural environment within which certain ISS or risk management activities take place, it is undoubtedly a determining factor in terms of how risks are identified, made sense of, and controlled.

In the case of this study, the organizational context - namely that of a major event - is a significant component of the research question. As presented in section 1.2, the researcher aims to understand ISS risk management needs and practices in a major event context, interpreting the organizational capacity to deliver highly reliable IS operations.

Thus, apart from investigating the research work conducted in the ISS and risk disciplines, it is also important to consider the significant work conducted in the mega project/event fields. This will demonstrate the characteristics and challenges of such contexts, and will shed some light on the potential implications that a major event context can have on efforts to produce reliable ISS operations.

2.4.1. Megaprojects and events in demand - a 'performance paradox'

Mega infrastructure projects of every kind have been labelled as "a new political and physical animal" (Flyvbjerg et al, 2003:1), forming part of 'the Great War of Independence from Space', and resulting to a new mobility that is the most powerful and coveted stratifying factor in contemporary society (Bauman, 1998). Mega infrastructures aim to increase connectivity, whether that is physical, virtual/technological, or socio-cultural, giving rise to the new 'politics of distance'. Megaprojects are central to this, since infrastructure is increasingly built as *megaprojects* (Flyvbjerg et al, 2003).

In addition to such projects, there is an increasing demand for *major events*, a form of megaprojects, which aim to connect people at a specified time and place for a variety of purposes. Similar to projects, events touch virtually every life on the planet generating economic and socio-cultural value through the development and enhancement of business and personal relationships, facilitating fraternal and familial reunion, and increasing community pride and improving quality of life (IFEA:

2005). Events are produced every day for all manner of purposes and attracting all sorts of people. There is, therefore, an increasing recognition that this is a significant line of business that carries great obligations and is becoming increasingly greater in scope and complexity (Silvers, 2008).

The physical and economic scale of today's megaprojects and events are such that whole nations may be affected in both the medium and long term by the success or failure of just a single project. As Merrow (1998) suggests, the success of these projects is so important to their sponsors that firms and even governments can collapse when they fail.

However, a study by the Major Projects Association (1994) concludes that too many projects proceed that should not have done so, often with a significant cost-overrun calamity that extends beyond the public sector.

While many more and much larger projects and events are being proposed and implemented around the world, it is becoming clear that cost overruns and lower-than-predicted revenues frequently place project and event viability at risk, redefining them from effective vehicles to economic growth to possible obstacles to such growth[67]. The reasons behind this 'megaproject performance paradox' are multiple. Among others, researchers have identified a biased motivation to generate optimistic demand forecasts, to 'cook' project costs and benefits, and to use the alibi of economic growth. Megaproject and event development today is not a field of 'honest numbers' (Williams, 1998). It is a field where one group of professionals and experts will call the work of another not only 'biased' and 'seriously flawed' but a 'grave embarrassment' to the profession (Huszar, 1998). "Megaproject development is currently a field where little can be trusted, not even numbers produced by analysts" (Flyvbjerg et al, 2003:5).

In addition, Flyvbjerg et al. (2003) identify a lack of accountability in the project decision-making process, which aggravates matters. Project stakeholders do not always adequately represent publics, thereby highlighting the need to properly involve publics in the decision-making in carefully designed deliberative processes from the beginning and throughout large-scale projects[68].

[67] I.e. Morris and Hough, 1987; Flyvbjerg et al, 2003.

[68] I.e. Ryan and Destefano, 2000; Weeks, 2000; Dryzek, 2000.

Furthermore, it is often evident that "once the promotion process of a project/event is off to a successful start, it is hard to stop again [...] It takes outsider forces to stop this process" (Flyvbjerg et al.; 2003:39). As such, in megaproject development it is crucial that outside checks and balances are institutionalised to restrain and govern a process that otherwise tends to become an anarchic and self-serving means for rent-seeking by special interest groups (Khan & Jomo, 2000).

Similarly, "in the majority of instances of cost changes in projects, the responsible authorities did not recalculate the project viability" (Flyvbjerg et al., 2003:42). A review of the World Bank's project portfolio documented an increasing number of poorly performing projects, identifying as the main cause the over-optimistic estimates of project viability in the planning phases. There has been a widening gap between forecast and actual viability, resulting to the World Bank demanding not only far more accuracy in estimates of viability, but also more honesty that will be improved through accountability controls (World Bank, 1994).

In another report by the World Bank (1992) it was indicated that out of 92 projects, only a handful was found to contain 'thoughtful' risk analysis showing 'good practice'. Further studies have indicated that

> "the most consequential problem regarding risk analysis in megaproject feasibility study and decision making [...] is the neglect of relevant downside probabilities in the calculation of project viability [...] Threshold levels need to be established for costs, revenues, environmental impact and viability, namely levels that, if crossed, redefine the project as a new project that must be appraised and approved anew" (Flyvbjerg et al., 2003:80).

It is not uncommon that the riskiness of megaprojects is attenuated. This is particularly evident in the case of major events, where the emotional bias surrounding these often blinds stakeholders and the public from appreciating fully their riskiness.

> "'What could be risky about an event? Events are fun! [...] This is a typical attitude encountered all the time [...] People do not see anything that could go wrong. But when explained to what could go wrong, the most common response is an awestruck 'I had no idea!' [...] Risk management is one of the most primary responsibilities of event organizers, yet so often ignored or misunderstood, particularly by inexperienced planners, because one cannot envision what one has not been exposed to - they do not know what they do not know" (Silvers, 2008:1).

Therefore, a main instrument for reducing the costs of project and event risk is to prepare a risk management plan as part of a feasibility study by fully identifying the scope for risk management, and to communicate that it is much wider than what is normally appreciated. In addition, "feasibility studies and risk analyses should be carried out together with considerations regarding the possible institutional, organizational and financial set-ups for the project. Especially so, as institutional change may be a prerequisite for risk reduction" (Flyvbjerg et al., 2003:85).

Finally, researchers identify a further reason for the 'megaproject performance paradox', namely that of a lack of learning and project/event post-auditing capability. "The reason for the lack of learning is that projects and their impacts are rarely audited ex post, and without post-auditing learning is impossible" (Flyvbjerg et al., 2003:49). It is suggested that megaproject and event developments require close scrutiny in the years to come after their completion, in order to investigate accurately what their economic and other impact truly is. Moreover, Flyvbjerg et al (2003:55-57) suggest that "it is remarkable how few studies have been carried out that compare predicted impacts with actual outcomes. [...] More comparative research is needed on predicted versus actual outcomes". Wood et al. (2000) concur with this view and support that with regards to impact assessments, monitoring and auditing, it is critical that an institutional framework is developed. "The objective should be [...]to define appropriate project goals and then set up the organization that can effectively adapt and audit the project to achieve the goals in an ongoing process from project design through construction to implementation" (Flyvbjerg et al., 2003:57-58). In fact, a few are those who advocate in favour of a set of legislations, standards and best practices that will help project and event professionals manage exposure to the possibility of loss, damages etc (Silvers, 2008; Flyvbjerg et al., 2003).

Given the focus of this research, namely ISS risk management practices within a major event context, the researcher continues by examining the objectives of event management, the associated processes, functions and challenges.

2.4.2. Project and event management

Major events: definition and literature

Events, namely the gathering of people at a specified time and place for a variety of purposes, include a broad range of genres[69]. Yet, it is the purpose of the event that will dictate the decisions about what will be included in the event and the definition of success for the event (Frame, 2003).

Although *'major events'* do not have an official and clear definition, certain universal characteristics can be identified. According to Hiller (2003) such an event is of short, fixed term and high-profile, with a significant impact primarily on the local but also global community. Debates about such events span from the pre-event to post-event usage of resources and impacts on the various stakeholders, while they are often promoted and considered as instruments of boosterist ideologies and economic growth.

Due to the legacy that a major event will create within a particular context - whether that is on an infrastructural, economic, resources/skills, or socio-cultural level- it involves considerable political decision-making with national or international governing bodies which get directly or indirectly involved.

Finally, a major event is commonly not an annual event, but one that is unique in nature, related to the specific location(s) and time that it is hosted. It is, thus, very particular to its context.

Therefore, similar to megaprojects, major events are great in scope, with a global impact and exposure, and set within an inter-disciplinary, diverse organizational, cultural and socioeconomic context. They require a significantly long process to prepare, a significant amount of resources, their operations need to be reliable and sustainable, and the associated costs and benefits are realized by a number of very diverse stakeholders.

Nonetheless, major events have certain characteristics different to those of other events and mega projects, which add to the importance of risk management (Hatton, 2000). Some of these include: large crowds; use of volunteers and inadequately trained staff; untried venues and sites; quick decisions and inadequate time, particularly as the event gets closer; complex and specialist activity; thrills and

[69] I.e. Silvers, 2008:8.

spills; a need for good community relations; untried communications; new event companies; and little 'continuing work' control over subcontractors and suppliers.

Three types of major events are identified, namely cultural (e.g. Expos), political (e.g. IMF/World Bank conferences), and sporting (e.g. Olympics) (COHRE, 2007). Such events are not merely experiences, but represent ambitious dreams, which involve awesome responsibilities, great expectations, benefits and risks. Major events cannot fail. There is too much at stake[70].

Thereby, as major events are increasingly frequent in a globalised world, one would expect that there must be a significant body of literature with regards to the successful preparation and delivery of major events. However literature is very limited, focusing only on three areas, namely the facilities and event management aspects[71]; the sociological, political and cultural aspects and impacts of a major event[72]; and to a lesser extent, the operational strategies of major events[73]. There is extremely limited research and reference to the telecommunications and IT infrastructure of major events, none of which truly considers this critical component of a major event both in its scope and context[74].

As for the Olympic context, which is under investigation in this study, research also remains limited focusing more on the high-level organizational structure behind such events, the marketing opportunities, and the socioeconomic impacts on the hosting city[75]. The technological aspects of such a major event, or any other such event for that matter, have been only briefly and superficially considered by journalists before each event. The technology that supports - in fact makes or breaks a major event - has only been treated as a news item, not a research one.

---

[70] I.e. Silvers, 2008; Hatton, 2000.

[71] Event literature on facilities and event management aspects covers topics of design and construction, marketing, crowd and audience management, physical security and safety, funding, and operations management (i.e. Westerbeek et al, 2005; Berlonghi, 1995; Stedman et al., 2001; Tarlow, 2002).

[72] I.e. Roche M, 2000; Horne and Manzenreiter, 2006.

[73] Literature on major event operational strategies cover topics of finance, ticketing, transport, venues, communications, equipment and personnel (i.e. Masterman, 2004 and 2009).

[74] I.e. Stavroulakis, 2002; Cheng, 2008.

[75] I.e. Theodoraki, 2007; Chappelet and Bayle, 2004; Masterman, 2009.

Therefore in conducting this research, in depth knowledge about the challenging preparation and successful delivery of major events can only be retrieved from a much wider body of research related to event management.

Event management - EMBOK

'Event management' is the process by which an event is planned, prepared, and produced. According to Silvers (2008), as event projects are becoming increasingly woven into the various aspects of our lives, the level of expected professionalism from event managers has increased significantly, while penalties for not meeting event expectations and requirements will increase in frequency and severity. However, there is no single source or organization collecting event data. In addition, the event industry is both horizontal and vertical. "It is unfortunate that the entire events industry has yet to come together, recognize its commonality and combined economic influence, and conduct the necessary research necessary to quantify the actual number of events and their true event spends" (Silvers, 2008:11). Event professionals and stakeholders urgently need better tools to ensure the safe and successful delivery of (major) events, including methodologies, best practices and an expanding body of ongoing and systematic research and literature.

Given the great similarities between project and event management, perhaps the most holistic approach to event management that indeed applies principles of project management, is that of EMBOK (Event Management Body of Knowledge)[76].

EMBOK takes a process view of event management (i.e. Fig.2.3), supporting a sequential and iterative system that promotes a dynamic approach to the changing nature of events and the risks that emerge. The stages to this process are defined below in Table 2.1.

[76] I.e. Silvers, 2003, 2008; Silvers et al, 2006.

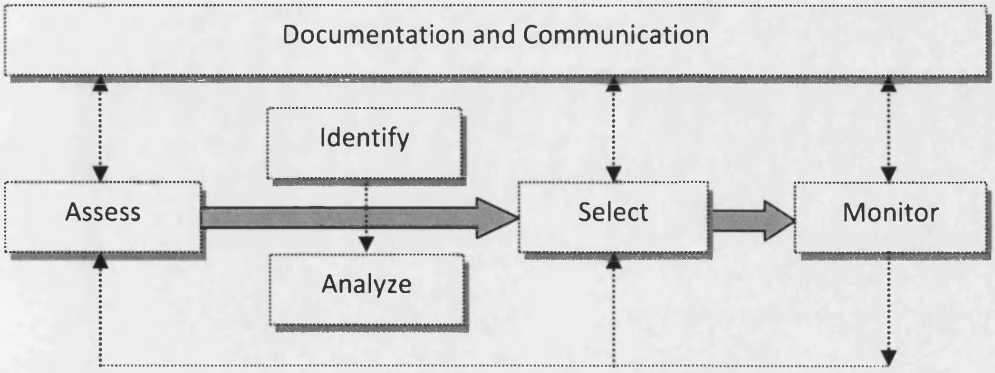


Figure 2.3: *The process system of the EMBOK model* (Source: Silvers, 2008:12).

Table 2.1: Stages and definitions to the EMBOK event management process

EMBOK Event Management Process Stages		Definition
1	*Assessment*	A two-step process of 'identification' and then 'analysis'.
2	*Selection*	The stage where the methods/tactics that will achieve the goal and objectives are chosen.
3	*Monitoring*	A process where the progress of the selected tactics is tracked, including the performance of risk control actions. The assessment and selection processes are reiterated as needed.
4	*Documentation*	The recording, reporting, maintaining and archiving of project records and documentation, thus providing valuable data and evidence which lead to a robust management process.
5	*Communication*	The timely information acquisition and distribution, plus the appropriate consultation in decision making.

In addition, similar to any other project, event management has five phases (i.e. Fig. 2.4), namely initiation, planning, implementation, the event, and closure (i.e. PMI, 2000).

> These "phases are sequential, highlighting the criticality of *time* in any event project as it gathers momentum toward the event itself. The progression is also cyclical, with the results of the evaluation phase contributing to the research phase of the next event. [...] Effective event management relies on engagement at each juncture of this continuum throughout the life of the event project" (Silvers, 2008:13-14).

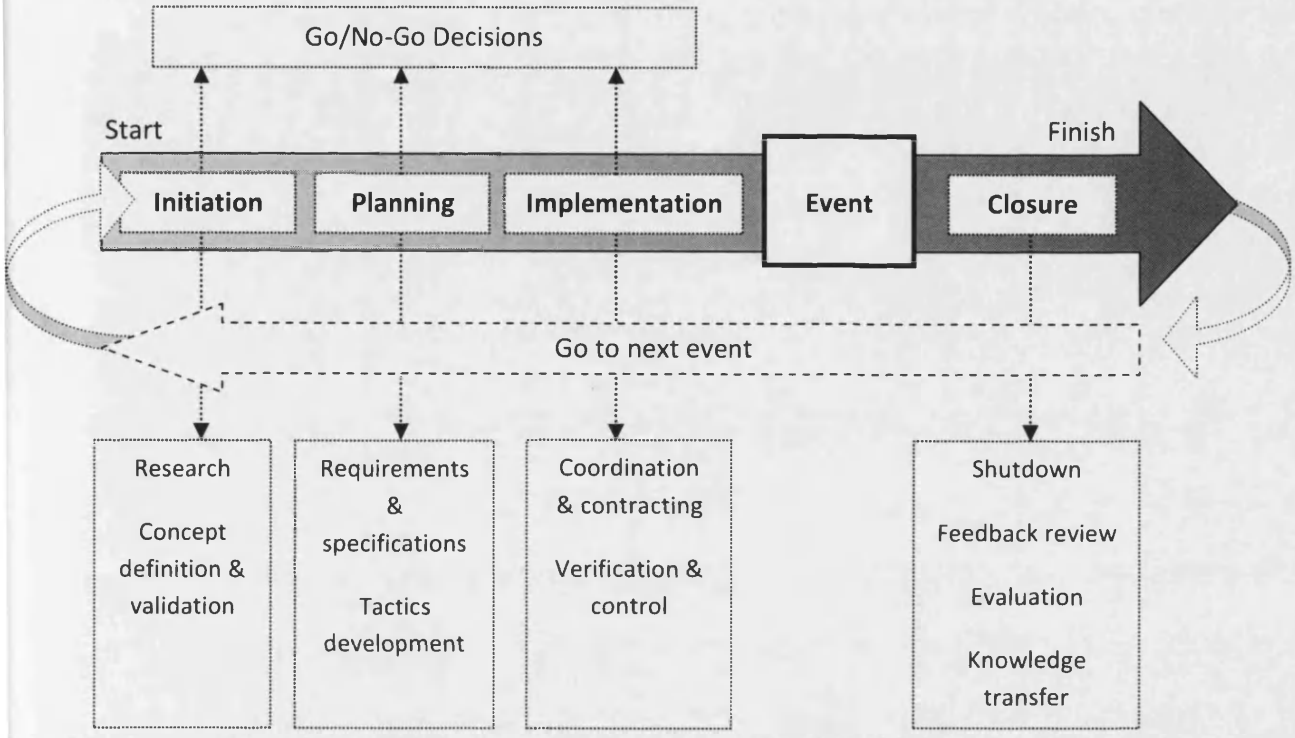


Figure 2.4: *The five stages of a project and/or event* (Source: adapted from Silvers, 2008:13).

Perhaps, however, the most important aspect of EMBOK is that it recognizes the importance of risk management throughout the above event management process and stages, and it includes 'risk' as a domain equal to other typical domains of event management (i.e. Table 2.2). The proponents of the EMBOK model stress that it is "of prime importance to illustrate the full scope of the responsibilities and therefore risk management obligations, assigned to event organizers" (Silvers, 2008:12).

EMBOK identifies five functional domains to event management, each of which has specific characteristics and is affected by and subject to different objectives, procedures, constraints, and standards during the different phases and processes. These are summarized in Table 2.2 below.

Table 2.2: *EMBOK functional domains of event management* (adapted from Silvers, 2003).

	Event Management Knowledge Domains				
Functional Units	**Administration**	**Design**	**Marketing**	**Operations**	**Risk**
	Financial	Content	Marketing Plan	Attendees	Compliance
	Human resources	Theme	Materials	Communications	Decisions
	Information	Program	Merchandise	Infrastructure	Emergency
	Procurement	Environment	Promotion	Logistics	Health & Safety
	Stakeholders	Production	Public Relations	Participants	Insurance
	Systems	Entertainment	Sales	Site	Legal
	Time	Catering	Sponsorship	Technical	Security

The 'classes' of each domain - which can vary in priority from one event to the next - can be further subdivided into 'elements'. For example, the human resources class can be subdivided into volunteers, motivation, and leadership.

The purpose and value of such a taxonomy is to indicate the multiple event management areas, all of which have a varying significance in the successful preparation and delivery of an event. Each domain will require a diverse set of skills and resources and will have to deal with a set of associated challenges, resource constraints and risks.

In addition, the above taxonomy can be useful in conducting ongoing analyses with regards to the functions of each domain (a) across the various event project stages (i.e. Fig. 2.4) and (b) for each event management process phase (i.e. Fig.2.3). Such analyses can help identify objectives, tactics, required resources, constraints and interdependencies, hence improving event risk understanding, mapping and management.

According to the EMBOK proponents[77] this model can be valuable in several ways. Firstly, it can illustrate the complexity of the profession while providing conceptual clarity and reducing the likelihood of overlooking or discounting factors that may have a significant impact on the ability to manage risks associated with an event project. Furthermore, the EMBOK framework stresses that the risk management

[77] I.e. Silvers, 2003, 2008; Silvers et al, 2006.

process is a sequential and cyclical one, as well as an iterative one, since each and every aspect of an event has an impact on the whole event. Therefore, it serves as the strategic framework for consistent and comprehensive risk management for events. Finally, the EMBOK framework will facilitate effective competency and conformity assessments, as well as knowledge transfer systems.

2.4.3. Risk management and communications in projects and events

Event management literature does not cover specifically the area under investigation in this study, namely the ISS or ISS risk management practices within a (major) event context.

However, it is understood that from the 35 event functions identified in Table 2.2, there are several that directly or indirectly relate to ISS risk management practices, whether by defining the scope and/or context of such a function.

In addition, as indicated above, event management literature has considered the topic of risk management, its function and challenges.

Risk management at event projects

Starting with the issues directly related to risk management in event projects, it is important to understand the definition of 'risk' within the event management discipline.

> "'Risk' is any condition or occurrence that might affect the outcome of an event or event activity and might expose an event organization to loss measured in terms of probability and consequences. [...] An event itself is a speculative risk[78]; its production incurs liabilities yet has the potential for economic, political, and/or social rewards. One needs to look at the worst that can happen and the best that can happen in order to be prepared for anything in between" (Silvers, 2008:4).

Therefore, the definition of risk in events identifies that there is both an objective and more uncertain and ambiguous dimension to the perception of risk, stressing the

[78] A 'speculative risk' is one where there is both a possibility of loss and a possibility of gain. This contrasts to the definition of an 'absolute risk' where there is only the possibility of loss (i.e. Silvers, 2008:4).

need for preparedness, stakeholder involvement and context understanding (Berlonghi, 1990).

Understanding the dimensions of risk at events will have to identify (a) what is at risk, and (b) what are the risks.

> "The relative severity of the risks will be different in different contexts and different event genres. [...] Inexperience, lack of expertise, and insufficient planning and resources have a significant impact on the level of risk associated with an event. This expands exponentially as the size and scope of the event increase" (Silvers, 2008:5-7).

Hence, the objectives of risk management in an event include the protection of event assets, the minimization of legal and financial liabilities, the control of potential loss, the proper management of growth, and the responsible and reliable operations. Risk management includes legal, ethical, and operational responsibilities, while the role of risk management is to prevent and reduce loss by "making events as safe and secure as possible" (Berlonghi, 1990:4).

Risk management in an event is a process (i.e. Fig.2.5) that must be ongoing and dynamic

> "because the risks surrounding the meetings and events are constantly emerging, growing, subsiding, changing, and fluctuating in terms of urgency and priority. The risk management process must also be proactive and cyclical, facilitating communication, forecasting, and forward planning" (Silvers, 2008:25).

Furthermore, Silvers (2008:33) stresses that aside from the activities of the event risk management process, event personnel and risk managers must appreciate that one does not 'control' what can or will happen at an event.

> "Event management, and consequently risk management, encompasses the initial and iterative planning and then it is all about *change management*. And there are always changes or incidents occurring at an event. [...] You have no control over changes happening, only your ability to react effectively to those changes. *You must be proactive about the ability to be reactive*".

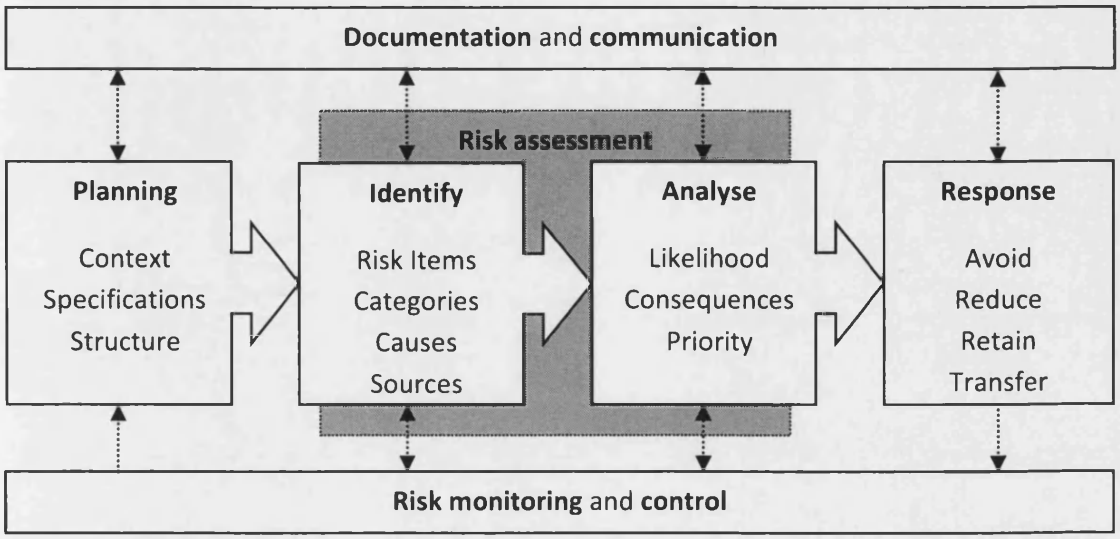


Figure 2.5: *The risk management process* (Source: Silvers, 2008:25).

The effectiveness of change management relies upon the availability and quality/type of information, familiarity, good judgement, and being prepared, not paralysed. Gladwell (2005) suggests that in the throes of an event the efficacy of change and risk management decisions is determined by the depth and breadth of our experience and knowledge.

Control in events is about incorporating preventative measures and then focusing on *preparedness*. "The more you are aware of what could go wrong, the better prepared you can be to react and respond properly and effectively to an incident of occurrence" (Silvers, 2008:33).

In addition, Smith and Merritt (2002) suggest that effective *risk communication* should facilitate collaboration and the acquisition of proactive data that will help predict and prepare for risks, and getting risk messages before, not after, something has happened. They argue that communication procedures and methods should be embedded throughout the event project, to ensure the right information gets to and is received from the right people at the right time. Similarly, the risk manager needs to involve stakeholders from an early stage of the event project and support the creation of a teamwork environment that will become even more important as the event project goes into production.

Integrating risk management with administrative event management activities

From the above it is made clear that risk management needs to be integrated into the event project lifecycle and techniques as early as possible, consisting a key part of all administrative activities and the event's organizational structure.

> "An event is a project, and the administrative functions such as time management, financial management, human resources management, procurement management, and the systems used to implement and integrate them, are typically included within the discipline of project management. The tools, techniques, terminology, processes, and procedures used by the project managers in many other industries serve the event organization equally well, particularly in the pursuit of effective administrative practices and risk management. [...] The integration of risk management throughout the organizational structure and project planning helps manage the scope of an event and its exposure to risk" (Silvers, 2008:157-158).

The scope and context of the administrative functions of an event project will also determine the nature and severity of associated risks. The challenges and risks of the administrative safeguards of an event are considered in more detail below.

Time management: Every event project has a limited time dimension into which all the tasks required to produce it must be scheduled. Being a limited and finite resource, time restrictions will determine the *tempo* of the event management processes, as well as define certain critical milestones and areas of risk[79]. Event and production schedules may be seen as *time maps* showing the scope and intensity of activity required in order to achieve objectives throughout the life-cycle of the event project (e.g. Fig.2.6).

Time management starts with the early stages of event project and activities scope definition, while Silvers (2008) suggests that when creating timelines it is vital to identify the various related activity-stakeholders, and to seek input especially from those responsible for delivering the various tasks. Event activities and tasks need to be identified in as much detail as possible, along with the associated dependencies and milestones. All these elements of a time plan need to be closely monitored, since milestones and deadlines often become the triggers and thresholds for risk

[79] I.e. Silvers, 2008:158 and Kendrick (2003) .

response actions. Therefore, it is understood that time management is closely related to activity and task management.

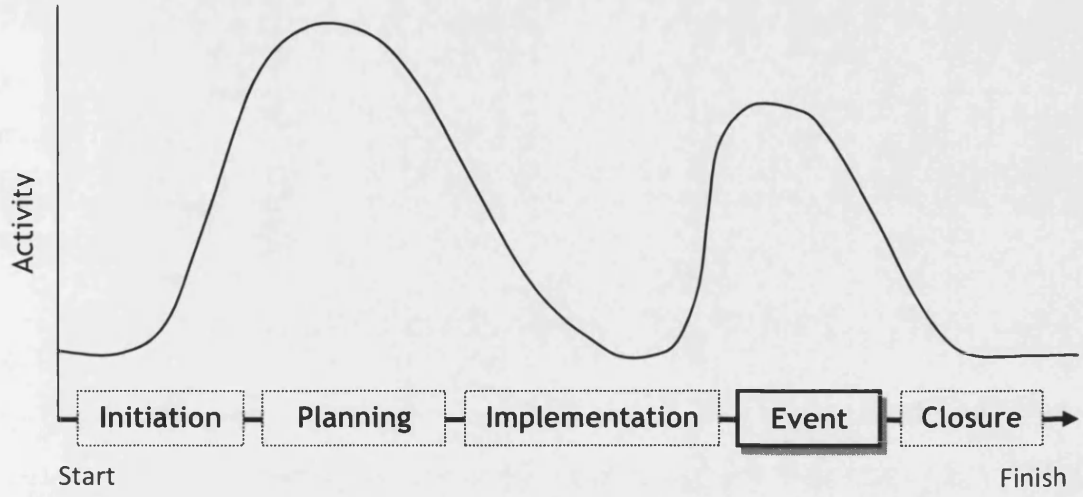


Figure 2.6: *Activity dimension of the event timeline* (Source: Silvers, 2008:159).

In addition, time management is also related to resource management.

> "Time is linear an irreplaceable; the only way to expand time is to compensate by adding other resources, in other words, do more, be more productive within the time given. However, as Lewis (1997) points out, effective resource allocation is contingent upon the skill levels, capabilities, capacities, and outputs of the particular people and suppliers" (Silvers, 2008:160).

Kendrick (2003) further suggests that estimating the time it will take to complete tasks can be a significant challenge, since such kind of planning if often prone to optimism, over-confidence, lack of information, and scope creep. Yates (2003) calls this the 'planning fallacy'.

Financial management: Similar to other event resources, the budget needs to be planned and integrated into the project timeline. It needs to be monitored closely to ensure decisions minimize financial risk, maximize opportunities, and maintain the integrity of the event.

However, and perhaps more importantly, in a time-finite event project costs increase the closer one gets to the event[80], and last-minute changes can be expensive because there is little time or suppliers impetus for price negotiations. Therefore, spending upfront can prevent having to spend even more money at the back end.

As for risk management expenditure, Silvers (2008: 165) points that "risk management activities are often viewed as an expense that can be reduced when budgets must be cut because they seemingly do not directly contribute to the event content, environment, or experience".

Human resources management: Human resource management is viewed by many researchers and professionals as the most critical, as well as the most problematic.

> "It is the most critical because it is the people who convert the other factors into 'real' resources. [...] From a manager's perspective, all the other kinds of resources become valuable only if the people in the organization use them effectively. [...] However, despite the critical importance of human resources, the recognition of and importance attached to it are much lower that one would expect" (Chelladurai and Madella, 2006: ix).

Similarly, the human resource risks in an event are commonly overlooked[81].

Human resource management encompasses the formulation of the appropriate organizational structure, policies, and procedures for the recruitment, orientation, motivation, training, compensation, supervision, and discipline of employees, contracted workers, and volunteers.

Effective human resource management is key to building the organizational structure and culture that will serve the needs of both the event enterprise and the people within it. Getz (1997), however, warns that organizations that are less bureaucratic and formal and instead have a team-oriented structure - frequently the case of event organizations - although they may benefit from a certain level of camaraderie and efficiency, they can also subvert policy and control processes. This can be further aggravated by the often small and insular community of event workforce, leading to

[80] I.e. Bowdin et al, 2006.

[81] For more information on common event human resources management risks see Silvers (2008:167).

cases of conflict and dispute which need to be timely and impartially managed, without disrupting the event operations.

A further important issue in event human resource management involves knowing who is hired and for what position. Hiring and induction may include background, criminal and credit checks for certain positions, in order not to compromise overall levels of competence, safety and security. According to Berlonghi (1990) walk-up and last-minute volunteers should not be allowed.

Finally, inexperience is cited as one of the biggest risks in events management. This can be overcome by training, mentoring and practice within the event context, that will eventually lead to experience[82].

Procurement management: According to Monks (1996) good procurement management will facilitate risk management by determining the risks associated with the individual vendors or suppliers and the business interaction with them. Third parties need to be carefully selected and contracted, possibly with the help of product specialists, the product users, and those administering the contracts and payment functions.

It is vital that the procuring organization has properly determined the need and scope of contracted goods and services. Meanwhile it also needs to understand which of the goods and services are critical to the event, in order to ensure quality control and that contingency plans are in place[83].

Systems management: Finally, and more pertinent to this research, event management literature identifies 'systems management' as one of the key administrative safeguards to event risks. Under the event management perspective, systems management involves the implementation and coordination of the various event systems using suitable technology to integrate the needs of the event project and enterprise.

According to Silvers (2003, 2008) in order for event systems to meet their administrative and operational efficiency and effectiveness potential, users must be able to recognize the impact of their actions (or inactions) on those systems. Event

[82] I.e. Chelladurai and Madella, 2006; Silvers, 2008; Berlonghi, 1990.

[83] For more information on common event procurement risks see Silvers (2008:174).

organizations need to embrace that event systems need to be continually improved in order to achieve increasing safety, security and sustainability. Weaknesses in the implementation of a system are a risk, and steps must be taken to either improve training in the use of the system or improve the system itself.

One of the critical areas in which development of a system will facilitate effective event risk management is decision making. A system will provide its users with the tools and information to make a good decision at the right time - this is particularly important in times of crisis. However, event management literature also identifies that decision-making systems need to exist within a greater policies and procedures framework, which defines roles and responsibilities, chain of command, and allows users to share their experience and expertise with the right authority. The implemented systems need to reflect this greater organizational structure and mission, and must be incorporated into a greater security system that includes the physical, behavioural and procedural loss prevention tactics (Silvers, 2008).

In addition to managing the administrative safeguards of an event, the event risk professionals need to be involved as early as possible with a number of other operational, risk and marketing event activities, and monitor the performance of associated risk controls. Some of these functional areas include: event loss prevention and security[84], preparedness and emergency management[85], communications management, including also information and stakeholder management[86], marketing and public relations management[87], and site security and attendee access management[88].

[84] I.e. Silvers, 2008; Berlonghi, 1990; Broder, 2000; Smith and Merritt, 2002.

[85] I.e. Silvers, 2008; Crown, 2005; Regester and Larkin, 2008; Au et al., 1993.

[86] I.e. Silvers, 2003 and 2008; Silvers et al., 2006; Alexander, 2002; Kennedy, 2006; Berlonghi, 1996; Chelladurai and Madella, 2006; O'Toole, 2006.

[87] I.e. Silvers, 2008; Kotler et al, 1996; Regester and Larkin, 2008; Glaesser, 2006.

[88] I.e. Silvers, 2008; Garber, 2004.

2.5 Conclusion: moving towards a cross-disciplinary research

The literature review for the purposes of this study was a process carried out throughout the various research phases. It informed the study's focus with regards to the research problem (i.e. Chapters 2 and 3); its directions with regards to the underlying theoretical and methodological assumptions (i.e. Chapters 3 and 4); and the insights and conclusions with regards to its findings (i.e. Chapters 4 and 5).

The research initiated with an interest in organizational ISS management practices in environments with great levels of operational uncertainty, as well as great demands for operational reliability and information integrity. Hence, the research initiated and continued with a parallel investigation of two themes: (a) the practices of ISS management and (b) organizational theories examining issues of operational reliability, organizational uncertainty, as well as the management of hazards and accidents.

With regards to ISS management practices, the literature presented above indicated the emergence of a more recent discipline within ISS - that of risk management, primarily in order for ISS practitioners to improve the prioritization and justification of ISS management decisions and controls. However, research also demonstrated a lack of maturity of this field.

The parallel investigation of themes related to organizational risk/hazard management and operational reliability, indicated a greater risk field to the one explored in ISS, suggesting the benefits of a cross-disciplinary research.

The study of the approaches to risk and the organizational theories that focus on managing this and delivering operational reliability pointed to a number of critical parameters to the individual and organizational experience of risk.

Firstly, the risk literature review verified the increasingly appreciated significance of the human dimension/behaviour with regards to experiencing and encountering risk. Despite the real - i.e. physical impact - dimension of risk, it has been demonstrated that risk is also greatly subjective in terms of its perception, and hence associated communication focus. Therefore, issues of human psychology, cultural and organizational context have been underlined.

In addition, the need for more communicative, participatory and inclusive approaches to dealing with risk has been highlighted[89]. Moreover, as the multi-

[89] I.e. Renn, 2008; Morgan et al, 1992; Breakwell, 2007.

dimensional nature of risk has been put forward, the need for holistic and integrative theoretical and methodological frameworks has been proposed[90].

Finally, the above literature review has indicated the dynamic and changing nature of risk, which implies the need for an *ongoing, repetitive risk management process*, which supports learning and gradual optimization in order to deal not only with the complex and uncertain, but also the ambiguous and unexpected[91].

Further to the review of literature in the fields of ISS and risk/hazard management, an investigation was conducted into the characteristics and risk management challenges of the organizational environment under study, namely that of a major event organization. Such environments demonstrate high operational uncertainty as well as high demands for operational reliability. In fact, the literature review revealed that this was not only an organizational context inadequately explored - especially so in terms of IS and ISS management practices - but also one that demonstrated poor past performance and an increasing demand for investigation and performance improvement.

The research focus was thus made concrete. If the organizational management of risk and the delivery of operational reliability are as complex as implied by the extensive associated literature, then what are the risk management practices and challenges faced by a major-event organization - which is inherently risky and with high stakes - in relation to ISS?

The literature review not only provided a greater focus to this research, but also pointed to the directions taken and assumptions made in order to answer the research question. These will be further explored in Chapter 3 of this study. In summary, however, the literature review established that in order to answer the research question, a cross-disciplinary approach was required. This should aim to *understand* in depth[92] major event organizations, their scope, context, and the ways in which ISS risks are perceived, managed and communicated in order to deliver highly reliable operations. The multiple dimensions and dynamic nature of an organization's risk experience were appreciated and incorporated into the study's explorative framework of analysis.

---

[90] I.e. Klinke and Renn, 2004, 2006.

[91] I.e. Vaughan, 2005; Cooke and Rohleder, 2006; Hutter and Power, 2005b.

[92] Hence opting for an interpretive case-study approach.

3. Research Methodology and Conceptual Framework

3.1 Introduction

The previous chapter of this study reviewed the various schools of thought across three disciplines - namely Information Systems Security (ISS), risk and hazard management, and event (risk) management - and identified the potential benefits of a cross-disciplinary research, with the 'notion' of risk as the common denominator.

The above literature review indicated an overall orientation across the three disciplines towards the 'softer', human/behavioural aspects of the risk experience, underlining the significance of parameters such as the organizational/structural, technological and cultural context, the criticality of communications and inclusive, integrative frameworks of risk analysis.

It was noted earlier that with the growing appreciation of the multiple and dynamic dimensions to risk involved in the management of ISS, reliable organizational operations, and event management, there has been a recognition of the need to *understand* practices and challenges across the three disciplines, while investigating the associated processes of change.

The researcher agrees with a number of scholars across the three disciplines[93], who have stressed that with regards to perceiving, managing and communicating risk there is a need to investigate human and social reality within its particular contextual/organizational settings. Therefore, this research is supporting the identified need to increase the use of *interpretive* approaches for the analysis of organizational risk experiences, with a particular focus on the implications of context.

Yet, such a research orientation implies a number of underlying ontological and epistemological assumptions with regards to the topic of risk, as well as having implications on the research framework of analysis and methodology.

The purpose of this chapter is to consider the assumptions underlying the research's theoretical perspective, as well as examine any conceptual and methodological implications. This chapter is, thus, organized into the following sections. Section 3.2 focuses on the ontological and epistemological beliefs shaping this research, as well

[93] E.g. Pattinson and Anderson, 2005, 2006a, 2007; Dhillon, 2007; Renn, 2008; Berlonghi, 1990; Silvers, 2008.

as the implications associated with the study's theoretical perspective and methodology. Section 3.3 continues with a presentation of the research argument, the conceptual framework for conducting the argument, and the associated methodology. The research design is covered in Section 3.4, while Section 3.5 draws out the conclusions and contributions of this chapter.

3.2 Research assumptions and implications

3.2.1. Ontological and epistemological assumptions

The conceptual framework that informs the research across its various stages, as well as the methodology used for collecting and making sense of research data, is based upon fundamental assumptions with regards to the research's ontology, epistemology and human nature. Burrell and Morgan (1979:3) have summarised this as indicated in Figure 3.1 below.

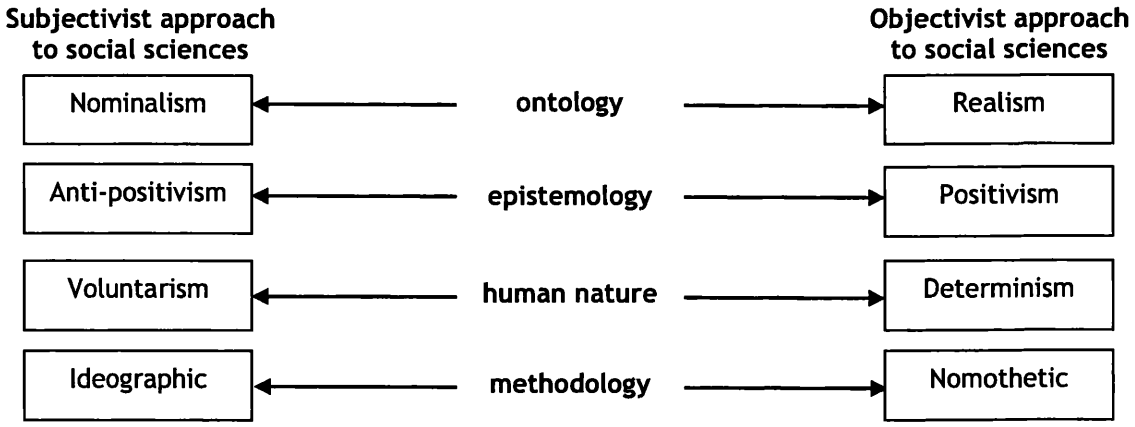


Figure 3.1: *Scheme for analysing assumptions about the nature of social sciences* (Source: adapted from Burrell and Morgan, 1979:3).

As Crotty (2003:10) suggests "ontological and epistemological issues tend to emerge together". The two sit alongside each other and inform the theoretical perspective (i.e.Fig.3.2), "for each theoretical perspective embodies a certain way of understanding what is (ontology) as well as a certain way of understanding what it means to know (epistemology)".

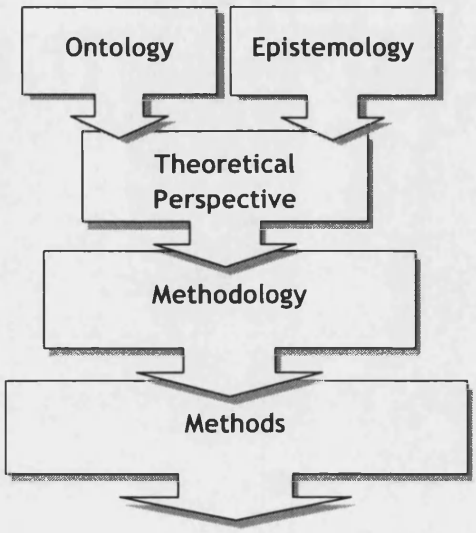


Figure 3.2: *The five elements that inform a research and its approach* (Source: adapted from Crotty, 2003:4).

Given that the central concept under investigation is that of 'risk', and the research focuses on the risk meanings/perceptions, behaviours and controls associated with delivering reliable ISS operations, the researcher considers necessary to examine the ontology and epistemology of 'risk'. This is key to the definition of the research's underlying assumptions and frameworks of analysis. The risk ontology and epistemology will define the scope of this risk investigation.

The scope of risk investigation - the ontology and epistemology of 'risk'

Supporting the approach adopted by a number of risk scholars[94], this study suggests that

> "risk is in part an objective threat of harm to people and in part a product of culture and social experience. Hence, hazardous events are 'real': they involve transformations of the physical environment or human health as a result of continuous or sudden releases of energy, matter, or information or involve perturbations in social and value structures" (Kasperson, 1992:154).

'Risk' involves a "situation or an event where something of human value is at stake and where the outcome is uncertain" (Rosa, 2003:56). This definition comprises of three elements: (a) risk expresses some state of reality of human concern or interest;

[94] E.g. Renn, 2008; Rosa, 1998, 2003; Kasperson, 1992.

(b) some outcome is possible; and (c) it seems impossible to talk of risk in the absence of the notion of uncertainty.

Therefore, the proper scope of risk investigation is where there is a conjunction of uncertainty and human stakes (i.e. Fig.3.3).

Human stakes	Uncertainty: YES	Uncertainty: NO
NO	**Indeterminacy** (quantum mechanics) 4	**Determinism** (celestial mechanics) 1
YES	3 **Risk** (decision science)	2 Fate (myth)

Figure 3.3: *Risk defining dimensions* (Source: Rosa, 2003:58).

By defining risk as an as an objective state of the world, the logical consequence is that

> "risk exists independent of our perceptions and our knowledge claims, subjective judgements, about what is at risk and how likely a risk will be realized. Furthermore, placing risk into an ontological category leaves open the question of our knowability of given risks: the question of the epistemology of risk. [...] It neither inherently defines away, nor contradicts, the variety of paradigms in the risk field [...] In effect it defines paradigmatic debates over risk as an issue in epistemology" (Rosa, 2003:60-61).

Therefore, the concept of 'risk' adopted is a synthetic one. As Rosa (2003:50) suggests it is misleading to view risk through the lens of either domain separately. The view of risk comprises both an ontological and an epistemological domain. "As an objective threat or harm to people, risk enjoys an *ontological realism*. As an element of the world subject to interpretation, filtered by social and cultural factors, risk enjoys an epistemological liability".

This position taken by Rosa (2003) is not, however, one of phenomenology and strong constructivism[95], but one of *hierarchical epistemology*, which does not deny the fallibility of all knowledge claims, but denies that all knowledge claims are equally fallible. Hence, Rosa's logic makes the ontology and epistemology of risk logically independent, but complements of one another. He has, thus, given this combination of ontological realism and hierarchical epistemology the acronym HERO (Hierarchical Epistemology and Realist Ontology). HERO admits to differences in the types, the quality, and the aptness of our knowledge.

Therefore, while the ontological approach to the study of risk is one of realism, the epistemological assumptions present characteristics of 'hierarchical constructivism', where meaning is indeed constructed out of something (the object), yet not all knowledge claims are of equal validity.

> "Indeed, if all knowledge claims were equally fallible (or equally valid), we all would be living behind a veil of ignorance where there would be no knowledge at all. Instead, [...] knowledge claims, while always short of absolute truth, admit to degrees of approximation to what is true" (Rosa, 2003:63).

Hence, coming back to Burrell and Morgan's (1979) scheme for analysing assumptions about the nature of social sciences, the ontology of this study is one of realism. With regards to epistemology, on the other hand, the research leans towards an anti-positivist stance, proposing an orientation of constructivism - hierarchical constructivism.

At this point it is worth stressing further that a realist ontology does not contradict an epistemology of (hierarchical) constructivism. Realism has been often identified with objectivism, yet this position has been widely criticised[96]. As Crotty (2003:11) suggests, "the existence of a world without a mind is conceivable. Meaning without a mind is not. Realism in ontology and constructionism (or constructivism) in epistemology turn out to be quite compatible".

Therefore, the above assumptions and the reviewed literature both point towards the need to *understand* risk experience across various levels of analysis. The meanings assigned to risks by various actors require an *in-depth* empirical investigation, which

[95] Such an approach would assume that all claims to knowledge about worlds are relative, and therefore one claim is generally as good as any other.

[96] I.e. Guba and Lincoln, 1994; Merleau-Ponty, 1962; Heidegger, 1962; Crotty, 2003.

does not necessarily aim to predict, but rather to describe and explain. Such an approach is particularly relevant in the case of subject matters such as the one under investigation, that still have a lot of maturing to do.

The above philosophical orientations have implications for the theoretical and methodological perspectives adopted in this study. These will be considered in the section below.

3.2.2. Implications on the study's theoretical perspective and methodology

As suggested by Crotty's (2003:4) model depicted in Figure 3.2, a researcher's ontology and epistemology inform the choice of theoretical perspective and methodology. The theoretical perspective is defined as "the philosophical stance informing the methodology and thus providing a context for the process and grounding its logic and criteria", while the research methodology refers to "the strategy, plan of action, process or design lying behind the choice and use of particular methods and linking the choice and use of methods to the desired outcomes" (Crotty, 2003:3).

According to Burrell and Morgan (1979) the above two elements of any research are also determined by assumptions with regards to human nature. This can be either deterministic, where people and their activities are regarded as completely determined by their situation, or voluntarist, where people are considered to be completely autonomous and free-willed. This research is inclined to neither of these two extremes, but rather regards human activities as a consequence of a complex interplay of situational and voluntary factors.

The above 'risk' definition and the research focus on organizational encounters with ISS risk in an environment of great uncertainty and high stakes, point towards the need for an in-depth understanding of the dynamic and ongoing processes involved in identifying and making sense of ISS risks, and organizing for reliable operations.

This research primarily aims to describe and explain the identified organizational risk experience. The identification of patterns of behaviour and organization that provide some predictive value for future cases is a secondary objective.

Therefore, the theoretical perspective of this research is one of *interpretivism*, "looking for culturally derived and historically situated interpretations of the social life-world" (Crotty, 2003:67). As for the associated methodology, this has a primarily

ideographic focus. The research does not aim to test hypothesis (i.e. nomothetic approach), but to understand the underlying causes and the related patterns of behaviour leading to the reliable, or not, ISS operations.

More specifically, the definition of 'interpretivism' to which this research is aligned is the one offered by Weber (1962; 1968). He suggests that social sciences are concerned with *Verstehen* (i.e. understanding) and there is a need to focus social inquiry on the meanings and values of acting persons in order to arrive at a causal explanation of the course and effects of social action. Therefore, Weber (1962) aims to explain as well as understand. As Weiss (1986:68) suggests, "Verstehen is for the purposes of explanation". To achieve this, however, "Verstehen has to be substantiated by empirical evidence" (Crotty, 2003:69).

According to Weber (1949: 90-94), the amassing of such empirical data can be done with a heuristic device that will operate as the principal diagnostic tool. Such a 'tool' is a conceptual or mental construct that guides the social inquirer in addressing real-life cases and discerns where and to what extent the real deviates from the ideal.

What we understand today as the Verstehen or interpretivist approach to human inquiry has appeared historically in many guises, such as hermeneutics, phenomenology, and symbolic interactionism. The theoretical orientation of this study falls in line with symbolic interactionism that stems from the pragmatist thinking of social psychologist George Herbert Mead (1934). According to Blumer (1969:2), a student of Mead, interactionism makes the following assumptions:

- 'that human beings act toward things on the basis of the meanings that these things have for them';
- 'that the meaning of such things is derived from, and arises out of, the social interaction that one has with one's fellows';
- 'that these meanings are handled in, and modified through, an interpretive process used by the person in dealing with the things he encounters'.

The methodological implication of this approach is that it "directs the investigator to take, to the best of his ability, the standpoint of those studied" (Denzin, 1978:99). This role taking is an *interaction*, while it is *symbolic* for it is possible only because of the symbols that humans share and through which they communicate.

Across the various schemes of symbolic interactionism[97], the one that describes best the approach of this study, is that of *negotiated order theory*. Negotiated order theory - explored primarily by Strauss (1978, 1982) - disputes that social settings are definitively structured and social actors have very clear-cut roles. Instead, societal arrangements and procedures are considered to be constantly reworked by those who live and work within them. There is an ongoing, albeit often tacit, process of negotiation and adjustment of action.

Meaning in this theory is dynamically (re)created and (re)negotiated, and therefore depends on the context of the communicative acts (Flower, 1994; Clausen, 2007). Thus, communication is an ever-evolving process of the co-creation of meaning (Yoshikawa, 1987) that allows for ambiguity and paradox in intercultural encounters (Fang, 2003).

Furthermore, Strauss (1978) suggested that negotiations have temporal limits, and they are renewed, revised, and reconstituted over time. In addition, he argued that structural changes in an organization require a revision of the negotiated order. As Gerson (1976) has noted, individuals and society continually generate each other through a process of negotiation, while "real constraints direct and channel the actions of individuals and organizations" (Fine, 1984:24).

At this point, it should be also noted that proponents of the negotiated order perspective can examine either negotiations that occur among individuals or those in which negotiators represent larger social units such as organizations or organizational segments[98]. However, "negotiated order theorists reject the naïve radical phenomenological position that all negotiations are feasible. Some actors have more power and greater control than others" (Fine, 1984: 251). Therefore, a number of scholars[99] suggest that because of the importance of the negotiation setting, any system that does not look at the *context* and suggests means of controlling it will be unacceptable to interactionists. This view has a number of methodological and theoretical implications.

With regards to the methodological implications, a careful consideration of the structural and negotiation contexts leans towards the application of *qualitative* approaches to aid in the implementation and utilization of research findings.

---

[97] I.e. Crotty, 2003.

[98] I.e. Maines, 1977.

[99] I.e. Beyer and Trice, 1982; Fine, 1984; Currie, 1999.

Therefore, the metaphor of organizational negotiated order is most useful as a sensitizing concept of *understanding* a social scene, rather than as a device for hypothesis generation.

As for further theoretical implications, the theory of negotiated order stresses some key concepts in 'organizing'. These are the concepts of meaning, interaction/ communication, change and context, as well as the interplay between these factors to organizing. Currie (1999) suggests that in organizational environments of a negotiated order, dynamic processes of sense-making and change can be managed only through a sensitivity to and appreciation of context. Thus, the key concepts of negotiated order have also greatly influenced *dynamic* interpretive approaches such as this of 'contextualism' by Pettigrew (1985), which focuses his analysis on the context, process and content of organizing and organizational change. Pettigrew regards problem-solving and decision-making processes as containing elements of 'muddling through' and views organizations as systems of political action.

However, Pettigrew's (1985) contextualist approach has a number of drawbacks[100] . Despite the fact that Pettigrew claims that connections between the outer and other contextual levels of an organization are a vital element to his approach, inadequate emphasis is put on these. In addition, although Pettigrew emphasizes the utility of understanding the socio-political elements of the context, his approach falls short of providing a means of identifying the various interest groups which wield power.

In the field of IS research, Walsham (1993) has attempted to address several of these problems with regards to the contextualist approach, and has suggested the additional utilization of approaches to study the context and the process of change. He, thus, proposes the use of a sociological model to conceptualize the linkage between context and process in social systems.

Given this research's focus on understanding the organizational processes of change that establish reliable ISS operations in a major event context, the researcher leans towards Walsham's approach to contextualism, where a model of context and process are introduced, as well as a model to link the two.

Therefore, this study adopts a contextualist analysis perspective, which identifies vertical and horizontal levels of analysis and the interconnections between those

[100] I.e. Dhillon, 1995:51-52.

levels through time[101]. As Walsham (1993) suggests, the concept of 'context' is a static one and needs to be repeatedly considered to review the type, extent and reasons for change. Therefore, it is critical to consider the evolution of context over time, as well as its links to the process under study.

For the purposes of analysing the organizational context of change across various levels, the approach used is a scheme offered by Mintzberg (1979, 1981) that can provide a rich description of the organizational structural context and situational factors. As summarised in Table 3.1, Mintzberg's scheme considers the basic parts of the organization, the processes of activity coordination, the parameters used to design their structures, and the contingency or situational factors.

Table 3.1: *Mintzberg's scheme of organizational context levels* (Source: adapted from Theodoraki, 2007:23-25).

Contextual Elements		**Parameters**
Parts of the Organization		1. The *Operating Core*: where the operators (i.e. those who perform the basic work of producing products or rendering services) are found. 2. The *Strategic Apex of Managers*: those who oversee the systems operation. 3. The *Techno-structure of Analysts or Technical Staff*. 4. The *Support Staff*. 5. The *Ideology or Culture of the Organization*: this encompasses the traditions and beliefs of an organization.
Coordinating Mechanisms	The structure of an organization can be defined as the total of the ways in which its labour is divided into distinct tasks and then its co-ordination achieved among those tasks.	1. Mutual adjustment, whereby coordination is achieved by the process of *Informal Communications*. 2. Direct supervision as coordination is achieved through *Orders*. 3. Standardization of *Work Processes*. 4. Standardization of *Outputs*. 5. Standardization of *Skills*. 6. Standardization of *Norms* (common beliefs).

[101] In contextualist analysis (i.e. Pettigrew, 1987), the *vertical* level refers to the interdependencies between levels of analysis based upon phenomena at a further level. The *horizontal* level of analysis involves the connection between phenomena in historical, present and future time.

Contextual Elements		Parameters
Parameters of Design	The essence of organizational design is the manipulation of a series of parameters that determine the division of labour and the achievements of coordination.	1. *Job Specialization*: this is performed horizontally and vertically, of unskilled and professional jobs. Managerial jobs are typically the least specialised in the organization. 2. *Behavioural Formalization*: this is achieved through the imposition of operating instructions, job descriptions, rules and regulations. Behaviour formalization is most common in the operating core of the organization. At the strategic apex the work is the least programmed. 3. *Training* through Use of Formal Instructional Programmes: this aims to transfer skills, knowledge and indoctrination. 4. *Unit Grouping*: this refers to the choice of the bases by which positions are grouped together into units. 5. *Unit Size*: this is the number of positions contained in a single unit. 6. *Planning and Control Systems*: these are used to standardize outputs, evaluate performance, and plan action. 7. *Liaison Devises*: these are the series of mechanisms used to encourage mutual adjustment within and between units. 8. *Decentralization*: the vertical or horizontal diffusion of decision-making power.
Situational Factors	Situational factors influence the choice of the design parameters.	1. *The Age and Size of the Organization*: these affect the extent to which the organization's behaviour is formalized and its administrative structure elaborated. 2. *The Technical System of the Organization*: this influences especially the operating core and those staff units most clearly associated with it. 3. *The Environment of the Organization*: this can vary in its complexity, in how static or dynamic it is, in the diversity of its markets, and in the hostility it contains for the organization. 4. *The Power Factors of the Organization*: these include external control, personal power needs, and fashion.

For the purposes of analysing the process of organizational change, the researcher utilizes a number or organizational metaphors. As Walsham (1993:27) suggests, a metaphor is "a powerful and interesting approach to the 'reading' of organizations". Morgan (1986:12-13) agrees, and argues that "the use of metaphor implies a way of thinking and a way of seeing that pervade how we understand our world generally. [...] Many of our taken-for-granted ideas about organizations are metaphorical, even though we may not recognize them as such".

Therefore, similar to Walsham (1993), the researcher utilizes a synthesis of organization metaphors to understand organizational processes of change. The metaphors that are taken into consideration in the current study are three - the cultural, political action and communication metaphors of organization. Briefly, these suggest the following with regards to organizations.

The *cultural metaphor* of organizing suggests that culture is an active, changing phenomenon, while organizations do not have a single, unified culture, but rather a system of subcultures and a set of complementary perspectives (Riley, 1983). "The organizational culture metaphor emphasizes that organizations are not just settings of instrumental action but of expressive behaviour as well" (Fine, 1984:256). Scholars using this metaphor are explicitly concerned with how it can be applied to help managers control their environments - not necessarily in any direct way, but in terms of the symbolic consequences of their actions and their influence on culture. It thus offers a macro-level sensitizing tool for interpretive, symbolic interactionist studies. It directs research towards investigating how and why cultures and subcultures are created, maintained and changed over time. It also points towards investigating how the various subcultures interact with one another.

The *political action metaphor* of organizing adopts a more interpersonal, micro-level view to organizing, suggesting that organizations are loose networks of people with divergent interests who gather together for the sake of expediency (Morgan, 1986). Political action is seen as an endemic and continuous process, while 'power' is the medium through which conflicts of interest are resolved. The process of exercising power is not exempt from moral judgements. From an organizational management point of view, the metaphor of political action points towards investigating the balance between management control and individual and group autonomy across multiple levels of the organization.

Finally, the *communication metaphor* of organizing suggests that all organizational activity involves communicating. Therefore, this metaphor views organizations as the

interface of communication and interaction between various actors or groups in an effort to coordinate organizational activities.

The communication metaphor has evolved over time (Clausen, 2007) from a linear and mechanical process of information transmission[102] to a model that includes sociological factors in communication and highlights the importance of culture. In particular, culture may be a filter through which people construct (encode) and receive (decode) messages. Thus, communication models include sender, message, channel, noise (e.g. the perceptions or cultural backgrounds of the communicators), receiver, feedback and cultural context[103]. By introducing elements of the culture metaphor into the communication one, there are implications with regards to management and control. Communication is no longer linear and controllable; rather managers can influence its evolution, while they need to be considerate of varying communication methods and needs across groups. Having already recognized the significance of the cultural context in an organization, the communication metaphor that the researcher adopts is the latter one.

Overall, with regards to the above metaphors to organizing (or process models), although they involve distinctly different concepts, "they should not be seen as separate and non-overlapping; indeed they are inextricably interlinked" (Walsham, 1993: 48). Across the above three metaphors, or ways of seeing organizations, there are a number of common and research complementary concepts. Firstly, all three metaphors suggests that organizations *change*, while they stress the importance of *meaning* and the dynamic, ongoing processes involved in (re)creating this. Furthermore, all above metaphors suggest that an organization and its management need to take into consideration its *context*, whether that is the political, cultural or communications context. Finally, with regards to implications for decision-making and management all metaphors suggest that organizations are not rational entities that can be directly controlled - only influenced. This clearly has implications on the degree to which predictions can be made, as well as the methodological perspectives used to analyse organizations. Organizations need to be considered across various (vertical) levels of analysis as well as over time (i.e. horizontal analysis). Therefore, the above three metaphors reinforce the contextualist analysis view adopted in the current study, as well as point towards a need for longitudinal case-studies[104].

[102] I.e. Shannon and Weaver, 1949; Laswell, 1948;

[103] I.e. Jandt, 1998; Dahl and Habert, 1986.

[104] I.e. Walsham, 1993; Pettigrew, 1990.

All above process models/organizational metaphors need to be explicitly or implicitly encompassed in the sociological framework that will link the context and process. As Walsham (1993) suggests, the key feature of contextualist analysis is the linkage between context and process. This is key in order to understand in the current study the organizational impact of ISS management, which is constrained by the context as well as a factor in maintaining/altering that context.

Therefore, given the focus of this research on organizational encounters with (ISS) risk, the chosen framework is a risk one, namely that of the Social Amplification of Risk (SARF). The SARF, which was summarized earlier in Appendix-A1, is a heuristic tool that appreciates the dynamic organizational interactions - both at a social and individual level - across the various contextual levels of risk perception (i.e. Fig.3.4). It considers the processes involved in identifying risk, (re)creating meaning, as well as the ripple effects and impact of these. This 'risk encounter' process is one that may initiate a new process/cycle of organizational interactions. The SARF and its application by this study will be considered in the following section.

3.3 The research argument, conceptual framework and methodology

3.3.1. The research argument

After a review of organization theories and the practices associated with the management of ISS, technological hazards/risks, and major events/projects, the researcher has identified that as organizations become increasingly complex and interconnected, their ability to control - or rather influence - the processes of change is increasingly compromised. Yet, economic, political and social demands are increasing with regards to organizations and governments delivering highly reliable ISS operations.

This research argues that the process of ISS (risk) management is one of organizational change. A change whose outcome is not always controllable, and which is constrained by - as well as affects - the context within which it takes place. Therefore, the researcher suggests that in order to understand the organizational capacity to manage ISS reliably, researchers and practitioners alike must pay closer attention to the structural, political and cultural context of the organization.

The perceptions of risk and ISS behaviours that the organization aims to manage need to be considered across various levels of analysis - both vertical and horizontal. In addition, the processes of risk attention and sense-making need to be also understood in order to improve organizational communications[105] and risk controls.

The research, therefore, proposes the following elements of interest:

- The structural context (scope) of an organization and its impact on ISS risk perceptions (i.e. meanings), behaviours, and management efforts to deliver highly reliable ISS operations.
- The cultural and political context of an organization and its impact on ISS risk perceptions, behaviours, and management efforts to deliver highly reliable ISS operations.
- The nature of ISS risks and their impact on risk perceptions, behaviours and management efforts to deliver highly reliable ISS operations.
- The expectations, obligations, motivations and roles of different ISS management process stakeholders with regards to delivering highly reliable operations.

[105] 'Organizational communications' cover inter-, intra- and external organizational communications.

- The organizational processes of ISS risk attention, sense-making and re-organizing under 'routine' versus 'emergency/incident' conditions.

Throughout all these elements of interest the concept of 'time' is key, since the researcher wishes to also consider how the above elements change over time. As suggested earlier (i.e. section 2.3.4), the organizational process of delivering highly reliable ISS operations is a learning one. Therefore, the above research elements will not only be considered in terms of their interaction at a specific point in time, but also over time, thus reviewing the organizational capacity to learn and improve ISS behaviours and practices.

A number of conceptual and methodological approaches will be utilized in order to analyse the elements of interest identified above. These will be examined below.

3.3.2. The conceptual framework for conducting the argument

As presented earlier, the current study adopts an interpretivist analysis approach in order to investigate the organizational process of change relating to the delivery of highly reliable ISS operations in a major event context. Therefore, breaking down the research question into its context, process and content components, the following emerge:

The organizational *context* under investigation is that of a major event, namely the A2004 Olympic organization. As suggested earlier this will be described in detail with the use of Mintzberg's scheme of organizational context levels. The parameters considered by this scheme are summarised in Table 3.1.

The organizational *process* of change under investigation is the preparation and delivery of a secure IS infrastructure that will support the A2004 operations. The analysis of this is based on the assumptions of three organization process models/metaphors (i.e. section 3.2.2), which suggest that an organization is a communication network whose outcome is determined by the structural characteristics of the network as well as the cultural and political interactions, expectations, motivations and behaviours.

In order to *link the context and process* the Social Amplification of Risk Framework (SARF) is utilized in this study, encompassing the above assumptions and supporting the investigation of dynamic organizational interactions related to the risk attention,

sense- and decision-making processes, as well as the impact of these. The SARF is summarized in Appendix-A1, yet it will be considered here in some more detail.

Lastly, with regards to the *content* of the change process, this will have to be assessed against the organizational objective with regards to the change process outcome - namely the delivery of highly reliable IS(S) operations. Therefore, it will be necessary to consider in more detail the notion of 'high reliability'. This will be done by drawing upon the work of high reliability theorists.

Therefore, the following paragraphs will consider in more detail the conceptual framework of SARF and the parameters to highly reliable organizations, in order to then proceed with presenting the method used to apply these frameworks to the research question and argument.

3.3.2.1 Linking the context and process of change: the SARF

The various scholars who developed the SARF[106] aimed to develop an integrative theoretical and empirically operational framework capable of accounting for findings from a wider range of studies. They aimed to understand risk perceptions and behavioural patterns at both a social and individual level, by considering the dynamic processes of risk identification, sense-making, and communication. In particular, the SARF's focus was on processes by which certain hazards and events that experts assess as relatively low in risk can become of a particular concern and socio-political activity within a society (*risk amplification*), while other hazards that experts have judged to be more serious receive comparatively less attention from society (*risk attenuation*).

The theoretical starting point is the assumption that 'risk events', which might include actual or hypothesized accidents and incidents, will be largely irrelevant or localized in their impact unless human beings observe and communicate them to others (Luhmann, 1979). The SARF suggests that

> "risk, risk events and the characteristics of both become portrayed through various risk signals which in turn interact with a wide range of psychological, social, institutional or cultural processes in ways that intensify or attenuate perceptions of risk and its manageability. The experience of risk, therefore, is

[106] I.e. Kasperson et al, 1988; Renn, 1991; Kasperson, 1992; Burns et al., 1993; Kasperson and Kasperson, 1996.

> not only an experience of *physical* harm but the result of processes by which groups and individuals learn to acquire or create *interpretations of risk*. [...] Within this framework, risk experience can be properly assessed only through the interaction among the physical harms attached to a risk event and the social and cultural processes that shape interpretations of that event, secondary and tertiary consequences that emerge, and the actions taken by managers and publics" (Kasperson et al, 2003:15).

Therefore, the fundamental concept used in the SARF is that of a 'risk sign' and its associated perceptions and behaviours. The underlying organization metaphor of this framework is the communication/amplification one. Kasperson et al (1988:181-182) argue that regardless of the mechanistic description of the amplification metaphor, "the process of transmitting is far more complex. [...] The information system and characteristics of the public response that compose social amplification are essential elements in determining the nature and magnitude of risk". As Renn and Rohrmann (2000) have suggested, risk signs are dynamically filtered through a number of contextual levels of risk perception (i.e. Fig.3.4).

Proponents of the SARF suggest that by understanding the properties of the risk sign along with the organizational context within which this is interpreted and controlled, it is possible to improve the appraisal, evaluation/characterization, management and communication of a risk. This applies both in cases of proactive risk management and reactive incident/event management.

Thus, in terms of applying this conceptual framework to the investigation of ISS, this approach views organizations and their IS(S) as communication networks where people do the processing. Understanding the processes of risk attention and sense-making will lead to better re-organization, improving ISS management practices. At this point, the SARF's stages and mechanisms of amplification will be presented in more detail.

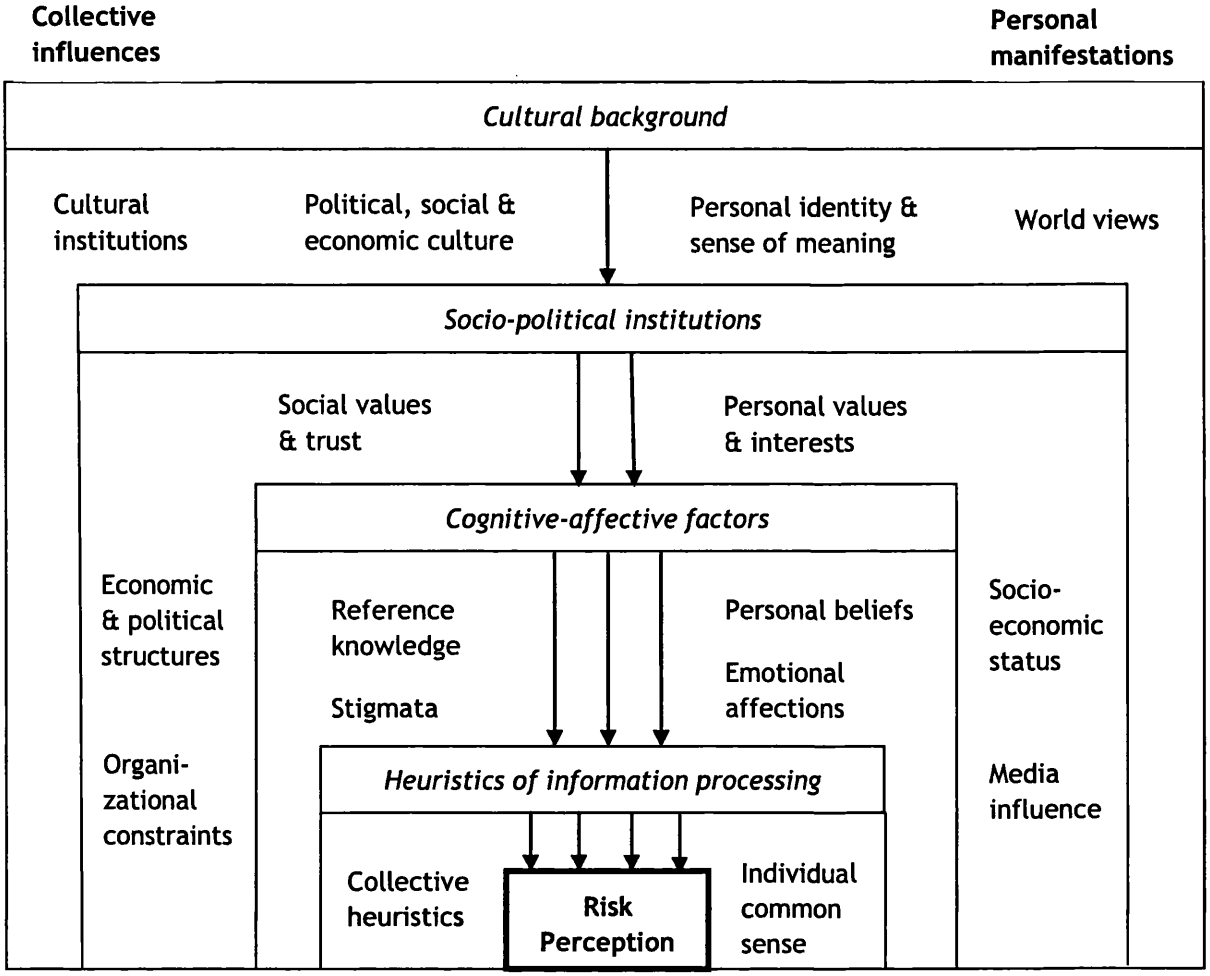


Figure 3.4: *Four context levels of risk perception* (Source: adapted from Renn and Rohrmann, 2000).

SARF - the stages of amplification

The SARF suggests that an IS may amplify/attenuate risk events in two ways - by either intensifying/weakening signals that are part of the information that individuals and social groups receive about the risk; or by filtering the multitude of signals with respect to the attributes of the risk and their importance.

Kasperson et al (1988) suggest that risk signals are subject to predictable transformations as they filter through various *amplification stations* (i.e. Fig.3.5).

Individual stations of amplification are affected by considerations - well documented by the psychometric tradition - such as risk heuristics, qualitative aspects of the risks, prior attitudes, blame and trust. These same individuals are also members of

cultural groups and other social units that codetermine the dynamics and social processing of risk[107].

For *social stations of amplification*, the likes of institutional structure, functions and culture influence the amplification/attenuation of risk signals. Even the individuals in institutions do not simply pursue their personal values and social interpretations; they also perceive the risks, those who manage the risks, and the risk 'problem' according to cultural biases and the values of their organization or group[108].

Thus, Kasperson et al (1988) suggest that some key amplification steps consist of the following:

- Filtering of signals (e.g. only a fraction of all incoming information is actually processed);
- Decoding of the signal;
- Processing of risk information (e.g. the use of cognitive heuristics for drawing inferences);
- Attaching social values to the information in order to draw implications for management and policy;
- Interacting with one's cultural and pier groups to interpret and validate signals;
- Formulating behavioural intentions to tolerate the risk or to take actions against the risk or risk manager;
- Engaging in group/individual actions to accept, ignore, tolerate or change the risk.

[107] I.e. Vaughan, 1995; Palmer et al, 2001.

[108] I.e. Rayner, 1992; Peters and Slovic, 1996.

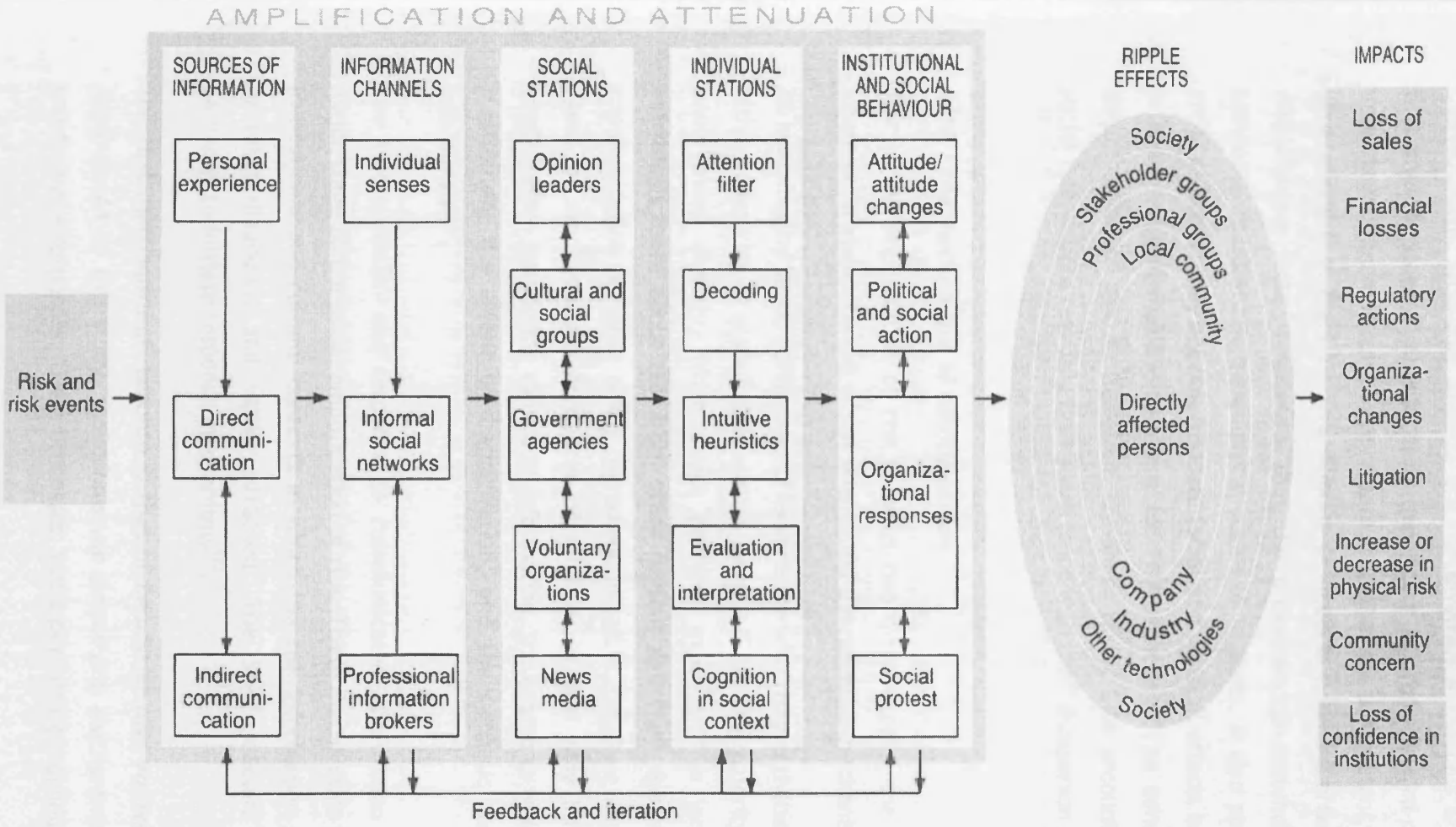


Figure 3.5: *Conceptual framework of social amplification of risk* (Source: Kasperson et al, 1988).

Consequently, secondary impacts are perceived by individuals and social groups so that another stage of amplification may occur to produce third-order impacts. The impacts thereby may spread, or '*ripple*', to other parties, distant locations or future generations (i.e. Fig.3.5). This rippling of impacts is an important element of risk amplification since it suggests that the processes can extend or constrain the temporal, sectoral and geographical scales of impacts. It also points out that each order of impact may not only allocate social and political effects but may also trigger or hinder managerial interventions for risk reduction."The concept of the social amplification of risk is, therefore, dynamic, taking into account the learning and social interactions resulting from experience with risk" (Kasperson et al, 1988:183).

SARF - the mechanisms of amplification

The social amplification of risk involves two major stages: the communication of information about the risk or risk event, and the response mechanisms of society.

As indicated by Slovic (1986), direct experience with risky activities or events can be either reassuring or alarming. However, many - if not the majority of - risks are not experienced directly. When direct personal experience is lacking or minimal, individuals learn about risk from other persons and from the media. Information communication becomes a key ingredient in public response and acts as a major agent of amplification. Attributes of information that may influence the social amplification include the volume of information, the degree to which the information is disputed, the extent of dramatization, and the symbolic connotations of the information[109].

The interpretation and response to communicated information form the second major stage of the social amplification of risk. These mechanisms involve the social, institutional and cultural contexts in which the risk information is interpreted, its meaning diagnosed and values attached. The SARF scholars hypothesize five pathways to initiate response mechanisms[110].

The first mechanism of response is that of ***heuristics and values***. As presented in Appendix-A1 of this study, individuals use simplifying mechanisms to evaluate risk and to shape responses. These processes, while permitting individuals to cope with a

[109] I.e. Kasperson et al, 1988; Mazur, 1981; Blumer, 1969.

[110] I.e. Kasperson et al, 1988; 2003.

risky world, may sometimes introduce biases that cause distortions and errors[111]. Similarly, the application of individual and group values will also determine which risks are deemed important or minor and what actions, if any, should be taken. Most information to which the average person is exposed will be ignored. However, the attention and selection process is not random. According to Chaiken and Stangor (1987) the major criteria for selection are ability and motivation[112]. If both these criteria are met, a complex procedure of information selection and processing takes place after the initial attention-drawing stimulus[113].

In order to economize information processing, individuals are likely to evaluate whether it is necessary to study the content of the information in detail or to make a fast judgement according to salient cues in the message received[114]. These *intuitive heuristics* explain why individuals do not base their risk judgements on expected values. There is ample evidence for clear violations of logical rules in common-sense reasoning when it comes to processing probabilistic information. *Biases* have been identified in people's ability to draw inferences from probabilistic information[115]. Some of these are summarized below in Table 3.2.

In addition to the cognitive heuristics and biases, more recent research has brought to the fore an additional heuristic, that of *affect/emotion*, and its interplay with cognition[116]. The affect heuristic suggests that people may judge the risks and benefits of hazards by accessing a pool of positive and negative feelings that they associate with the hazards. According to Finucane et al (2000) the existence of such a heuristic would explain the empirical observation where perceived risk and perceived benefit are inversely related in people's minds.

---

[111] I.e. Kahneman et al, 1982.

[112] *Ability* refers to the physical possibility of the receiver to follow the message without distraction. The conditions necessary to satisfy the criterion of ability are: (a) information must be accessible, (b) the receiver must have the time to process the information, and (c) other sources of distraction should be absent. *Motivation* refers to the readiness and interest of the receiver to process messages. The factors influencing the motivation of the receiver include: (a) the relevance of the information content, (b) the extent to which the information can trigger personal involvement, (c) the receiver's prior knowledge or interest in the subject.

[113] I.e. Renn, 1992b, 2008.

[114] I.e. Renn and Levine, 1991; Renn, 2008.

[115] I.e. Kahneman and Tversky, 1973, 1979; Slovic et al, 1976, Slovic, 1972.

[116] I.e. Finucane et al, 2000; Slovic, 1997; Alhakami and Slovic, 1994; MacGregor, 2003.

Table 3.2: *Biases related to drawing inferences from probabilistic information.*

Availability bias	Events that come immediately to people's minds are rated as more probable than events that are of less personal importance.
Representativeness bias	Singular events experienced in person or associated with the properties of an event are regarded as more typical than information based on the frequency of occurrence.
Hindsight bias	Being told that some event has happened increases people's feeling that it is inevitable. In retrospect, people tend to believe that they (and others) had a much better idea of what was going to happen than they actually did have. Such misperceptions can seriously prejudice the evaluation of decisions made in the past and limit what is learned from experience (i.e. Fischhoff, 1974).
Anchoring effect	Probabilities are estimated according to the plausibility of contextual links between cause and effect, but not according to knowledge about statistical frequencies or distributions. People will use an anchor as a first approximation to the judgement. This anchor is then adjusted to accommodate the implications of additional information. However, the adjustment will be crude and imprecise and will fail to do justice to the importance of additional information.
Selection bias	Information that challenges perceived probabilities that are already part of a belief system will either be ignored or downplayed.

Without ruling out the use of cognitive heuristics by individuals, researchers[117] suggest that judgements of risk and benefit are guided and linked by affect. Reliance on affect ebbs and flows according to various contextual factors. Finucane et al (2000) suggest at least two conditions under which affect plays an important role and intensifies in people's minds the inverse relationship between perceived risk and perceived benefit. This is when (a) risk and benefit judgements are taken under time pressure, and (b) when manipulating affect by providing risk and benefit information.

Another important finding in the field of risk perception is that heuristics and biases - both cognitive and affect - are applicable to both experts and laypersons. Therefore, the importance of social values in risk perception and acceptance has become apparent[118].

This also applies at the stage of decision-making, where the presentation of the risk information is rife with subjectivity. Numerous research studies have demonstrated that different ways of presenting - *framing* - the same risk information can lead to different evaluations and decisions[119]. We thus know that every form of presenting

[117] I.e. above footnote.

[118] I.e. Slovic, 1987b, 1997; Thompson and Dean, 1996.

[119] I.e. McNeil et al, 1982; Tversky and Kahneman, 1981; Gregory et al, 1993.

risk information is a frame that has a strong influence on the decision-maker. "There are often no 'right frames' or 'wrong frames' - just 'different frames'" (Slovic, 1997:281).

Therefore, contrary to the traditional view of risk characterised by event probabilities and consequences, the subjective and contextual factors described above are no longer secondary or accidental dimensions to risk. Extensive research has indicated that gender, race, political worldviews, affiliation, emotional affect and trust are strongly correlated with risk judgements. In fact most people, including laypersons and experts, demonstrate a mix of all value clusters depending upon context and social relations[120].

The second mechanism of risk sign interpretation and response in the SARF is that of ***social group relationships***. Risk issues enter into the political agenda of social, political and organizational groups. The nature of these groups will influence member responses and the types of rationality brought to risk issues. If a risk becomes a central issue in a political or social debate, it will be vigorously brought to more general public attention, often coupled with ideological interpretations of technology or the risk management process[121]. Such social alignments can become anchors for subsequent interpretations of risk management and may become quite firm in the face of conflicting information. Therefore, the social group relationships amplification mechanism consists of institutional structures, functions and cultures.

Research in the field of risk perception has indicated that the seriousness and higher-order impacts of a risk event are determined, in part, by what that event signals or portends[122]. Therefore, the third mechanism of response in SARF is that of the ***signal value***. The informativeness or 'signal value' of an event appears to be systematically related to the characteristics of the event and the hazard it reflects. Risks or a risk event can signal the degree to which it is controllable, familiar, competently managed etc. Fischoff's and Slovic's research[123] has indicated that risks in the upper right-hand sector of the classic dread/knowledge psychometric factor space (i.e.

[120] I.e. Slovic, 1997; Renn, 2008.

[121] I.e. Rayner and Cantor, 1987; Douglas and Wildavsky, 1982; Johnson and Covello, 1987.

[122] I.e. Slovic, 1987b; 1992; Kasperson et al, 1988.

[123] I.e. Fischhoff et al, 2000; Slovic et al, 1980; Slovic, 1987, 2000.

Fig.3.6) have a signal value in terms of serving as a warning for society, providing new information about the probability that similar or even more destructive mishaps might occur with this type of activity.

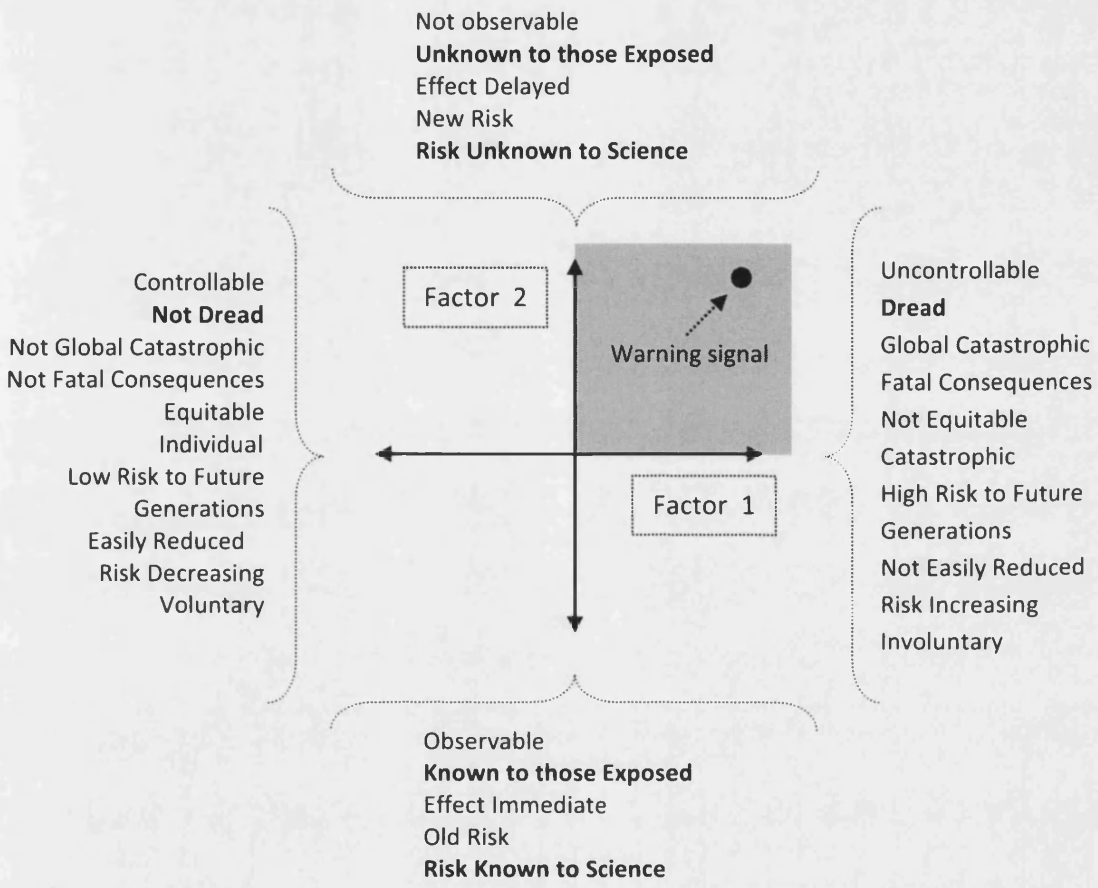


Figure 3.6: *Factor-analytic representations of risk characteristics* (Source: adapted from Slovic et al, 1980).

The fourth SARF mechanism of risk response is that of ***imagery and stigmatization***. Stigma refers to the negative imagery associated with undesirable social groups or individuals (Goffman, 1963). However, environments, technologies and organizations can also be associated with negative images. According to Slovic (1987a), since the typical response to stigmatized persons or environments is avoidance, it is reasonable to assume that risk-induced stigma may have significant social and policy consequences.

Research has demonstrated the importance of stigmatization as a principal route by which risk amplification can generate ripples and secondary consequences[124]. Stigma-induced effects are associated with risky technologies, products, projects or services, and can be substantial. Gregory et al. (1995) suggests that those that are stigmatized share several features.

> "The source of the stigma is a hazard with characteristics such as dread consequences and involuntary exposure, that typically contributes to high public perceptions of risk. Its impacts are often perceived to be inequitably distributed across groups. [...] Often the impacts are unbounded, in the sense that their magnitude or persistence over time is not well known. [...] Management of the hazard is brought into question as concerns surface regarding competence, conflicts of interest or a failure to apply needed safeguards and controls" (Kasperson et al, 2003:27-28).

Accompanying the process of stigmatization - or *marking*[125] - will often be a story or narrative that interprets the evolution of the stigma and assigns responsibility or blame for its presence.

SARF scholars suggest that understanding stigma effects is crucial in anticipating which new technologies, controls, policies etc. will be stigmatized through amplification processes. Stigma effects have broad implications for risk management and risk communication efforts, since they can greatly enlarge the potential of rippling[126] (Kasperson et al, 2001).

The final mechanism to amplification identified by the SARF is that of ***social trust***[127]. More recent and broad research has indicated that recurrent failures in risk

[124] I.e. Flynn et al, 2001.

[125] I.e. Kasperson et al, 2003:29.

[126] I.e. Kasperson et al, 2001.

[127] Definitions and functions of trust vary. It has been suggested that trust facilitates the working of the political system (Inglehart, 1988), is an important dimension of social capital (Coleman, 1990; Putnam, 1993, 1995b), and also functions to reduce complexity in our social environment (Barber, 1984), hence making life more predictable. Earle and Cvetkovich (1995) suggest that trust is the similarity in our basic values, rather than attributes of technical competence, that underlies whom we trust or distrust. Renn and Levine (1991), on the other hand, have argued that trust underlies confidence, and, where this is shared across a community, one has credibility. They thus suggest five attributes to trust, namely competence, objectivity, fairness, consistency, and faith.

management stem in no small part from a failure to recognize the more general requirements of democratic society, and especially the need for 'social trust'[128].

> "Risk control efforts have frequently gone awry due to a lack of openness and 'transparency', a failure to consult or involve so-called 'interested' and 'affected' persons, a loss of social trust in managers, inadequacies in due process, a lack of responsiveness to public concerns, or an insensitivity to questions of environmental injustice" (Kasperson et al, 2003:31).

Slovic (1993, 2000) has argued that trust emerges slowly, is fragile, easily destroyed, and once lost it may prove to be extremely difficult to recover. He posits an 'asymmetry principle' to explain that it is easier to destroy than to create trust. He suggests that negative (trust-destroying) events are more visible or noticeable than positive (trust-building) events. Negative events often take the form of specific, well-defined incidents such as accidents, while events that are invisible or poorly defined carry little weight in shaping our attitudes and opinions.

The SARF scholars argue that from a policy implication point of view, the research on trust suggests that we need to frame the principal goals of risk communication around building trust through participation. However, one needs to be considerate towards the impacts of candid communications. These can signal honesty for some while invoke greater distrust in others. Therefore, effective risk communication may follow only if a resolution of conflict is obtained first[129]. SARF proponents raise caution of broad 'stakeholder' participation methods, which are often seen uncritically as essential to the wider processes of risk assessment and management and a route to success[130].

Overall, SARF scholars suggest that issues of social trust are important components of the dynamics of social amplification.

> "Distrust acts to heighten risk perceptions, to intensify public reactions to risk signals, to contribute to the perceived unacceptability of risk, and to stimulate political activism to reduce risk. [...] Trust is highly interrelated with other components and mechanisms in what we think of as 'amplification dynamics'" (Kasperson et al, 2003:32-33).

---

[128] I.e. Kasperson et al, 2003; 1992; 1999; Cvetkovich and Löfstedt, 1999.

[129] I.e. Renn et al, 1995; Arvai et al, 2001.

[130] I.e. Kasperson et al, 2003; Kasperson, 2003; Stern and Fineberg, 1996.

The SARF scholars conclude that understanding the phenomenon of risk amplification is a prerequisite for assessing the potential impacts of projects and technologies, for establishing priorities in risk management, and for setting health, safety, operational reliability and other related standards (Kasperson et al, 1988).

3.3.2.2 Assessing the content of change: highly reliable organizations

As stated earlier, the focus of this research is to understand an organization's capacity to deliver highly reliable ISS operations in an inherently risky, high performance demand environment. It is, thus, imperative that the concept of 'high reliability' is clearly defined.

'High reliability' in the organization theory discipline refers to an organization's ability/objective to succeed in avoiding significant operational failures and disasters in an environment where 'normal accidents' can be expected due to risk factors and complexity[131]. The organizations that aim for high reliability tend to be those that cannot afford to fail, since otherwise their existence and/or legitimacy, would be compromised.

As described in section 2.3.4, scholars acknowledge that organizational encounters with error and the unexpected are an inescapable part of organizational reality[132]. Therefore, they do not suggest that highly reliable organizations are error-free. Instead, they suggest that organizations which operate risky/hazardous technologies and have a low tolerance for failure create strategies that are focused on operational robustness and/or resilience, anticipating and containing errors[133].

Thus, high reliability - and normal accident - theorists[134] acknowledge that 'high reliability' involves a set of organizational design (OD), organizational culture (OC), and operations management (OM) controls, which can have an error anticipation (A) or containment (C) focus (i.e. Table 3.3).

---

[131] I.e. LaPorte and Consolini; 1991; Weick and Sutcliffe, 2001 and 2007.

[132] I.e. Turner, 1978; Turner and Pidgeon, 1997; Vaughan, 2005.

[133] I.e. Sagan, 1993; Roberts and Bea, 2001; Wildavsky, 1988; Weick and Sutcliffe, 2007.

[134] I.e. Sagan, 1993; Roberts, 1990a; Weick and Sutcliffe, 2001 and 2007.

Table 3.3: *Controls required for the delivery of highly reliable operations.*

High Reliability Controls			Control Focus
1	*Reduction of interactive complexity*	Reduce the number of variables in the system, the number of relationships between the variables, and the number of feedback loops trough which the variables interact.	OD (A+C)
2	*Reduction of process tightness*	Increase component redundancy, resource buffers/slack, and process flexibility.	OD (A)
3	*Prioritization of safety & reliability across the organization's leaders & political elites*	Organizational leaders should clearly communicate that short-term efficiency will take the second seat to very high reliability operations. In addition, they must be prepared to spend on significant levels of redundancy and training.	OC (A) OD (A)
4	*Redundancy*	Implement multiple and independent channels of communication, decision-making, and implementation. Technical controls and key personnel should be duplicated and overlap where possible.	OM (A) OD (A)
5	*Decentralization*	Reduce where possible the number and severity of organizational component failures, by decentralizing decision-making authority with regards to safety issues.	OD (A) OM (A)
6	*Reliability culture*	Personnel must be able to correctly and quickly identify problems, while responding appropriately. Recruiting, socializing, and training personnel are required, in order for them to know when to use formal rules and when to improvise.	OC (A)
7	*Continuous operations & training*	Maintain continuous operations and training in order to avoid routinization and lack of challenge that lead to complacency.	OM (A) OC (A)
8	*Organizational learning*	Develop a strong capability to learn by regularly adjusting procedures and routines, and support learning through a process of trial and error.	OM (A)
9	*Preoccupation with failure*	Encourage personnel to pay close attention to weak signals of failure, while clearly stating the mistakes that they should not dare make. Support variety of error detection and reporting mechanisms, while encouraging personnel to question their own/other's expectations.	OC (A) OM (A)
10	*Reluctance to simplify*	Encourage personnel to question the existing categories and expectations, while also seeking the viewpoint and expertise of other organizational groups/individuals.	OC (A)
11	*Sensitivity to operations*	Encourage personnel to give undivided attention to operations, small deviations and interruptions. Inter-disciplinary and -departmental meetings can help to that end.	OM (A) OC (A)
12	*Commitment to resilience*	Encourage personnel to be attentive to expanding their knowledge and technical facility, while elaborating their response capabilities.	OC (C)
13	*Deference to expertise*	As the tempo of operations increases and unexpected problems arise, decisions must be able to migrate both up and down in the organization, where expertise lies.	OM (C) OC (C)

Overall, if we consider the parameters to highly reliable operations suggested by the various high reliability, normal accident, and mindful organizing approaches, a variety of control requirements need to be in place in order for an organization to deliver highly reliable operations. As summarised in Table 3.3, these controls will often overlap yet vary in their focus, indicating that there is a need for a multi-layered controls approach to high reliability.

For the purposes of this study, while the focus remains on the organizational processes of risk identification, sense-making, response and re-organizing, the outcome of these processes is assessed against the parameters of the organization's high reliability objective.

In fact, this study will later consider the value of the above high reliability parameters as an audit tool that will direct organizations towards assessing and evaluating the efficiency and effectiveness of their controls and culture.

3.3.3. The method for conducting the argument

As suggested earlier, this research takes an interpretivist analysis approach and, in a fashion similar to Walsham's (1993) research, it utilizes three different conceptual schemes to investigate and later discuss the elements of context, process and content/outcome of a major event ISS management project.

The research analysis starts with the presentation of the organization's structural context. Given that the investigation of context will be static unless examined repeatedly across time, Mintzberg's scheme is utilised across the various stages of the ISS management project. The reasoning behind this approach is that the organizational structure and context change across project phases in parallel to changes in work activities and situational factors.

Once the contextual setting to each project phase is defined, the study continues with the investigation into the process of ISS risk amplification. At this stage of research analysis, the processes and parameters involved in the creation of ISS risk meaning, perceptions, and eventually behaviours are considered. The various mechanisms of amplification identified by the SARF contribute towards defining how the organizational context interacts with ISS risk perceptions and behaviours.

Finally, following the identification of ISS risk perceptions and behaviours, the impact and ripples of the risk amplification process is considered in terms of the organizational level of ISS high reliability.

The basic objective of the method presented above and summarised in Table 3.4 is to provide a means of evaluating organizational reality and guiding the researcher during empirical work. Although the researcher's objective is to develop a rich description and understanding of the various parameters to the organization's encounter with ISS risk, she remains open to any further conceptual elements that may emerge as research progresses.

Table 3.4: *Levels of research analysis.*

Contextualist Analysis Dimension	Analytical Level	Elements of Analytical Level
Context of change	Parts of the organization	The IS(S) operating core; the strategic apex of IS(S) managers; the IS(S) technical staff; the IS(S) support staff; the organizational IS(S) culture/ideology.
	Coordination mechanisms	The informal IS(S) communications; the IS(S) direct supervision and orders; the standardised IS(S) work processes; the standardised IS(S) outputs; the standardised IS(S) skills; the standardised IS(S) norms.
	Parameters of design	IS(S) job specialisation; IS(S) behavioural formalization; IS(S) training; IS(S) unit grouping; IS(S) unit size; IS(S) planning & control systems; IS(S) liaison devices; IS(S) decentralization.
	Situational factors	The age & size of the IS(S) organization; the technical system of the IS(S) organization; the environment of the IS(S) organization; the power factors of the IS(S) organization.
Process of change	1st stage of amplification: risk communication	The source(s) of ISS information; the ISS information channel(s); the individual/social station ISS messages; the factors determining individual/social risk perceptions.
	2nd stage of amplification: risk response	Individual/social ISS behaviours; social ISS impacts; stakeholder ISS impacts; professional group ISS impacts; local community ISS impacts; individual ISS impacts.
Content of change	Organizational design (OD) controls	IS(S) interactive complexity; IS(S) process & resource tightness; IS(S) redundancy; IS(S) technological control decentralization.
	Operations management (OM) controls	IS(S) communication channel redundancy; IS(S) roles & responsibilities duplicity and overlap; IS(S) decision making decentralization; IS(S) continuous training & operations; IS(S) continuous learning & adjustment of procedures and training; variety of IS(S) error detection & reporting mechanisms; inter-disciplinary & - departmental meetings to cross-check operational IS(S) expectations & experience; migration of IS(S) decision making to expertise.
	Organizational culture (OC) controls	Communication of 'high reliability' IS(S) mission objective; training for correct identification & response to IS(S) problems; IS(S) messages communicated via recruitment, training & socializing; IS(S) routinization & complacency avoidance; acknowledgment of IS(S) expectations' limitations; vigilance/attention to weak IS(S) risk signals; encourage communications with other experts/occupations; communication of IS(S) operations priority; encourage the expansion of IS(S) knowledge base and skills; encourage reporting any suspicious IS(S) activity; encourage the delegation to expertise & the seeking of assistance.

3.4 The research design

3.4.1. The research strategy

This research adopts a longitudinal in-depth case study approach, aiming to observe the patterns of behaviour and events that unfold over a period of time. As suggested by Walsham (1993) and Pettigrew (1990), the best research method for contextualist studies focusing on processes of change is indeed longitudinal case-studies, since such an approach can

> "explore the contexts, content, and process of change together with their interconnections through time. [...] The longitudinal case study method provides the opportunity to examine continuous processes in context and to draw in the significance of various interconnected levels of analysis. Thus there is scope to reveal the multiple sources and loops of causation and connectivity so crucial in identifying and explaining patterns in the process of change" (Pettigrew: 1990:268, 271).

As suggested by Creswell (1998), the choice of a case-study strategy is based on a number of reasons, all of which match the objectives of the current study. Firstly, the research argument needs to be studied in a natural setting, focusing on contemporary events, without, however, requiring to control such events. In addition, the 'case' under study is one of a 'bounded system', bounded by time and place, while its investigation is expected to advance the knowledge of the phenomenon, context and theory under consideration. This is especially true in the case of *instrumental* case studies[135], such as the current one, where the case itself provides a supportive role and facilitates understanding.

With the use of extensive, multiple sources of information in data collection to provide the detailed in-depth picture of the 'case'[136], the researcher spends considerable time describing the context or setting for the case, along with the detailed events during the investigation period. Thus, "the investigator narrates the study through techniques such as a chronology of major events followed by an up-close or a detailed perspective about a few incidents" (Creswell, 1998: 63). In the final interpretive phase of a case study, the researcher highlights lessons learned (Lincoln and Guba, 1985), and links "emerging conceptual and theoretical ideas

[135] I.e. Stake, 1995.

[136] I.e. Yin, 1989.

inductively derived from the case both to stronger analytical themes within the case and wider theoretical debates in the literature" (Pettigrew, 1990:280).

Case-studies are criticised on two grounds. Firstly with regards to the challenge of identifying a case and its boundaries - how it might be constrained in terms of time, events, and processes (Creswell, 1998). More importantly, however, case studies are criticised on grounds of non-representativeness and lack of statistical generalizability, a term that holds little meaning for most qualitative researchers[137].

> As Walsham (1993:15) suggests "from an interpretive position, the validity of an extrapolation from an individual case or cases depends not on the representativeness of such cases in a statistical sense, but on the plausibility and cogency of the logical reasoning used in describing the results from the cases, and in drawing conclusions from them".

3.4.2. The unit of analysis

The current study focuses on the IS aimed to support the Athens 2004 (A2004) Summer Olympic Games during the event time. This IS solution is otherwise known as the 'Games-IS' and it aimed to capture and report every moment of the event's action, communicating this to the world via a number of media, including television and the Internet. This IS solution involved a complex mix of technology, processes and people, was great in scale, covered a variety of clients, sites and systems, while it also was a multi-supplier project with many varied dependencies.

One of the key areas upon which this project focused on was that of security and risk management, aiming to deliver highly reliable, secure IS operations.

Although Olympic sports events are repeated at regular intervals and some knowledge transfer can be assumed from one event to the next, the management of ISS had not been strategically considered prior to the A2004 event. The particular event was the first one in the history of Olympic events to consider ISS and risk management as fundamental processes in the successful delivery of highly reliable IS operations.

As is described in the following section of this study, the first elements of the organization that would prepare and operate the Games-IS infrastructure were put in place approximately four years in advance of the event. The first elements of the ISS

[137] I.e. Glesne and Peshkin, 1992.

management project organization, on the other hand, were put in place two years prior to the A2004 Games. The researcher joined the organization at that stage and continued her research, data collection and analysis for the entire two-year period of the Games-ISS project; from initiation to closure. Therefore, the case-study boundaries were relatively clearly defined - both the timeframe and scope.

As presented above, the focus of the research is the process of risk management and organizational change involved in preparing and delivering highly reliable ISS operations[138]. This is the process under investigation and the two-year period (from June 2002 to September 2004) during which data was collected and analysed. Organizational structures, activities, priorities, the cultural and political context changed during that period, as well as ISS perceptions, behaviours and controls.

The A2004 Olympic organization, the IS integration and ISS management projects under study are unique as they were specific to their time, space and context. Yet, major project and event organizations and their requirement for highly reliable IS(S) infrastructures are certainly not unique. As covered in section 2.4 of this study, organizations and their deliverables are increasingly organized in megaproject and event structures. In addition, complex and great in scale IS infrastructures that are implemented by various partners, for diverse clients, and with highly reliable security requirements, are not at all uncommon. Yet, such case studies have been rarely investigated; in fact, there is no evidence of prior research with a focus similar to the one presented in the current study.

Therefore, the researcher considers that the investigation of the A2004 Olympics ISS case-study operates instrumentally to facilitate greater understanding with regards to a major-event organization's capacity to deliver highly reliable ISS operations. The organizational structure, scope, outer and inner context will be considered in relation to the organization's objective to deliver highly reliable ISS.

[138] As quoted by one of the managers overseeing the Games-time IS integration, this was an organization that within a period of two years had to "get from zero to hero".

3.4.3. Data collection methods

From early on in the data collection research stage, the researcher had to address issues of site and information access, and rapport. Initial access to the case study environment initiated by approaching executive members of the ATHOC (Athens Olympic Committee) and the IOC (International Olympic Committee) approximately six months prior to entering the organization for in-depth data collection. Informing them of the researcher's interests and requirements, members of the two organizations provided some background information on the structure, mission and high-level plan of the A2004 IS Integration project. They agreed to provide the researcher access to the ATHOC organizational environment, where data collection could officially commence.

Therefore, the on-site data collection started in June 2002, observing daily activities and focusing data collection on understanding better the greater organizational structure, the project plan, partners' roles, responsibilities, interests and expectations.

As is demonstrated in Chapter 4 of this study, given that this was a project organization with distinct project phases, deliverables and deadlines, the pace of organizational change was relatively fast. As was foreseen, the organization grew quickly in scale and complexity, while partnering organizations and teams had to increasingly coordinate their mutual and/or interconnected activities. Direct access to people and information was harder to obtain, with direct implications onto the data collection activities of the researcher[139].

Research data had to be collected from both primary and secondary sources, while the data methods varied depending on the focus of analysis, the availability and number of respondents (sample size). Therefore, both quantitative and qualitative data was collected, although the research focuses primarily on the latter type. Data collection methods are summarized in Table 3.5. In addition, the researcher maintained her own personal log of daily project activities, observations and views. These were later compared to findings associated with workers' perceptions, observed behaviours and incidents.

[139] During the period of data collection the researcher held the following positions in chronological order: (a) March 2002 - June 2002: independent observer (reporting to the IOC); (b) June 2002 - June 2003: independent observer (reporting to ATHOC); (c) June 2003 - September 2004: ISS Risk Associate & Transfer of Knowledge Consultant (reporting to SchlumbergerSema/Atos Origin).

Table 3.5: *Data types and collection methods*

Primary Sources		Secondary Sources	
Interviews (structured & semi-structured)	>90	Policies & Procedures	>150
Meeting Minutes	>80	Audit-Trail Logs	>50
Questionnaires	>120	Performance Metric Reports	>100
Device Logs	>100	Audit Reports	>160
Incident Logs	>20,000	SL2002 ToK Documents	>15
Incident Reports	>20	Training Material	>10
Focus Group Meetings	>10	AAR Reports	>20
Daily/Monthly Journals (Field Note Observations)	24	Marketing Presentations	>20
		Publications/Press Articles	>150
		IT Design Documents	>20
		Strategy Plans & Guidelines	>10

In relation to the interviews conducted (i.e. Appendix-A3), a number of ISS management process stakeholders were identified depending on their organizational (formal and informal) role and responsibilities, while interview topics and degree of structure depended on the project phase and emerging issue under investigation. Therefore, interviews at the early project stages were concerned more with the formal organizational structure, mission, activities, responsibilities, and decisions. The longer the researcher remained in the organization, the more she could appreciate many of the above issues by purely observing behaviours and reviewing secondary information sources. Thus, interviews gradually became more structured and focused on risk perceptions and behaviours associated with ISS risk communications, decisions and incidents.

During interviews verbatim notes were taken, while the recorded responses were analysed as soon as possible, focusing on identifying new patterns, topics and directions of inquiry. Apart from the interview responses, the researcher would include into her field notes the behavioural response of the interviewees.

At this point it has to be noted that given the interactive intimacy of interviewing, data collection via this method often required a certain rapport to be built between the researcher and respondent, which would facilitate the required discussion openness. This was particularly so as interviews became more structured and

investigated topics in considerable detail. The required rapport was built up over the extended period of field work and the regular contact with the respondents, while the researcher consciously avoided communicating her own views.

In addition to one-to-one interviews, a number of focus group meetings were organized following operational incidents in order to obtain a rounded view of the incident, as well as to encourage participation from people reluctant to be interviewed on their own, or who felt they had nothing to say. Once again, behavioural responses of the focus group members were also considered.

With regards to questionnaires, these were utilized to assess workers' perceptions of risk, behaviours and decisions, as well as the appropriateness and effectiveness of ISS management controls. They were repeatedly completed by the same or additional respondents, in order to determine any changes in perceptions. In addition to scoring a particular questionnaire statement, respondents were encouraged to provide any further comments, elaborating their views.

Finally, in each organizational group an informant was identified who at different project stages helped validate the findings and the emergent concepts. This approach was particularly useful in assessing the political and cultural context, while identifying themes that would have to be further investigated.

3.4.4. Data analysis and presentation methods

Like any other longitudinal case-study research, this study involved a continuous 'learning process' of data gathering and analysis[140]. In addition, given the contextualist analysis approach of this research, information was collected and analysed across a number of levels of analysis as well as over time. The various themes and issues identified from the collected primary and secondary information sources were categorised on basis of the analysis levels identified in Table 3.4.

Such a *layered method* of analysis has been supported by a number of scholars[141], suggesting that not only can it provide an in-depth description of the environment under study, but also it can increase model predictability. By investigating the interactions of various parameters across different levels of analysis (i.e. Table 3.4) and by including the time dimension as a systematic focus of the analysis, the

[140] I.e. Horlick-Jones et al, 2003.

[141] I.e. Breakwell and Barnett, 2003; Pidgeon, 1999.

relationships of constructs can be investigated at one time and over time. Therefore, data analysis of this research was focused on the examination of both coterminous and sequential change.

The interpretation of the research findings was undertaken in line with the ontological and epistemological assumptions of this research, thus aiming to generate meaningful principles which can be applied in other settings.

As for the credibility of the data analysis and transferability of interpretations these were operationalised via the prolonged engagement in the field and the triangulation of data sources (i.e. Lincoln and Guba, 1985).

Finally, with regards to the presentation of the collected and analysed data this was done through the use of narratives - specific to the various project phases. Such narratives focus on the contextual settings of the organizational process of ISS management, as well as provide an in-depth description of ISS incidents and their impacts. The narratives are augmented by tables and figures.

3.5 Conclusion

The main contribution of this chapter is to present clearly the research argument and the researcher's sociological and philosophical beliefs and assumptions that guide the choice of theoretical perspective and methodology.

This chapter stresses that organizational encounters with risk and ISS management processes of change are characterised by complex and dynamic social interactions. Such interactions require to be investigated across various levels of analysis, while the associated relational rules need to be understood within their contextual setting and over time.

Therefore, this chapter argues in favour a contextualist, layered approach to interpreting ISS and risk management, which is driven by empirical investigation. The following chapter presents the empirical findings of this study.

4. Empirical Findings

4.1 Introduction

The in-depth case study described in this chapter concerns the lifecycle of the A2004 Games-ISS project, which aimed to design, build and operate a highly reliable ISS management solution for the A2004 Olympic Games.

As presented earlier, the case study investigation was a longitudinal one, commencing with the data collection approximately four months prior to the formal initiation of the A2004 Games-ISS project and continuing throughout the project's lifecycle to event-time and project conclusion. Therefore, the environment under study was one of continuous change and increasing maturity[142] across various levels, with the Games-ISS project aiming to deliver by event-time a highly reliable ISS management solution. Indeed, it was this process of organizational change and the organization's mission and strategy that led the researcher to choose this case study. The analysis of the changing formal and informal organizational structures[143], activities and context provides insight into the delivery and management of highly reliable ISS.

This chapter presents the organizational scope, structure, socio-political and technological context that determined the event organization's capacity to deliver highly reliable ISS. These factors are examined within a wider contextual and organizational level, taking into consideration the impact of/on the greater A2004 Games-IS Integration project and A2004 Games Event.

Thus, section 4.2 utilizes Mintzberg's (1979) scheme of organization structural context to describe the Olympic and A2004 Event organization, and the A2004 Games-IS Integration project organization. The A2004 Games-IS processes and infrastructure are presented along with the growing significance of the ISS management function and associated project. Section 4.3 presents an analysis of the

[142] The term '*maturity*' in this research draws from Weick and Sutcliffe's (2001, 2007) work of organizational and operational mindfulness. The authors suggest that controls of mindful/highly-reliable organizing are classified into varying categories of maturity, ranging from 'non-existent' (immature) to 'existent' (mature) (i.e. Appendix-A10).

[143] The term '*formal*' organizational structure and controls refers to the fixed set of rules of intra-organizational procedures that govern the ways in which collaboration and coordination will serve one (or more) common goal. The '*informal*' organization is the natural means to augment the 'formal' organizational structure, communications and controls (i.e. Dhillon, 2007:3-5), and it is the dynamic and interlocking social structure that governs how people will work together in practice.

case study. It uses the conceptual framework developed in section 3.3.2 in order to examine the delivery and management of highly reliable ISS. Section 4.4 identifies the emergent issues for discussion, and section 4.5 concludes the interpretation of the ISS management practices in the A2004 IS-Games project organization.

4.2 The organization and project contextual background

4.2.1. The Olympic event organization and the A2004 Olympic Games

The parts of the Olympic event organization

The preparation and running of any Olympic Games event involves the contribution of a number of organizations, all of which are guided by the *Olympic Charter*. The latter is the codification of the fundamental principles of Olympism, rules and bye-laws adopted by the International Olympic Committee ("IOC"), governing the organization, action and operation of the 'Olympic Movement'[144].

The five main constituents of the Olympic Movement are the IOC, the temporary Organizing Committees for the Olympic Games ("OCOGs"), the International Sports Federations ("IFs"), the National Olympic Committees ("NOCs") and the National Sport Federations ("NSFs").

All the above organizations within the Olympic System are non-profit ones according to the laws of the country where their headquarters are located. However, over approximately the past twenty years, the Olympic Movement has been increasingly confronted by four other types of actor whose legal nature is different. These are depicted in Figure 4.1 below.

[144] According to the Olympic Charter (IOC, 2007:11), "Olympism is a philosophy of life, [...] blending sport with culture and education", while "the goal of Olympism is to place sport at the service of the harmonious development of man with a view to promoting a peaceful society concerned with the preservation of human dignity".

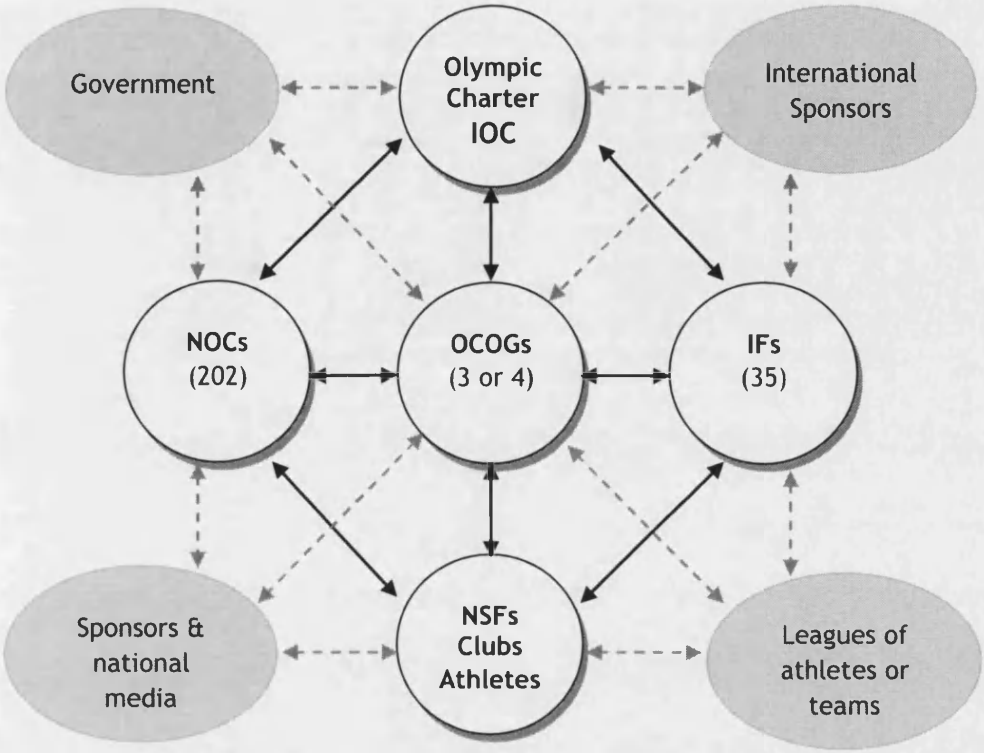


Figure 4.1: *The Olympic System and the new actors encircling it* (Source: adapted from Chappelet and Bayle, 2005:19-21).

Utilizing Mintzberg's scheme of contextual analysis (i.e. Table 3.1) for the Olympic organization and System, the Olympic System's ***ideology*** is summarised by the objectives of the Olympic Movement. The majority of the Olympic constituents - particularly those that work at the top - work voluntarily with their main goal the performance of their mission. They thus have members and stakeholders rather than customers and clients; they depend on many volunteers, and usually have a two-level governance made up of elected officials and hired managers. As such, they are often more open to public scrutiny than profit-focused companies.

However, most Olympic sport organizations have progressed from an administrative logic to a marketing approach and then to a strategic one.

> "The strategic and performance management approach aims to define a project, to structure it in a way that will permit it to be successful, and then to evaluate it once it is completed in order to draw useful conclusions for the continuation of this project or development of new ones" (Chappelet and Bayle, 2005:ix).

This shift in management approach has been led by the IOC, which has increasingly identified the need for sustainable and performance-controlled Olympic Games.

According to IOC's Director of Technology,

> "costs have been steadily increasing over the past 15-20 years, and it seems that each OCOG is aiming to outperform the previous one in scale and services they provide. This is not the goal of the IOC. We do not want Olympic projects to creep into something we cannot manage. [...] The growing size of the Games has made it imperative for us to seek the expertise and economic assistance of our sponsoring partners. But sponsorships do not come easy. We need to provide sustainable Olympics, transfer knowledge and resources from one event to the next - which we haven't done as much as we needed to in the past. Our role in the IOC is to ensure that all necessary services and infrastructures are in place for the Games. Beyond that, anything additional has to remain manageable and not jeopardise the entire project" (i.e. Appendix-A3:1).

Understandably, the Olympic marketing programme has become the driving force behind the promotion, the financial security, and stability of the Olympic Movement. The latter generates revenue through broadcasting, The-Olympic-Partners (TOP), domestic sponsoring, ticketing, and licensing.

With regards to the ***operational core*** of the Olympic System, the IOC has no financial responsibility whatsoever in respect to the Games' organization and staging. It merely governs the organization and operation of the Olympic Movement, stipulating the conditions for the celebration of the Games. The organization primarily responsible for the operational functions of the event[145] and the preparation and organizing of the Games is the OCOG. Among others, the OCOG is responsible for the sourcing of volunteers - an integral part to the hosting of any Olympic Games. Volunteers are utilised across a number of technical and operational support positions, while their training depends on their allocated responsibilities. In addition to the OCOG, the NOCs and IFs will assist by specifying the rules of and requirements for the hosting of each sport event, and the TOPs will provide their know-how and technology to support the Games' operational services.

[145] For more information on the operational functions of an Olympic Games see Theodoraki (2007).

The ***technical and support staff*** of the Olympic System is comprised by professional workers that are sourced from a number of organizations such as the TOPs and various IOC subsidiary organizations[146].

The Olympic System organizational actors identified above were also evident in the case of the A2004 Olympic Games under study. The Athens 2004 OCOG was that of ATHOC, while the Athens Olympic Broadcasting (AOB) was the Host Broadcaster of the Games. The AOB produced the international television and radio signal of the Games, delivering it to the venues and the International Broadcasting Centre (IBC). The AOB also provided the broadcast services and equipment to the various IOC broadcasting partners, such as the NBC and CBC networks.

The TOP sponsors included among others Kodak, Xerox, SchlumbergerSema (later Atos Origin), Panasonic, Samsung and SWATCH. The National Sponsors were relatively limited in the A2004 Games, owing to the small size of the domestic economy.

However, as argued earlier (i.e. section 3.2.2) and as Mintzberg's (1979) scheme of organization contextual analysis suggests, although an organigram may show the division of labour and how authority flows among divisions, it does not capture informal relationships and does not necessarily show work flows either.

[146] IOC subsidiary organizations include the OBS and OGKS.

The Olympic Event and the A2004 project phases and functions

As stated above, the most critical organization in the planning and delivery of an Olympic Games event is that of the OCOG. It utilises the IOC's project management framework of the *Masterplan* in order to coordinate work activities across the numerous partners and divisions. A temporary organization in nature, the OCOG's planning processes evolve to match the tasks at hand. Table 4.1 summarises the project phases and activities. These also applied to the case of the A2004 Games.

Table 4.1: *(A2004) Olympic event project phases, activities and outputs.*

	(A2004) Project Phase	Activities
1	***Foundation Planning phase*** (Games-98 to Games-66 months)	This phase initiates when the host city is selected. The board is formed, top management staff is recruited, the need for Games-related legislation is identified, corporate governance structure is selected, and the image of the Games is envisioned.
2	***Operational Planning phase*** (Games-72 to Games-12 months)	The OCOG progressively creates more detailed planning for the Games operations, which aims to move the organization towards a state of readiness to deliver the Games. The focus is on functional planning, although gradually moving to a venue-based focus.
3	***Test-Event Planning phase*** (Games-20 to Games-10 months)	The OCOG and its partners test its Games-time preparations. This involves planning to conduct venue-based test events. The focus is shared between functions and venues. Feedback and lessons learned from these events are incorporated into the Games planning documents.
4	***Operational Readiness Planning phase*** (Games-12 to Games-1 month(s))	Simulation exercises and rehearsals take place across functions and venues. The focus is increasingly becoming venue-based.
5	***Operational phase*** (Games)	During a period of approximately 2 weeks, the Games are executed and the focus is venue-based. Few functions retain a central management and monitoring capability. In A2004 the Games took place on the 13-29 August 2004.
6	***Dissolution phase*** (Games+12 months)	Venues are reinstated to their owners. The OCOG is dissolved, and any assets are liquidated.

There were 53 functional areas in the A2004 Organizing Committee (ATHOC)[147], where each had to include in its functional plans the scope and level of service along with elements of time, resource, budget, and (workforce or volunteer) training planning. Plans were communicated among functions in order to identify interdependencies, risks and issues, supporting the integration process.

According to ATHOC's Director of Technology,

> "by reviewing each other's plans, the entire organization is being educated on the operations necessary to run an Olympic Games. [...] Appreciating the scale and complexities of a project such as the hosting of a Games event requires a lot of time, structured communications and coordination. Before each function understands what it needs to do, it has to appreciate the greater picture; and that is not an easy task. This is where the transferred IOC knowledge can come in handy. It is unfortunate that the IOC transfer of knowledge programme did not initiate prior to the Sydney Games in 2000" (i.e. Appendix-A3:24).

As the OCOG organization moves to a venue-based focus[148], similar to the functional plans, the venue operating plans bring together and integrate the operations of each functional area required to operate the venue. This is also when volunteer requirements are specified in greater detail. In the case of the A2004 Olympic Games the venues were 60 in total, 35 of which were competition venues, hosting a total of 28 sports, or 300 sport events.

According to the Games-IS Chief Integrator(i.e. Appendix-A3:9), as an OCOG and its partners move from one project phase to the next, higher understanding is secured given that the detail of operations and responsibility boundaries are made clear. Similarly, staff confidence gradually increases.

Utilizing Mintzberg's scheme of organization structural context, the key coordinating mechanisms, design parameters, and situational factors of the A2004 OCOG (ATHOC) are summarised by the researcher as in Table 4.2.

---

[147] I.e. Theodoraki E (2007).

[148] The shift to a venue-based focus and operations is known within the Olympic context as *'venuisation'*.

Table 4.2: *Athens 2004 Organizing Committee (ATHOC) organizational characteristics across project phases.*

Age	**Foundation Planning phase** (G-98 - G-66 months)	**Operational Planning phase** (G-72 - G-12 months)	**Test-Event Planning phase** (G-20 - G-10 months)	**Operational Readiness Planning phase** (G-12 - G-1 months)	**Operational (Games) phase**	**Dissolution phase** (G+12)
Size	Medium	Medium	Medium	Large	Large	Small
Environment	Simple/dynamic	Complex/dynamic	Complex/ relatively stable	Complex/ relatively stable	Complex/ relatively stable	Simple/ stable
Resource Dependence	High	High	High	High	High	Moderate
Power	High external control	High external control	High external control	High external control	High external control	High external control
Strategic Capacity	Low	Low	Low	Low	Low	Low
Job Specialization	Little	Moderate	Moderate	Great	Great	Little
Unit Grouping	Functional-based	Functional-based	Functional- & venue-based	Functional- & venue-based	Venue-based	Functional-based
Liaison Devices	Few	Moderate	Many	Many	Few	Few
Behavioural Formalization	Little	Moderate	Much	Much	Moderate	Little
Centralization	Centralization	Some decentralization	Some decentralization	Decentralization	Decentralization	Selective decentralization
Training	Little	Some	Some	Much	Little	Little
Basic Organizational Part	Strategic apex	Strategic apex/ operating core/ technical staff	Technical staff/ operating core	Technical staff/ operating core	Operating core	Technical staff/ operating core
Basic Coordination Mechanism	Mutual adjustment	Standardization of outputs	Standardization of work processes	Standardization of work processes	Mutual adjustment	Standardization of outputs

4.2.2. The A2004 IS organization and the Games-IS Integration project

One of the functional areas of the A2004 Games organizational system was that of information technology. This involved the implementation and operation of two separate solutions. The purpose of the first, labelled *Admin-IS*, was to support the Games' administrative and preparation activities by ATHOC and its partners.

This IS came into existence soon after the establishment of ATHOC, approximately seven years prior to the A2004 Games. The IT solution and respective organization was developed ad-hoc by ATHOC personnel in order to meet the organization's needs at the time. The Admin-IS was exclusively managed and monitored by the ATHOC IT Department personnel.

The second IS solution, which is the one this research focuses on, was labelled *Games-IS* (or Games-network), since it was deployed during the Games. The key functions of the Games-IS involved three mission-critical IT-enabled services:

- the support of planning and operation activities related to a number of ATHOC Games management functions, such as accreditation, sport entries and qualification, transportation and accommodation schedules, medical encounters reports, protocol for VIP activities, arrivals and departures, and staff and volunteer management;
- the capture of the Olympic sport competition timings and scores, and their on-venue communication;
- the diffusion of Olympic Games event information, including the real-time delivery of competition results and athlete information to commentators, and the provision of related information to the media, athletes, judges, coaches and sponsors via on-site kiosks.

The Games-IS solution constituted a major IS integration project, where a number of partners and functional teams had to coordinate their activities to deliver and operate the end solution during the 17 days of the A2004 Games event. The IS-Integration project started approximately 3.5 years in advance of the Games. The organization responsible for leading the integration and project management, as well

as managing the IT operations, was the IOC's information technology TOP sponsor, SchlumbergerSema[149].

The Games-IS objectives, processes and solutions

According to the SchlumbergerSema Games-IS Chief Integrator, the objective of the Games-IS Integration project is

> "the seamless integration of Olympic technologies, processes and people, delivering high quality Olympic services and results. [...] This is a highly visible project, and the services we support are critical to its success. We get no second chance. The project end date does not move. The performance cannot be compromised. We must succeed. The solutions we develop, integrate and operate have to be reliable and available throughout the duration of the Games.[...] The one thing that absolutely cannot happen is that competition is interrupted" (i.e. Appendix-A3:9).

As suggested above, the role and responsibilities of SchlumbergerSema was not merely that of system integration. The key IS services expected of the TOP IT sponsor included: partner management; systems integration; change control; information security; and Olympic operations (i.e. Appendix-A4).

In addition, ATHOC and SchlumbergerSema had been directed by the IOC that "successful Games mean reliable Games, without increasing their complexity and cost" [150](i.e. Appendix-A3:1). The IOC urges its TOP sponsors to demonstrate ways of cost containment through the transfer of knowledge and the reuse of past-event technologies. Therefore, in terms of IS solutions and services, a successful Games is not only one that demonstrates high reliability, but also cost and resource effectiveness and efficiency.

---

[149] In September 2003, Schlumberger Ltd. sold the majority of its SchlumbergerSema business to Atos Origin, including the Major Events Division. However, the change of executive management, corporate logo and marketing strategy of the IOC TOP sponsor did not take effect until January 2004, when the business deal was finalised.

[150] The budget allocated to the preparation and operation of the Olympic Games IT infrastructure has steadily increased over the years, currently being the second greatest cost after the construction of Olympic venues. In 2002, the IOC IT Director estimated the GAMES-IS cost of a Summer Olympic event to start at approximately $400 million.

As suggested in Appendix-A4, the eventual A2004 Games-IS solution was a complex one, of great size and many interfaces and service dependencies. The IT-supported processes to be delivered by the Games-IS solution could be best understood through a brief presentation of the three main systems and their applications deployed on the Games-network (i.e. Table 4.3). A high level architectural diagram showing the data flows between the Games-IS systems can be found in Appendix-A5.

Table 4.3: *The systems and applications deployed on the A2004 Games-network.*

A2004 Games Systems	Description
Results System	The system supporting the results transmission process. It was divided into two subsystems: 1. There was one *Timing and Scoring (T&S)* system for each A2004 sport (28 in total), which was responsible to capture all data from different types of devices at the competition venues, as well as all manually entered data. 2. The *On-Venue Results (OVR)* system, running at each of the competition venues, collected T&S data in order to calculate results of each sport event, and then distributed the results to other systems in various formats. Results data was distributed in two different ways: (a) real-time to the Commentator Information System; TV Graphics, and Scoreboards; and (b) non real-time to the Central Information Repository, Print-Distribution, Results Distribution, Info2004, and Internet Data Feed. The design, development and operation of the Results Systems were the responsibilities of Olympic A2004 Sponsor, SWATCH. The Results Systems interfaced (pushing or pulling information) with 11 other applications.
Information Diffusion System (IDS)	The IDS gathered and distributed event-related information to multiple clients. The information had to be accessed: - on line from hundreds of information points located across the Olympic venues; - by members of the Olympic Family at venue-located kiosks; - real-time by commentators (i.e. information about the competitions in progress); - by journalists who received official result printouts at their desks; - by Press Agencies at the Media Centre. - by the INFO-2004 application which published information received from different subsystems. Overall, the IDS consisted of six applications, while these interfaced with 28 other applications.

Games Management System (GMS)	The GMS assisted in the gathering of information about the people attending the event and their needs. It was divided into several loosely coupled, departmentalized applications, whose utilization started prior to the Games. GMS applications included and supported functions such as: accommodation; accreditation; arrivals & departures; medical; sport entries and qualification; staff information systems; staff scheduling; and transportation. The GMS system interfaced with 24 other applications.

The Games-IS applications had been re-used from previous Olympic events, although certain attribute and interface adjustments had to be completed in order to accommodate the evolving needs of the Olympic System organizations.

As the SchlumbergerSema/Atos Origin Major Events Marketing Vice President suggested,

> "the Olympics are not an opportunity for us to showcase innovative technology. We want to deliver a reliable solution on time; and we want to minimize risk and cost. This is why we do not re-invent the wheel[151]. The technology that supports the applications of the Games network has been used and tested before. We are merely adjusting this to new requirements. [...] The only area in which we use the latest most innovative technology is monitoring. There, we want the best there is. This is where we spent most of our budget - monitoring solutions; and of course testing. We test and re-test. We probably spend more than 80% of the project's time on testing. The risk-taking is disproportionate to the amount of time we spend testing" (i.e. Appendix-A3:79).

Indeed, in the A2004 Games-IS Integration project the majority of time and resources was spent on testing, since systems were developed by different teams or organizations, supported by different technologies and vendors, and required the controlled management of their overall procurement, integration, and support.

[151]IBM, the IOC TOP IT sponsor prior to SchlumbergerSema/Atos Origin, faced problems during the Atlanta 1996 Games when their innovative IT generated athlete information inaccuracies. IBM was forced to issue a public apology after this incident, and opted not to renew their contract with the IOC.

Therefore, from the above analysis it is evident that the Games-IS solution was one of great scale and complexity, with a variety of project challenges. As the Games-IS Chief Integrator suggested "the Olympic Games project is the school of project management. There is no learning ground quite like this one" (i.e. Appendix-A3:82).

Meanwhile, the SchlumbergerSema Major Events Marketing Vice President seemed to recognize that "aside from the strong technological element of the Games IS solution, the success of this project is primarily dependent upon people and processes. Humans are vital, and all these people working together are like an orchestra. Technology should hum away tunefully and effectively in the background" (i.e. Appendix-A3:92).

Hence, understanding the organizational context and business requirements, while finding effective ways to coordinate and manage work activities, resources and risks, are all vital to the success of such mega-project IS endeavours.

In the case of the A2004 Games, the organizations involved in the design, implementation, testing and operation of the Games-IS are summarised in Appendix-A6.

The coordinating mechanisms of the Games-IS project organization

In the diverse, complex and tightly coupled A2004 Games-IS organizational structure and technological solution, coordinating work activities, labour and resources were key to the success of the project.

The Olympic ideology united diverse teams and individuals and helped towards establishing common beliefs and organizational objectives (i.e. ***standardization of norms***). Partnering organizations were not contractually bound with one another; however a clear and mutual need for a reliable end product and operations drove teams towards coordinating their activities.

In addition, the strict project time schedule and the great level of deliverable interdependency put great pressure on teams to avoid delaying decision-making and solution implementation. Teams often had to comply with dominant project directions, not due to mutual agreement, but because of the common understanding that any issues and problems would surface - and ideally corrected - during the long solution testing and re-testing phase of the project.

Therefore, Games-IS project tasks were coordinated primarily through the ***standardization of outputs***, which was achieved through a long process of repetitive and extensive testing, as well as the compliance to the ATHOC-managed *Masterplan*. Orders were rarely given in the Games-IS project organization. SchlumbergerSema/Atos Origin, the Games-IS Integrator and Games Operations Manager, did not have contractual superiority and power over other organizations of the Games-IS organization (i.e. Appendix-A4). As suggested by the Atos Origin Games-ISS Manager,

> "in this project organization policies and procedures cannot be enforced similar to a big corporation. We have a consortium of partners with which we have no contractual relationship. When we issue a policy we cannot say 'my way or the highway'. [...] We have to convince our partners of implementing our policies. We have to test and monitor their performance. We can never take anything for granted. [...] We also need to understand who matters the most in this project. We are not working for our IT partners. In all honesty, we are not even working for ATHOC or the IOC. We are working for the broadcasters since they are the ones that generate the greatest Olympic revenue" (i.e. Appendix-A3:66).

Furthermore, as the Games-IS Chief Integrator suggested "undoubtedly the most significant task and phase of this project is the testing. [...] The design and implementation of the solution takes little time compared to the time and resources we spend on testing. [...] This is the most critical success aspect of the project. Detecting solution defects, understanding what is normal, and managing changes in a controlled manner is what the success of the Games IS most depends upon" (i.e. Appendix-A3:74).

Indeed, testing was conducted across various solution levels, from the IT components to the organizational procedures and staff operational readiness. The aspects of A2004 Games-IS testing are summarised in Table 4.4.

Table 4.4: *A2004 Games-IS testing strategy*

Type of Games-IS Testing	Description of Testing	Timing of Testing
Unit/Standalone Testing	Conducted for each Games-IS application and completed by the application provider.	Games-24 to -16 months
Interface Testing	Conducted for each Games-IS application interface and conducted by the application provider and systems integrator. It intended to verify the uninterrupted and unchanged information communication between applications.	Games-16 to -14 months
End-to-End Testing	Tested each logical flow of the system, verifying that all required and expected outputs occurred. Normal and abnormal cases were tested. Conducted by the application provider and systems integrator.	Games-14 to -12 months
Homologation Testing	Involved user acceptance tests, where the IOC and IFs verified that all application and systems outputs were as required. Actual events were simulated to ensure the results system conformity to the running of real, live events.	Games-12 to -8 months
Test-Events (TEs)	Pre-Olympic events at the Olympic venues started 1 year prior to the Games. The real, live events acted as tests of system performance and functionality.	Games-12 to -2 months
Technical Rehearsals (TRs)	Involved system testing to breaking point, focusing on capacity testing, abnormal scenarios, fail over tests, exception cases, and overall readiness of systems and people. TRs were organized and conducted by the systems integrator and application provider.	Games-4 to -2 months

However, aside from focusing on the outputs, further coordination mechanisms were evident in the Games-IS project environment. The Games-IS Chief Integrator highlighted that

> "most of the staff on the Games-IS project is young, inexperienced workers. They have the basic necessary knowledge to do their job, but they learn even more on the job; and we encourage this by supporting a culture of team-work and transfer of knowledge. Our workers have to work with one another, and due to the nature of the project they also have to get involved in what others do, too. We also have approximately 30 to 40 people on the team that have

> worked on previous Games, who act as mentors to younger or Olympic-inexperienced staff. [...] In contrast, perhaps, to any other conventional organization, in the Games we encourage people to work and talk with one another. [...] Informal communications are very important to the project. This is how the staff creates a working relationship with one another, and finds out about the problems and progress of other teams" (i.e. Appendix-A3:77).

Therefore, ***standardization of skills*** and mutual adjustments through the process of ***informal communications***, were two further mechanisms of work coordination in the Games-IS project organization.

The design parameters of the Games-IS project organization

The organizational design of the Games-IS project was closely aligned to the five services provided by the Games-IS Integrator, as in Appendix-A4. An organigram of the Games-IS project organization is available in Appendix-A7, indicating the organizational ***job specialization***. Given that this was an IT solution project, most staff had a strong technical background, although across different technological areas. In most cases, managers too had a technical background, but primarily more senior or Olympic experience, often operating as mentors for their younger or inexperienced team members.

As suggested earlier, it is interesting to note that the operating core of the Games-IS Integration project team consisted of primarily young, Olympic inexperienced staff. The average worker of the Games-IS staff was in their mid/late twenties, while for 28% of the staff this was their first ever job. Olympic experienced workers - operating as mentors for their inexperienced colleagues - amounted to 12% of the staff.

During the initial design and implementation stages of the project, technical staff were greatly focused on their responsibilities and team activities. However, as the project progressed and moved to integration, testing and operational phases, the focus changed from functional to venue-based and operational, and project workers increasingly interacted with other teams as well as their own team members.

This gradual change in job specialization and focus also affected the ***behavioural formalizations*** observed in the project organization. Job descriptions and responsibilities did not change formally, but rather more organically, according to the project phase and demands. It is worth noting however at this point, that

restlessness was observed among project workers as the project progressed. The reasons suggested for this by a number of project staff was the speed of organizational change - from the physical location of work to the exponential growth of teams - along with the increasing levels of performance pressure.

As suggested by one of the Games-IS Network Administrators during a project phase of increasing venuisation[152], "the organization changes so quickly that it almost feels like there is no organizational history - this organization has no resemblance to how it was 6 months ago. I have never seen this before. The atmosphere may be relatively casual and informal, yet lately everything has been changing so fast, that everyone is feeling increasingly restless." (i.e. Appendix-A3:78).

The above interview statement is not only indicative of the behavioural formalization mechanisms and ***liaison devices*** in the A2004 Games-IS project organization, but also of the ***unit groupings and size***. Figure 4.2 below shows the size of the integrated Games-IS project organization from its creation to its dissolution. More detailed data can be found in Appendix-A8.

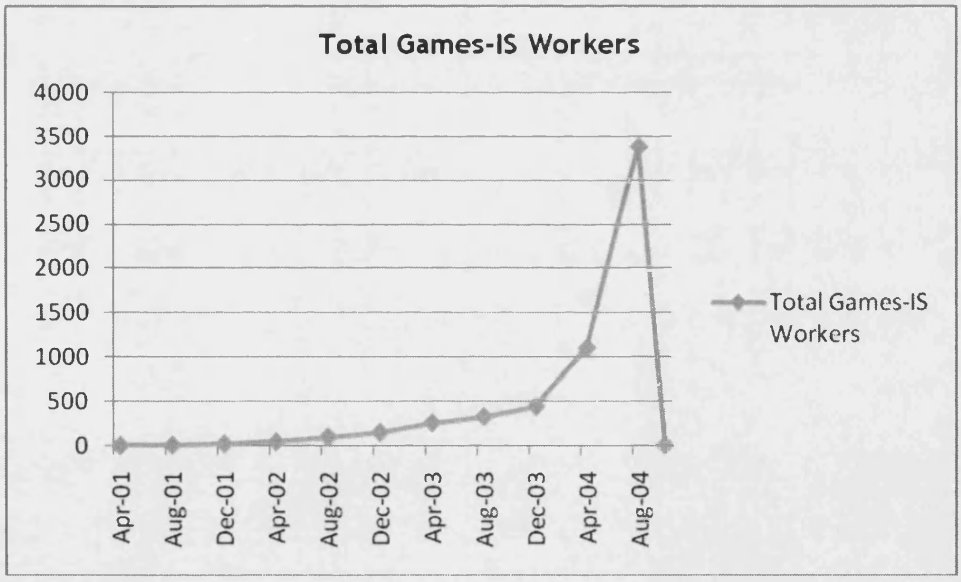


Figure 4.2: *Number of Games-IS project organization workers during project lifespan.*

[152] The term 'venuisation' is one used within the Olympic Games context to refer to the preparations involved in moving operations from the central OCOG headquarters to the Olympic competition and non-competition venues.

With regards to the ***training*** of the Games-IS personnel this was conducted only prior to major Test-Event and operational phases of the Games-IS and organization. From Figure 4.2 it is evident that training became increasingly challenging as Games-time approached. Not only did the number of Games-IS staff greatly increase prior to the Games, but also the number of IT volunteers - from a few dozens in August 2003 to over 2300 in August 2004. In addition, it is worth noting that by Games-time the Games-IS staff included over 46 nationalities.

Formal training involved the communication to all paid-staff and volunteers of role-specific operational policies and procedures. However, the majority of knowledge obtained and communicated throughout the project lifecycle was done tacitly, via the experience obtained from repetitive operational testing, and the mentoring provided by Olympic experienced managers and supervisors.

Finally, Games-IS work activities were ***planned and controlled*** according to the project *Masterplan* (managed by ATHOC), while levels of ***decentralization*** increased as the project progressed to Games-time and workers moved to the venues (i.e. venuisation). However, in contrast to most other ATHOC functions, the IT operations were to a great extent managed and monitored centrally - from the Technology Operations Centre (TOC). This was done in order to consolidate events and information from across the competition and non-competition venues, and thus efficiently allocate required resources - especially in the case of a crisis.

The situational factors of the Games-IS project organization

As indicated above, as the project progressed the organization quickly grew in **size** - particularly towards the later stages of the project. Such steep growth often led to personnel restlessness and stress, and in fact increasing personnel turnover rates. The IOC Director of Technology suggested that "this is a frequent phenomenon and project challenge. The image of the Olympics will attract a lot of workers - particularly younger ones. However, the Games project is one with an expiry date, and soon Olympic personnel will start looking for other jobs. This phenomenon is more evident as Games-time approaches, and this is a considerable project risk as workers who leave will be difficult to replace at the last minute. Most importantly it will be difficult to train a new worker since a lot of the knowledge obtained is tacit and learned from experience in the Olympic environment" (i.e. Appendix-A3:1).

It is not, however, only the size of the project organization that changed within a short timeframe, but the overall ***environment*** of the organization. Throughout the

project lifecycle the levels of organizational complexity and dynamism changed and peaked during the period of Technical Rehearsals (TRs), when the technology was fully integrated, pushed to its limits, and personnel and procedures were tested for operational readiness under extreme conditions. Almost two months prior to the Games, the environment became more stable, roles and responsibilities more clear, and the technology - relatively - fixed.

However, as Games-time approached, the visibility of the event increased to the outside world. This was partly due to an increased interest by the media, but also due to the increased marketing and promotion efforts of the Olympic sponsors, vendors and partners. Potential customers and journalists were regularly invited to the Olympic venues and Games-IS working premises to attend solution and corporate marketing presentations. In fact, it was commonly observed that prior to Games-time most Games-IS managers spend considerable of their time hosting their visitors, and otherwise only dealt with operational emergencies.

An observation worth noting, is that given the above mentioned increased media visibility and the increased job uncertainty after the completion of the Games, the Games-IS project environment became more ***political***, with tensions often witnessed within and between teams. Among others, this involved new structures of blame allocation when problems emerged.

The A2004 Games-IS project phases, activities and outputs

The A2004 Games-IS Integration project - managed by the TOP IT sponsor SchlumbergerSema/Atos Origin - adopted a typical design, build, test and operate approach. The project phases and activities are summarised below in Table 4.5. The characteristics of the associated project organization across project phases is summarised in Table 4.6, indicating the processes of organization structural and contextual change.

Table 4.5: *A2004 Games-IS Integration project phases, activities and outputs.*

	A2004 Games-IS Project Phase	Activities
1	***Project Initiation phase*** (April 2001 - August 2001)	This phase initiated with the recruitment of the project senior management staff, sourced from the TOP IT sponsor. The key ATHOC project-related personnel were identified and the project *Masterplan* was jointly reviewed and agreed.
2	***Analysis & Design phase*** (September 2001 - April 2003)	The project integrator created increasingly detailed functional plans, identifying the required resources, related inter-dependencies and risks. Technology and process interfaces were identified and assessed. Risk strategy decisions were made with regards to the solution and process design.
3	***Implementation & Testing phase*** (August 2002 - December 2003)	The project integrator implemented the designed system and network solutions and tested the delivered applications with ATHOC, IOC and other partners. Testing involved delivery acceptance, standalone, interface, and end-to-end testing. ATHOC and the Games-IS integrator planned for the venue-based test events. The focus was shared between functions and venues.
4	***Operational Rehearsals phase*** (August 2003 - June 2004)	Simulation exercises and rehearsals took place across functions and venues. Testing involved homologation testing (i.e. Table 4.4), venue-based Test Events and simulated and/or real operational stress tests. Detected defects were corrected via a controlled change management process. The focus became increasingly venue-based.
5	***Operational phase*** (July 2004 - August 2004)	The Games-IS was fixed approximately 50 days prior to the Games, and the venues and network went live (i.e. 24x7 operations) 1 month prior to the opening of the A2004 Games. Operations were transferred to the venues, although centralized monitoring was conducted from the TOC. The A2004 Games event lasted 2 weeks (13^{th}-29^{th} August 2004).
6	***Dissolution phase*** (September 2004 - October 2004)	The venues were reinstated to their owners, in preparation for the A2004 Paralympics event. Lessons learned sessions were held over a period of a few days, where A2004 Games-IS performance was discussed and documented. After that, the A2004 Games-IS organization was quickly dissolved.

Table 4.6: *A2004 Games-IS organizational characteristics across project phases.*

Age	**Project Initiation phase** (G-40 - G-36 months)	**Analysis & Design phase** (G-35 - G-16 months)	**Implementation & Testing phase** (G-24 - G-8 months)	**Operational Rehearsals phase** (G-12 - G-2 months)	**Operational phase** (G-1 month - Games)	**Dissolution phase** (G+2 months)
Size	Small	Medium	Medium	Large	Large	Small
Environment	Simple/dynamic	Complex/dynamic	Complex/dynamic	Complex/dynamic	Complex/ relatively stable	Simple/stable
Resource Dependence	High	High	High	High	High	Moderate
Power	High external control	High external control	High external control	High external control	High external control	High external control
Strategic Capacity	Low	Moderate	Low	Low	Low	Low
Job Specialization	Little	Moderate	Moderate	Great	Great	Little
Unit Grouping	Functional-based	Functional-based	Functional- & venue-based	Functional- & venue-based	Venue-based	Functional-based
Liaison Devices	Few	Moderate	Many	Many	Few	Few
Behavioural Formalization	Little	Moderate	Great	Great	Moderate	Little
Centralization	Centralization	Centralization	Some decentralization	Decentralization	Decentralization	Centralization
Training	Little	Little	Some	Much	Little	Little
Basic Organizational Part	Strategic apex	Strategic apex/ operating core/ technical staff	Technical staff/ operating core	Technical staff/ operating core	Operating core	Technical staff/ operating core
Basic Coordination Mechanism	Mutual adjustment	Standardization of outputs	Standardization of outputs	Standardization of work processes	Mutual adjustment	Standardization of outputs

4.2.3. The A2004 Games-ISS organization and project

As covered in Appendix-A4 of this study, the delivery of ISS was one of the key Games-IS Integration project deliverables, aiming to protect the Games-IS infrastructure and operations from any undesired and/or uncontrolled phenomena which could impact the Olympic Games.

In fact, with the completion of the A2004 Games, senior members of the Games-IS organization suggested that one of the project's greatest success stories was the delivery of a risk-based secure infrastructure (i.e. Appendix-A3: 92, 95, and 96).

However, the strategic significance of ISS to the success of the A2004 Games-IS was not appreciated to that extent from the early days of the project. The initial '*METER*'[153] contract between the IOC and its TOP IT partner did not cover any ISS requirements. Neither did the initial contract and agreed *Masterplan* between ATHOC and SchlumbergerSema. As the IOC IT Director and SchlumbergerSema Chief Integrator[154] later suggested, it was the increased global security awareness at the aftermath of the 9/11 attacks that raised the agenda for ISS in the Olympic Games.

According to SchlumbergerSema's ISS Risk Manager,

> "in the Salt Lake Games we did not have enough time to strategically incorporate ISS into our design. The Games were only a few months after the 9/11 attacks. We only had enough time to add a few last minute security monitoring solutions; but no time to customize these. It was pretty much fire-fighting - and it was very costly and inefficient. [...] After the completion of the Games in Salt Lake we initiated discussions with the IOC and ATHOC about strategically incorporating ISS into the IT *Masterplan*. It was not until June 2002 that we officially approached ATHOC with an ISS vision for the Games" (i.e. Appendix-A3:4).

Therefore, contrary to other A2004 Games-IS aspects - where knowledge and technologies were transferred from previous Games - the objectives, plan and deliverables of ISS had to be defined within the A2004 context.

---

[153] *METER* was the contractual agreement between the IOC and SchlumbergerSema (and later Atos Origin) that specified the IT services to be sponsored by SchlumbergerSema along with the Olympic promotional opportunities and privileges that the IT provider would benefit from.

[154] I.e. Appendix-A3:1 and Appendix-A3:9 respectively.

The Games-ISS project was one that received little strategic direction from the IOC and ATHOC, and was primarily defined by the TOP IT sponsor and its hired specialists. In line with the IOC's direction to deliver reliable and sustainable IT solutions, the Games-ISS project was expected to protect the Games-IS assets, information and processes with the adoption of a risk-based, cost-effective approach. However, a definition of the Games ISS risks, principles, baseline and priorities were not pre-defined. These had to be collaboratively defined by the various Games-IS partners, while the Games-ISS project was overall managed and directed by SchlumbergerSema's/Atos Origin Games-ISS Risk Manager.

Therefore, similar to the greater Games-IS project, the Games-ISS service was one that required a thorough understanding of the organizational/project context, business requirements and functional priorities. The organizations involved to varying degrees in the design, implementation, testing, management and monitoring of the Games-ISS solution were similar to these presented in Appendix-A6. The group overall responsible of delivering and managing the A2004 Games-ISS was the SchlumbergerSema/Atos Origin Games-ISS function. Interactions with other groups included mainly other SchlumbergerSema functions, ATHOC, SWATCH, IT vendors, Olympic broadcasters, and IT volunteers.

Table 4.7 below summarizes the key Games-ISS project modules as these were defined by SchlumbergerSema across the project length. The TOP IT sponsor proposed a comprehensive security plan that considered risks and ISS management controls across three dimensions - namely processes, technology and people. The ISS risk management methodology suggested by SchlumbergerSema/Atos Origin was aimed to support the centralized view of the organization's 'Security Posture', therefore bringing value to the organization by improving ISS decision making, incident management and resource allocation.

Table 4.7: *The A2004 Games-ISS modules and vision.*

	Games-ISS Project Module	Description	Objectives & Approach	The Challenges
1	*ISS Processes*	ISS processes were envisioned to involve a mixture of controls associated with: • the establishment of a risk management methodology; • the creation and implementation of ISS policies and procedures; • the identification and management of legal, forensic and ethical issues.	The objective was to have an overall view of the Games-IS Security Posture. This was achieved via: • a combination of risk modelling and risk mitigation strategies; • an ISS risk decision focus on solution functionality and business criticality; • the implementation of ISS architectural principles; • the establishment and compliance monitoring of ISS policies and procedures; • the establishment and communication of ISS metrics and KPIs; • the implementation of a SIM solution.	• Limited knowledge was transferred from previous events with regards to Games-ISS processes and risks; • No available industry standards & best practices for such an organizational context; • ISS policy and procedure compliance could not be imposed upon partners that were not contractually bound with the Games-IS Integrator.
2	*ISS Technology*	ISS technology involved a mixture of preventive, detective and corrective controls across the following areas: • applications, systems and network infrastructure; • access controls; • physical and environmental security; • disaster recovery and redundancy.	The objective was to have a centralised and aggregated view of the entire Games-IS infrastructure, thus supporting efficient ISS monitoring and problem resolution. The approach taken included: • the integration of technological ISS controls as early as possible across applications, systems and networks; • the implementation of a SIM solution; • building in redundancy and eliminating single points of failure.	• The Games-ISS project initiated after all other Games-IS activities, including design and implementation. • The Games-IS was great in size, complexity and module interdependence. • ISS monitoring alerts had to be reduced to a manageable number.
3	*ISS People & Culture*	A secure organizational culture was envisioned to support a two-way communication between the ISS management and Games-IS workers via: • security user awareness; • role-specific security training; • security notices and feedback.	A secure culture was defined as one where all IS workers were familiar with the ISS policies and procedures that applied to their role, thus contributing to the maintenance of security, while reporting any ISS incidents and suspicious activity.	• Training had to be offered to a large number of IS-workers in a very short timeframe; • The majority of Games-IS workers was last-minute volunteers.

The coordinating mechanisms of the A2004 Games-ISS project organization

The lack of an A2004 Games-IS *Masterplan* that incorporated ISS at the outset of the Games-IS Integration project, the very limited ISS experience from previous events, and the relatively delayed initiation of the Games-ISS project, all resulted in increasing the challenge of coordinating ISS management efforts across the various concerned organizations. In fact, coordinating the Games-ISS project was not only challenging with regards to partnering organizations, but also across the various SchlumbergerSema functional groups.

Across the various Games-ISS project stages different organizational coordination mechanisms were utilised. Thus, upon initiation of the project a strategic vision and direction was collaboratively achieved through the *standardization of norms* across senior members of key project partners (i.e. IOC, ATHOC, SchlumbergerSema, SWATCH). The approach taken was one that did not merely focus on the implementation of ISS technical controls (as had happened in SL200), but also stressed the importance of auditable ISS policies, robust operational procedures and a security-aware organizational culture.

Once a draft Games-ISS project plan was created specifying the various A2004 ISS domains, roles and responsibilities, coordination was primarily achieved through the *standardization of work processes*, as per planning process requirements.

With the incremental implementation and testing of the Games-IS and ISS infrastructure, efforts were made to define 'normal' (i.e. expected and permitted) network activity, thus increasingly achieving coordination through the *standardization of outputs*.

Prior to the A2004 Games, the communication of policies and procedures, and the ISS role-specific training of all Games-IS workers, aimed to also coordinate teams through the *standardization of norms*, stressing the transversal nature and organization-wide responsibility for ISS.

As for operational and Games-time, activities were coordinated through the *standardization of outputs* - particularly among manual workers, while white-collar workers also coordinated their activities through a *standardization of skills*.

Throughout the project lifecycle, *direct supervision* by the Games-ISS team was limited only within the organizational boundaries of SchlumbergerSema/Atos Origin, where power structures and lines of authority were more clearly defined. However,

even in this context, direct supervision was not a particularly effective coordination mechanism. This will be further explored later in this chapter.

Finally, within the Games-ISS team, most activity coordination took place via informal communications and *mutual adjustment*.

The design parameters of the A2004 Games-ISS project organization

The majority of A2004 Games-ISS management tasks were completed by the Games-ISS team, which until Games-time was comprised solely of SchlumbergerSema/Atos Origin ISS specialists and professionals.

The ***job specialization*** among this core operating Games-ISS team was along the areas identified in Appendix-A7, and as summarised in Table 4.8.

Table 4.8: *A2004 Games-ISS core team job specialization*

	Games-ISS Area	Focus	Objective	No. of Skilled Staff
1	*Secure Network*	The secure design, implementation, testing and operation of the Games-IS network.	The objective was to establish and implement a number of ISS network architectural principles (i.e. aligned to risk; defence in depth; redundancy; least privilege; centralized, real-time management & monitoring).	2
2	*Secure Systems*	The secure implementation, testing and operation of the Games-IS systems.	The objective was to identify system vulnerabilities and mitigate associated risks. A tool to centrally manage and monitor all Games-IS systems was implemented.	2
3	*Secure Applications*	The security testing of all Games-IS applications.	The objective was to identify all application security vulnerabilities and configuration problems, assessing the associated residual risk.	1
4	*ISS Risk Management and Assurance*	The establishment and communication of a Games-ISS baseline, policies and procedures, training material and risk management methodology.	The objective was to establish a risk-based approach and methodology to Games-ISS that would raise security awareness; monitor ISS baseline and policy compliance; assess residual risks and security posture; and inform risk management decisions.	2

The team members had strong technical backgrounds and their jobs demonstrated vertical specialization, although during operational times they had to exchange knowledge and considerably support one another in their roles. The Games-ISS area that demonstrated less of a vertical job specialization and ***behavioural formalization*** was that of ISS risk management and assurance, adopting a more strategic, business-aligned approach to information security.

The Games-ISS team expanded in ***size*** prior to the A2004 Games, incorporating members of the ATHOC Admin-ISS team (i.e. Fig.4.3). This expansion took place in order to support the 24-by-7 operations during Games-time. During the Games, the expanded Games-ISS team (labelled as *TOC-SEC* team) was broken down to three subsequent teams (of six each), which covered the Technology Operating Centre (TOC) operational shift requirements. Each team was comprised by a mixture of Games-ISS and Admin-ISS members.

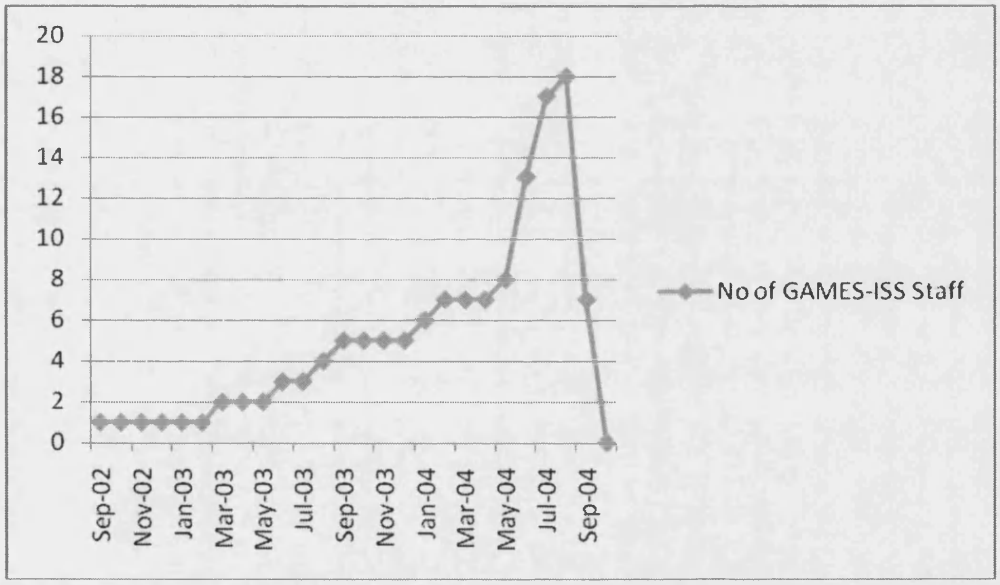


Figure 4.3: *Number of Games-ISS/TOC-SEC team members during project lifespan*

Prior to the A2004 Games all members of the TOC-SEC team were trained on the related ISS policies, operational procedures, technologies and methodologies.

ISS ***training***, however, was not only available for the TOC-SEC team. Job-specific ISS training was delivered to almost all - approximately 3500 - Games-IS workers. This training focused on ISS policies and operational procedures, and the efficient detection and management of ISS incidents during Games-time.

With regards to Games-ISS **planning and control systems**, these were far fewer in number and degree of formalization than for the rest of the Games-IS services. This was greatly due to the lack of prior Olympic ISS experience, methodologies and an IT Masterplan that incorporated ISS deliverables. However, the definition of a Games-ISS baseline at the early stages of the project, and the subsequent definition of architectural principles, ISS policies and procedures, operated as planning and control mechanisms. The definition and regular measurement of ISS metrics also operated as a performance control system. Overall, however, as the Atos Origin Games-ISS Manager stated,

> "it is the next Games that will benefit the most from the work our team has done here. We have already applied the Athens methodologies and lessons learned in Turin, and after that Beijing. This will save us time, money and effort. It will make a great difference" (i.e.Appendix-A3:95).

Therefore, given the lack of mature planning and control systems for the A2004 Games-ISS project, the utilization of ***liaison devices*** was critical for the mutual adjustment within and between Games-ISS units. Mentoring, physical proximity in the working environment, spontaneous discussions and meetings, and an overall atmosphere of team working, knowledge sharing and flat organizational structures assisted communications and the coordination of activities.

Finally, with regards to degrees of ***decentralization*** within the Games-ISS organization this was relatively low. Prior to the Games, ISS decision-making power remained primarily with the Games-ISS Manager, and in certain occasions with ATHOC. However, during Games-time decision-making remained with the Games-ISS team member that had the greatest expertise on the matter under consideration. Therefore, decision making during Games-time was decentralized as needed - especially in cases of crisis and incident management.

The situational factors of the A2004 Games-ISS project organization

Utilizing Mintzberg's scheme of organizational context levels (i.e. Table 3.1) it was also made evident that the degree of behavioural formalization in the Games-ISS organization depended on its ***size*** and ***project phase***. As ISS technology, policies and procedures matured, and ISS training was delivered to Games-IS workers, the ISS project organization became increasingly formalised. The same applied within the Games-ISS team as this expanded prior to the Games. In addition, going-live required

that decision making and incident management had to follow certain chains of command - although these were not inflexible.

In addition, as the Games-IS ***technological solutions*** matured they became increasingly fixed, and changes could be no longer implemented unless a strict change management procedure was followed. As such, the majority of IS(S) incidents during Games-time were in fact change requests.

Interestingly, an area where there was an evident change in organizational behaviours across project phases was that related to the ***power factors*** and ***environment*** of the organization.

The Games-ISS environment was one of great complexity at the early stages of the project due to the lack of previous Olympic knowledge, experience, and business requirements. This became increasingly clear, yet more dynamic controls had to be implemented within tight timeframes and touched upon every other changing and maturing aspect of the Games-IS solution.

However, what also changed was the degree of hostility (or friendliness) towards the Games-ISS project and team. As the objectives of the Games-ISS team became increasingly clear, their efforts to 'control' the Games-IS environment was often met with hostility and resistance, particularly by experts in other IT areas. In addition, it often appeared that ISS controls compromised the availability of Games-IS services, which generated considerable resistance from the Games-IS management as well.

Power struggles were, therefore, increasingly witnessed as ISS controls were implemented or resisted. These were once again reduced nearer to Games-time, when after a prolonged period of implementation and testing, problems were usually resolved and a common ground was found.

However, while power struggles across functions were gradually reduced, the opposite happened within the Games-ISS team. As the project approached its end, so did employment contracts, and team members were increasingly concerned with self-promotion and extending their contracts, often opposing or sabotaging the project contribution and actions of other team members[155].

[155] All above observations with regards to the parameters of organizational context will be further elaborated in sections 4.3 and 4.4.

The A2004 Games-ISS project phases, activities and outputs

Similar to the Games-IS project, the Games-ISS project adopted a design, build, test and operate approach. However, the lack of a Games-IS *Masterplan* that included ISS implied that during the first stages of the Games-ISS project a number of negotiations had to take place with regards to business ISS requirements, roles and responsibilities, project deliverables and approach.

In addition, the delayed initiation of the Games-ISS project compared to the IS-Integration one, resulted in a continuous effort by the Games-ISS team to catch up with the activities of the IS-Integration project, condensing the initial project phases and overlapping others (i.e. Appendix-A9).

The characteristics of the Games-ISS project organization across project phases are summarised by the researcher in Table 4.9, indicating the processes of organization structural and contextual change. Activities and challenges of the A2004 Games-ISS project with regards to identifying, making sense of, and reliably managing ISS risks are further explored per project phase in section 4.3 of this study.

Table 4.9: *A2004 Games-ISS organizational characteristics across project phases.*

Age	**Project Initiation phase** (G-26- G-23 months)	**Analysis & Design phase** (G-22 - G-12 months)	**Implementation & Testing phase** (G-14 - G-7 months)	**Operational Rehearsals phase** (G-12 - G-2 months)	**Operational phase** (G-1 month - Games)	**Dissolution phase** (G+1 month)
Size	Small	Medium	Medium	Medium	Large	Small
Environment	Complex/dynamic	Complex/dynamic	Complex/dynamic	Complex/dynamic/ occasionally hostile	Complex/relatively stable	Simple/stable
Resource Dependence	High	High	High	High	High	Moderate
Power	High external control	High external control	High external control	High external control	High external control	High external control
Strategic Capacity	Moderate	Moderate	Moderate	Moderate	Low	Low
Job Specialization	Little	Moderate	Moderate	Moderate	Great	Little
Unit Grouping	Functional-based	Functional-based	Functional- & venue-based	Functional- & venue-based	Venue-based	Functional-based
Liaison Devices	Few	Moderate	Many	Many	Few	Few
Behavioural Formalization	Little	Moderate	Great	Great	Great	Little
Centralization	Centralization	Centralization	Some decentralization	Some decentralization	Some decentralization	Centralization
Training	Some	Little	Some	Much	Little	Little
Basic Organizational Part	Strategic apex	Strategic apex/ operating core/ technical staff	Technical staff/ operating core	Technical staff/ operating core	Operating core	Technical staff/ operating core
Basic Coordination Mechanism	Standardization of norms	Standardization of work processes	Standardization of outputs	Standardization of work processes and norms	Mutual adjustment	Standardization of outputs

4.3 A2004 Games-ISS project empirical analysis

The previous section of this study presented the organizational structure and context of the A2004 Games-ISS and greater in scope Games-IS Integration projects. From this analysis it is evident that the two project organizations aimed to deliver clarity and reliability out of an organizational environment of great operational and technological complexity, uncertainty, and functional and partner interdependence. Thus, the project roadmaps considered in section 4.2 demonstrate the *changes* of the organizational situational factors, design parameters and work coordination mechanisms as these occurred across the various project phases. Yet, the question remains with regards to the processes and mechanisms of the above organizational changes, as well as the content of these.

Assuming that organizations represent socio-political communication networks (i.e. section 3.2.2), the researcher focused her data collection efforts on understanding the processes in which ISS risks were identified, assessed by the various Games-ISS project-related functions/groups, and eventually managed across the various project phases. The process of communication is considered key in understanding the Games-IS(S) project organization's capacity to achieve its business objectives, namely the reliable - and sustainable - operation of the A2004 Games-IS(S) infrastructure.

Therefore, the following section of this study focuses on the risk communication processes of the project organization under investigation, as well as the impact of such communication and management controls with regards to achieving highly reliable ISS operations. In order to link these processes and their impact to the organizational context, these are dynamically considered per project phase.

At this point it must be noted that since the ISS management of the A2004 Games IT infrastructure was the responsibility of the Games-ISS team, from a risk perception point of view, they were labelled as the ISS 'experts'. The rest of the Games-IS partners and teams that were directly or indirectly involved in the Games-IS encounter with ISS risks were labelled as ISS 'laypersons'.

4.3.1. A2004 Games-ISS project 'Initiation'

The A2004 Games-ISS project started over a year after the related A2004 Games-IS Integration project due to the untimely recognition by the IOC and ATHOC of the strategic significance of ISS services and management for the IS infrastructure of an Olympic Games event organization. As identified by the IOC's Technology Director

> "previous to the 9/11 terrorist attacks we had not considered the importance of information security. [...] We had never before included information security in the IT *Masterplan*. [...] After the 9/11 events we found ourselves asking our IT partners and the various OCOGs if they had done enough to avoid security incidents that would interrupt and compromise the Games. We never received conclusive answers" (i.e. Appendix-A3:8).

Following such an increased appreciation of a strategic approach to ISS management in the Olympic Games, the IOC directed ATHOC and the rest of its technological partners to address jointly issues of ISS. Given the lack of ISS expertise on a strategic, technology-integrative level across the IOC and ATHOC, it was agreed that SchlumbergerSema - the A2004 Games-IS integrator and IS provider - was the best candidate to address the A2004 Olympic ISS needs. ATHOC and SchlumbergerSema agreed that it was imperative to address ISS and clearly scope any related activities and project. As such, a two-day workshop was organized in June 2002 by the two organizations, with SchlumbergerSema preparing the agenda and presentations. The workshop participants included senior management of the IOC, ATHOC and its IT partners, and senior SchlumbergerSema corporate and A2004 Games-IS project functional management.

The topics considered included past ISS lessons from the SL2002 Games; ISS issues to expect in A2004; SchlumbergerSema's ISS vision; the technologies of ISS; the factors for and indicators of Games ISS success; and means to maximizing the organization's ISS benefits. The workshop was structured in a manner that would encourage upon its conclusion the definition of actions and next steps. It was hoped that the attendance of senior management from across organizations would contribute to that direction.

During the ISS workshop a number of ISS messages were communicated, originating primarily from the SchlumbergerSema ISS risk expert. These messages and the rest of the communication process parameters are summarised in Table 4.10 below.

ATHOC, the IOC and IT partners were encouraged to provide feedback to the workshop presentations and messages as well as to jointly explore the ISS expectations for the A2004 Games. ATHOC overall indicated to be receptive to the expert ISS risk messages, although the SchlumbergerSema ISS risk expert later stated that

> "the workshop did not go as I had expected and wanted to. They knew little about their environment and did not understand what their ISS needs were. I

hoped for more feedback and concrete future direction" (i.e. Appendix-A3:26).

Overall, the ISS risk messages communicated by the SchlumbergerSema ISS risk expert were met with agreement and it was approved by the end of the two-day workshop that SchlumbergerSema was an appropriate candidate to provide ATHOC with strategic ISS consulting services.

However, what was contested by ATHOC at the end of the workshop was whether they should pay an additional fee for such a service, claiming that the security of the Games systems and network was the responsibility of the Games-IS Integrator and should be covered within the existing contract. As suggested by the Games-IS Chief Integrator,

> "the ISS workshop increased confidence in SchlumbergerSema's capability to reliably integrate and operate the Games-IS. [...] There were no objections with regards to the messages communicated during the workshop. What was debated was who was going to pay for it" (i.e. Appendix-A3:9).

Due to time limitations and the scope of the workshop, it was agreed that this discussion would continue among the appropriate persons at a later point in time. With the conclusion of the workshop it was agreed that SchlumbergerSema would provide a formal proposal to ATHOC - no later than early September 2002 - for the provision of A2004 ISS services as presented during the workshop.

After a series of negotiations between SchlumbergerSema's ISS expert and ATHOC's IT department, the A2004 Olympic ISS Services Proposal was formally documented and submitted to ATHOC in early September 2002. The proposal re-iterated the ISS messages communicated during the June 2002 ISS workshop and stressed the need for a business-aligned A2004 ISS plan: "ISS business requirements aim to avoid over and under securing assets, thus leading to the maximization of returns of ATHOC's ISS budget".

Negotiations throughout September 2002 resulted in SchlumbergerSema agreeing to include the ISS risk expert in its Games-IS Integration project payroll, rather than ATHOC paying for the proposed ISS services. The ISS risk expert would commence work in October 2002. The 'Analysis and Design' stage of the Games-ISS project was initiated.

Table 4.10: *The A2004 ISS risk amplification process during project 'Initiation'.*

ISS Risk Event/Sign, Communication, Perception and Impact		
1	*ISS risk event/sign*	June 2002: ISS Workshop
	Source	SchlumbergerSema: ISS Risk Expert
	Message	*ISS attacks are extremely common*
	Channel	Interactive face-to-face workshop
	Receiver	ATHOC, IOC, Games-IS and IT Partner senior management.
	Noise: socio-political context	• Increased ISS awareness of ATHOC & IOC after the 9/11 events. • Increased ISS awareness of SchlumbergerSema after the SL2002 Games. • Inadequate support of ATHOC ISS section by its senior IT/Technology management. • Unclear contractual agreement between ATHOC/IOC and SchlumbergerSema with regards to the provision of Games-ISS services.
	Expert view & risk characteristics	• *Familiarity, old risk*: There is evidence that other organizations have been impacted by ISS attacks; • *Controllable*: ISS attacks cannot be avoided altogether, but they can be controlled; • *Not known to those exposed*: ATHOC & Games-IS may be already exposed to risk sources, yet they do know what their exposure is.
	Layperson view & risk characteristics	In agreement with expert view. No/limited prior knowledge on the subject.
	Risk perception impact	• Increased *awareness* across management groups with regards to the need to strategically address Games ISS. • Increased *trust* in the skills and competence of SchlumbergerSema team and experts as the Games-IS Integrator and Operations Manager. • Agreement between ATHOC and SchlumbergerSema that ISS needs to be addressed in the A2004 Games, yet negotiations with regards to 'who will cover the cost'. The issue of cost-coverage *attenuates* the urgency of defining A2004 ISS objectives, roles, responsibilities and deliverables.

ISS Risk Event/Sign, Communication, Perception and Impact		
2-4	*ISS risk event/sign*	June 2002: ISS Workshop
	Source	SchlumbergerSema: ISS Risk Expert
	Message	• ISS project needs to initiate as soon as possible - during the early Games-IS Integration project phases. • Olympic ISS needs to be addressed strategically and holistically; • It is imperative that ISS is aligned to business requirements.
	Channel	Interactive face-to-face workshop
	Receiver	As in message #1 of the Games-ISS project 'Initiation' stage.
	Noise: socio-political context	As in message #1 of the Games-ISS project 'Initiation' stage.
	Expert view & risk characteristics	• *Dread, controllability*: An ISS event/incident is possible, if ISS recommendations are not implemented soon; • *Dread, risk known to experts*: There is evidence of damage from previous experience.
	Layperson view & risk characteristics	In agreement with expert view. No/limited prior knowledge on the subject
	Risk perception impact	As in message #1 of the Games-ISS project 'Initiation' stage.
5	*ISS risk event/sign*	June 2002: ISS Workshop
	Source	SchlumbergerSema: ISS Risk Expert
	Message	Olympic ISS vision - a risk management, business-aligned and - interactive approach, utilizing ISS metrics to monitor ISS performance and transfer knowledge. "*There is no space for error*".
	Channel	Interactive face-to-face workshop
	Receiver	As in message #1 of the Games-ISS project 'Initiation' stage.
	Noise: socio-political context	As in message #1 of the Games-ISS project 'Initiation' stage.
	Expert view & risk characteristics	*Catastrophic, dread*: If you do not adopt the Olympic ISS vision, there will be ISS problems and incidents.
	Layperson view & risk characteristics	In agreement with expert view. No/limited prior knowledge on the subject.
	Risk perception impact	As in message #1 of the Games-ISS project 'Initiation' stage.

4.3.2. A2004 Games-ISS project 'Analysis and Design'

With the arrival of the SchlumbergerSema Games-ISS risk professional in the ATHOC Headquarters and the Games-IS project environments, the ISS expert spent the first few weeks negotiating and establishing lines of authority and report. It appeared that ATHOC expected the ISS risk expert to work full-time with the ATHOC ISS Section to address ISS issues, while the SchlumbergerSema Games-IS Integration project team initially expected the ISS risk expert to fully dedicate his time and efforts on the Games-IS environment, reporting to the Games-IS Technical team manager. Neither of these assumptions was in line with the expectations of the newly recruited SchlumbergerSema ISS risk expert.

Following a series of informal and formal meetings the SchlumbergerSema ISS expert established that he would collaboratively work with the ATHOC team, yet retain his independence as an expert, providing an A2004-wide[156] ISS strategy, guidelines and support. The ISS risk expert stressed that his primary responsibility was the security of the Games-IS solution and that he did not wish to interfere with the authority of the ATHOC ISS Section Manager.

In addition, the newly recruited Games-ISS expert had to clarify his role and responsibilities within his own organization. He explained to the Games-IS Integration Chief the strategic significance of ISS and the 'greater-than-technology' scope of ISS management. This was not met initially with agreement and the Games-ISS risk expert had to ask for the support of SchlumbergerSema executive and corporate management in order to achieve the desired authority and reporting structure within the Games-IS Integration project. This led to the Games-IS Integration management team labelling the ISS Risk expert as a 'diva'. Yet, the support shown towards him by the SchlumbergerSema executive management team indicated to the rest of the Games-IS function managers the existing degree of *trust* in the skills and competence of the ISS Risk Manager. Thus, the Games-IS Integration team accepted the new organizational structure.

Having established his organizational independence, role and responsibilities, the Games-ISS Risk Manager started working on producing a number of deliverables, which were not, however, aligned to those proposed earlier in the *A2004 Olympic ISS Services Proposal* document (i.e. section 4.3.1).

[156] I.e. both for the Admin and Games networks.

4.3.2.1 Games-ISS deliverables, controls and incidents

During the 'Analysis' phase of the Games-ISS project (October 2002 to April 2003), most Games-ISS project activities were focused on defining an Olympic ISS strategy and baseline, while there was also a lot of interaction and guidance provided to the ATHOC ISS Section. As stated by the Games-ISS Risk Manager

> "ISS on the Admin network is not our responsibility. However, matters are not that simple. Although the Games and Admin networks are meant to be separate and independent, in reality they are not. The entire planning and decision making on the issue of separating the networks has been wrong; but it is too late to do anything now. [...] We have to put logical security controls between the two networks, and we have to guide ATHOC in implementing ISS best practices on their network too. Otherwise, the Admin network could represent a vulnerability for the Games network; and we cannot afford that" (i.e. Appendix-A3:26).

As Games-ISS activities became increasingly design-focused (from April 2003 to August 2003), the interactions and deliverables associated with the ATHOC ISS section were reduced. The Games-ISS team became increasingly concerned with the ISS of the Games network and the preparations required for venuisation.

During the 'Analysis and Design' phase of the Games-ISS project activity coordination between and within teams was achieved primarily through the production and communication of strategic ISS planning and baseline documents. These aimed to standardise ISS work processes and norms, while their scope and content was defined by the Games-ISS expert. These documents were not developed linearly, but mostly in parallel and over several rounds of peer-reviews.

Games-ISS controls had not yet been implemented and Games-ISS incidents were not reported or relevant, given that the Games network environment was not yet operational. The only ISS controls to be implemented and ISS incidents to be reported were related to the Admin network or under the jurisdiction of ATHOC, such as the physical security of venues and technology secure areas (TSAs). Nevertheless, such ISS controls and incidents also had a direct impact on the Games-IS solution, since the power outages and lax physical security controls at the ATHOC headquarters and venues - which also hosted the Games-IS environment - implicated the reliability and security of the Games-IS(S) solutions and operations.

Each Games-ISS deliverable, control and incident - whether that was targeted to the Games-IS or Admin-IS groups - communicated a number of ISS messages across various project management and functional groups. These are considered in more detail below, along with their impact on ISS risk perceptions and levels of organizational reliability and operational preparedness. First, however, the 'contextual noise' of the 'Analysis and Design' Games-ISS project phase is considered.

4.3.2.2 Contextual noise - organizational politics, culture and project phase challenges

Apart from the organizational/structural changes related to the Games-IS Integration and Games-ISS projects that were summarised in Tables 4.6 and 4.9 respectively, a number of other contextual themes were evidenced during the Games-ISS project 'Analysis and Design' phase. These were directly related to the organizational culture, politics and project challenges experienced during this phase, and formed the contextual noise of ISS risk management and communication efforts.

The first such theme to be identified was related to the contrasting organizational cultures of ATHOC and SchlumbergerSema. According to the IOC Technology Director,

> "there is no ideal OCOG organizational structure and therefore there is no point for us to try and specify one. We have to allow OCOGs the flexibility to organize themselves as they see appropriate. [...] In ATHOC they take too long to make a decision, and by the time decisions are authorised they are no longer time relevant. [...] All formal decisions are taken by higher management levels, which results in transforming the decision-making process into a highly political one. [...] Their team spirit is very low and they do not realize the greater picture and the ways in which their activities are interconnected. The organizational structure and culture of the ATHOC is a bureaucratic one, resembling inefficient hierarchical public sector organizations; and this comes as no surprise since most members of ATHOC management have such background" (i.e. Appendix-A3:13).

The above, accurately described, inefficiency of ATHOC work coordination and decision making processes, as well as the lack of performance and product delivery monitoring was also widely acknowledged among ATHOC employees and partners.

The poor work coordination and communication structures in ATHOC were also blamed on the level and type of ATHOC personnel skills and competence. Olympic-experienced workers from both the IOC and SchlumbergerSema noted that the Olympic Games do not attract enough expert and skilled professionals, due to the temporality of the project organization and the absence of career promotion opportunities. The Games-ISS Risk Manager noted that

> "small countries like Greece do not have the available resources required for a project of such scale; but resource availability is not the only problem in A2004. Resource availability and management has been overall poor. Because the local market is small, there has not been enough interest from sponsors to finance the A2004 Games. As a result, the majority of the ATHOC workforce is not adequately skilled; they cannot pay for more expensive workforce. [...] ATHOC needs people with more experience and technical knowledge. [...] They should have integrated more international, skilled experts into their workforce" (i.e. Appendix-A3:38, 39).

However, the lack of ISS prioritisation by ATHOC management was not only the result of ATHOC internal politics and perceptions, but also the perspective adopted by the IOC. According to the IOC Technology Director,

> "information security is not of primary concern for us. It is not mandatory, not a priority. What matters is what is visible. What matters more is obtaining and broadcasting the results. [...] Information security was not a priority for us until Schlumberger entered the picture and a different approach was taken with regards to risk management and information security" (i.e. Appendix-A3:13).

As suggested by the above statement, the organizational culture within SchlumbergerSema differed to that of ATHOC and the IOC with regards to ISS concerns. ISS was perceived and marketed as a business enabler that was not merely a technological concern, but rather had strategic management implications.

In addition, the overall SchlumbergerSema organizational culture was different from that of ATHOC. The SchlumbergerSema workforce was comprised by a mixture of Olympic experienced and inexperienced personnel, with the former provided mentoring to the latter. The Olympic experienced workforce held mostly management positions, which resulted in a strategic outlook to work coordination activities and the relatively clear definition of workforce roles and responsibilities. The outcome was an organizational environment of trust and relative job

satisfaction, as Olympic inexperienced workers were encouraged to learn through trial and error and knowledge sharing. Therefore, during the 'Analysis and Design' stage of the Games-IS and Games-ISS projects, the overall environment was one of team-working, where personnel were required to be delivery-focused. This was also evident within the Games-ISS team, while other teams also seemed to be appreciative of the Games-ISS Risk Manager's skills and competence.

Despite, however, the positive SchlumbergerSema working environment, frustration was also evident within this organization. The demanding workload, where multiple tasks had to be implemented at the same time, and the coordination of activities across various functions and organizations - since SchlumbergerSema was the Games-IS Integrator - created considerable stress.

This was also evident within the Games-ISS team, where the Games-ISS Architect stated:

> "ISS touches upon every other technological and management aspect of the Games network. In creating a Games-ISS strategy and architecture all this information needs to be taken into consideration and made sense of. This is easier said than done. Things keep changing and new information and requirements or constraints keep surfacing. We cannot plan everything from the beginning. We do not know everything that is needed from the start. We find it along the way. The complexity of it all is too great, and it can get very frustrating" (i.e. Appendix-A3:41).

Therefore, aside from the cultural and structural differences across the various A2004 IT organizations, it was evident that the nature and complexity of the project determined to a great extent the ways of working and organizing. Furthermore, the SchlumbergerSema Games-ISS Risk Manager identified a number of additional local-market factors affecting the success of an Olympic event, such as the market availability of sponsors, budget, and skilled human resources, the type and size of economy, the availability of volunteers, and to a lesser extent the local culture (i.e. Appendix-A3:45).

In addition, he suggested that the nature of the project also determined the level of ISS and operational reliability risks. Specifically, he argued that

> "there will come a time when the Olympic Games will fail. It is mathematically certain. [...] In major events such as this it is impossible to control and mitigate all risks. Regardless of all the proactive, detection

mechanisms and controls one puts in place, something is bound to go wrong. What then matters is to have in place the right mechanisms to contain the disaster and its impact. [...] To contain and minimize impact you mainly require three things - the necessary resources, competence, and the right culture" (i.e. Appendix-A3:19, 42).

The contrast between ATHOC and SchlumbergerSema in the A2004 Olympic Games, refers to an extent to an issue witnessed across Olympic events, namely the contrast and power struggle between local and foreign/expert groups. Daily observations of the ATHOC Headquarters work environment, where SchlumbergerSema, SWATCH and other local and foreign technology partners were based, indicated that although ATHOC personnel welcomed the foreign expertise, they also felt threatened by it. The IOC Technology Director verified the existence of this phenomenon - to varying degrees - across OCOGs. However, he also noted that

> "over time their priorities will converge and team-bonds will strengthen. [...] There may be two distinct teams and perspectives right now, but the Test Events will act as a wake-up call - both prior and especially after - that will bring the two teams together" (i.e. Appendix-A3:13).

Indeed, the proximity of the first Test Events (TE-1) in August 2003, and the necessary process of venuisation - where operations moved to the competition venues - acted as a significant positive force of change in terms of coordination efforts and service delivery. Venuisation signalled the need to finalise a period of decision-making debates and negotiations, and concentrate on control implementation and efficient problem resolution. This change was evidenced across all A2004 technology organizations and partners. The ones less prepared for it - such as ATHOC - were the ones that demonstrated the greatest changes in organizational structure and culture, as well as the greatest levels of stress and frustration.

4.3.2.3 Parameters and mechanisms of ISS risk amplification

Given the above ISS management activities and contextual noise observations of the Games-ISS 'Analysis and Design' project phase, a number of Games-ISS risks were identified, communicated and managed during this period.

Utilizing the SARF conceptualization of the risk communication and amplification process parameters and mechanisms (i.e. section 3.3.2.1), the researcher identified during this project period 12 areas of formally acknowledged and communicated

Games-ISS risks (i.e. Table 4.11). These ISS risks and the associated messages are considered in more detail below.

Table 4.11: *Games-ISS risks identified and communicated during the 'Analysis and Design' project phase.*

	Games-ISS Risk Area
1	Lack of an Admin and Games networks ISS strategy.
2	Lack of a holistic approach to Games-ISS; addressed as a purely technical issue.
3	Poor and inadequate ISS management efforts on the Admin network.
4	Poor physical security of Olympic venues and TSAs.
5	Problematic ISS monitoring capability in the SL2002 Games.
6	Late involvement of ISS experts in Games-IS 'Analysis and Design' activities.
7	Known ISS risks present within the Games-network due to the prioritization of the network's availability and stability.
8	Games-ISS network design and controls do not reflect different levels of trust across the various network communications.
9	ISS of the Games-IS considered the sole responsibility of the Games-ISS Team. There is a lack of ISS audience-specific operational policies and procedures.
10	Unclear ISS technical requirements covering concerns of critical asset and service redundancy and loose-coupling.
11	A lack of ISS assurance controls.
12	A lack of ISS incident management controls and processes.

With the arrival of the SchlumbergerSema Games-ISS Risk expert, it was identified that the two distinct A2004 Games IT networks - namely the Admin and Games networks - and the two separate organizations preparing and managing each, had to **collaboratively define an ISS strategy**. The Games-ISS Risk Manager communicated that although the two solutions remained separate, the quality of service of each affected the other. Therefore, a common ISS vision and strategy would facilitate efficient ISS management practices across the two networks. Lack of such collaboration and coordination would lead to incomplete information about ISS vulnerabilities (i.e. a lack of risk knowledge to those exposed), and hence a lack of risk controllability.

The above ISS message was directly communicated by the Games-ISS Risk Manager, as well as personally experienced by the ATHOC ISS team, which admitted their lack of adequate ISS resources and expertise to implement an Admin-network ISS strategy and understand the ISS approach and activities undertaken by the Games-network organization. Informal meetings between the Games and Admin network ISS professionals, the production and content of the *Olympic ISS Strategy* and *Olympic ISS Roles and Responsibilities* documents, and the formation of inter-organizational and -departmental virtual ISS teams, all operated as further signals communicating the above ISS message. These encouraged the collaboration between the two network and organization environments.

However, as suggested by the SARF, the communication and sense-making of risk messages is a process of iteration and feedback. Although the above ISS activities established a level of *trust* from across organizations/functions towards the Games-ISS Risk Manager, the above deliverables did not generate enough momentum and the Admin-network environment remained greatly disorganized and ISS unreliable. Therefore, it seemed that the lack of adequate, competent and experienced resources within the ATHOC organization *attenuated* the level of perceived ISS risk.

ISS management on the Admin network remained a low priority until a series of Admin-network incidents that compromised the availability, quality and security of the network, and the accelerating process of venuisation, changed risk perceptions. These ISS risk and project events indicated to ATHOC IT management that ISS had to be urgently addressed and coordinated with the Games-ISS team. This led to the - otherwise delayed - production of numerous Admin-network ISS planning documents. More resources were allocated to the ATHOC ISS section, and an ISS audit was conducted by external consultants.

A further ISS risk message to be communicated by the Games-ISS Risk Manager during the early days of his project involvement related to the nature of ISS management. Across a number of occasions he stressed that ISS management was **not a purely technical issue**, but a strategic and management one. The ISS *opinion leader* stressed that the Games-ISS function required some organizational independence, reporting directly to senior project management, and collaborating with a diverse set of groups, experts and functions. He communicated that the Games-IS organization had to adopt **a strategic and holistic approach** to ISS that would be endorsed by project top management. Controls would have to be 'in depth' and 'across layers'. It was suggested that the lack of such an approach would lead to incomplete knowledge of ISS vulnerabilities, making it impossible and/or inefficient to control these. In

addition, it was stressed that with the lack of a holistic approach to ISS management, the poor ISS performance in one area could compromise other areas too.

The *trust* demonstrated towards the Games-ISS Risk Manager by SchlumbergerSema executive management and the past ISS experience in the SL2002 Games, persuaded the Games-IS project management teams with regards to the legitimacy of the messages communicated by the ISS expert. However, as suggested earlier, it is interesting to note that the organizational and structural independence granted to the Games-ISS Risk Manager was not fully accepted by the rest of the Games-IS management team, who labelled the former as 'a diva'.

On the other hand, it was observed that the same sentiment was not shared by the rest of the technical experts of the Games-IS organization. The latter group increasingly collaborated with the Games-ISS team and demonstrated great levels of appreciation and acknowledgment of the Games-ISS team's skill levels and vision. Therefore, despite the power struggle across the Games-IS management structures, the project organization overall accepted the ISS messages of a holistic and strategic approach to ISS.

During this period, the members of the Games-IS Operations group were the ones that interacted the least with the Games-ISS experts, indicating a relatively low level of awareness over ISS controls and requirements. As is demonstrated in sections 4.3 and 4.4, this resulted in the Operations group acting as an ISS risk amplification/attenuation station during the following project phases.

The third ISS risk to be identified and communicated during the Games-ISS project 'Analysis and Design' phase was that related to the interdependence and interaction of the Admin and Games networks. A series of new Admin and Games-IS business requirements demonstrated to Games-IS project management that the **Admin network** represented **an ISS vulnerability** to the Games network. This implied that connections with the Admin network were not to be trusted, since its ISS vulnerabilities were unknown to those exposed, uncontrollable, and with a potentially delayed effect. Also, the lack of adequate proof that the Admin-ISS was strategically managed by ATHOC suggested that any ISS risks would not be easily reduced and would potentially pose catastrophic and dreadful consequences to the Games network.

In addition, a series of Admin-network highly visible performance and security incidents *amplified* concerns, leading the Games-IS teams towards implementing a

series of logical ISS controls to segregate the two networks and strictly monitor the connectivity with the '*marked/stigmatised*' Admin network.

The fourth ISS risk to be identified during the project phase under consideration was related to the **poor physical security** of Olympic venues and technology secure areas (TSAs). Attention to this risk was raised both through a series of reported incidents as well as being directly visible to anyone who visited these areas. Although this risk became an increasing concern within both the Admin- and Games-ISS groups, it seemed that the former was often overwhelmed with the number of problems they had to resolve, and thus did little with regards to resolving the problem.

Such lack of proactive risk management generated a number of *ripples* and determined ISS actions of the Games-IS groups. Identification of the particular risk by the Games-ISS team led to significant concern since they perceived that there was little that they could do to resolve this problem as physical security was not within the jurisdiction of SchlumbergerSema, but within that of ATHOC. Physical security vulnerabilities were identified as potentially catastrophic, involuntary and not easily reduced. Therefore, the Games-ISS team resorted in putting pressure on ATHOC to address the issue, as well as designed ISS logical controls that would mitigate most of this risk. It was, thus, suggested that Games-IS systems had to limit functionality to what was absolutely necessary, while mapping system vulnerabilities and criticality to levels/zones of physical security.

A further ISS risk that was identified during the project 'Analysis and Design' phase was that related to **ISS monitoring**. The Games-ISS Risk Manager stressed throughout the particular project phase the significance of ISS monitoring and the need for an information integrating and consolidating solution. Hence, he stressed the need for a SIM solution, and underlined that past, SL2002 Games experience indicated that ISS monitoring information would become too great and uncontrollable as the Games-IS operations expanded. Therefore, the risk was an old one, known to experts, and controllable if risk mitigation solutions were timely implemented.

The need for a SIM solution was communicated by the Games-ISS Risk Manager across a number of formal and informal meetings with Games-IS project management and SchlumbergerSema executive management, as well as in a number of strategic planning and design Games-ISS documents. The SIM solution - that was initially not budgeted for by the Games-IS project - was presented as a means to obtain real-time understanding of the IT infrastructure's ISS posture, support efficient ISS risk decision making and incident management. After a series of negotiations, the budget for a

Games-IS SIM solution was approved, and design activities were incorporated into the Games-network ISS architecture.

It is interesting to note, that the approval of the considerable SIM budget was only achieved after the Games-ISS Risk Manager presented this as a corporate-wide SchlumbergerSema opportunity to collaborate with another pioneer in the IT industry, as well as a cost that would be justified by the re-utilization of the technology in future Olympic events. Therefore, *framing* the risk and associated control costs and benefits determined the impact of the particular risk communication.

The sixth ISS risk to be identified during the 'Analysis and Design' stage of the Games-ISS project was related to the **late ISS expert involvement** in the A2004 Games-IS project. The impact of this decision was clearly demonstrated with the identification of new Games-network business requirements that had significant ISS planning (costing and designing) implications.

The identification and acknowledgment of this risk by both the Games and Admin IS management teams was used by the Games-ISS Risk Manager to justify his involvement with the activities of various Games-IS functions. In addition, he suggested that any further top management ISS decision making delays and lack of commitment could lead to further future ISS risks and increased costs. Thus, although negotiations between the Games-ISS Risk Manager and rest of the Games-IS management team continuously took place during this project phase, his budgetary and authority requests were, overall, granted and not delayed.

On the other hand, however, the ATHOC Admin-network environment had a delayed response to the risk signal communicated by the Games-ISS Risk Manager. This was greatly due to ATHOC's organizational problems identified section 4.3.2.2 above. It was not until the ATHOC IT Manager was replaced and the demands of venuisation preparations underlined for ATHOC's Technology Department management the content of the above ISS risk message.

The seventh Games-ISS risk identified and communicated during this project phase was related to the ISS implications if the Games-network was not to remain closed to the outside world and strictly controlled with regards to its **Admin network and extranet connections**. This risk was communicated across a number of formal and informal meetings between the Games-ISS team and other Games-IS functions, as well as documented across a number of Games-ISS and Technical design documents.

In addition, the same documents communicated that within the Games network there were known **system vulnerabilities**. By focusing on and prioritizing the Games network's "high availability and utmost stability", the Games systems were lagging ISS patches and were more vulnerable than most standard systems. It was, thus, communicated that system images had to be strictly defined and controlled, as well as the Games network had to remain closed.

Furthermore, the problematic Admin network availability and quality of service incidents stressed the unreliability of the Admin network, and the need for the Games network to implement logical ISS controls to remain closed, thus retaining the maximum possible operational independence.

Thus, the message with regards to the criticality of keeping the Games network closed and tightly controlled at its perimeter was widely communicated and accepted across the Games-IS functional teams, although not all teams seemed to appreciate the full scope of related ISS vulnerabilities. If perimeter security were to be compromised, the consequences could be dreadful and catastrophic. However, if the specified controls were implemented, the ISS risks could be controllable and known.

Closely related to the above area of ISS risk was the issue of **trust across the various Games-network connections**. The Games-ISS team stressed - particularly through a series of solution design and strategy documents - that not all Games-network internal and external communications enjoyed the same levels of trust. Therefore, it was necessary that implemented technical/logical ISS controls reflected the level of necessary trust and were aligned to the criticality of the information and service supported by the particular network communication. Lack of such business-criticality and trust proportionate controls could lead to the compromise of not only the Games-IS network and services, but also the quality of communications of other, trusted and valued parties, such as the Olympic broadcasters. That would be catastrophic. Thus, the Games-ISS team closely collaborated with the Games-IS Network experts to identify and design the necessary ISS controls.

One further area of ISS risk identified during the Games-ISS 'Analysis and Design' project stage was that related to the need for audience-specific **operational policies and procedures**. It was communicated that an incomplete set of Games-ISS operational policies and the inefficient communication and application of these could compromise the organization's IS and ISS performance and services. The creation of audience/function-specific ISS policies was considered necessary in order for each

work group to clearly understand its ISS role and responsibilities, creating ISS accountability and awareness across the organization. It was communicated that ISS management was not the sole responsibility of the Games-ISS team, but an organization-wide one. Compliance with the Games-ISS policies was not only a matter of implementing technical ISS requirements, but also an issue of organizational behaviour and culture. In addition, it was also stressed that any exceptions to the approved Games-ISS policies and procedures should be communicated, managed and monitored.

Therefore, during the Games-ISS 'Analysis and Design' phase, seven policies were defined, each identifying a separate set of audience-specific ISS risk areas and associated controls. These ISS policies were overall positively received by the various related groups, while any concerns and foreseen exceptions were discussed with the Games-ISS team. This was particularly the case for Games-IS Technical teams, several of which had requested from the Games-ISS team a set of ISS requirements that would guide their IT designs and solution configurations.

Overall, the risk signal associated with the presence and enforcement of Games-ISS operational policies and procedures communicated that defining and complying with a Games-ISS baseline contributed towards better identification, management and monitoring of ISS risks. ISS risks would become known to experts, potentially observable, and controllable. Lack of enforced ISS policies and procedures would have the exact opposite effects.

A further area of ISS risk identified in the Games-IS environment by the Games-ISS and Games-IS Technical experts - primarily through a series of formal and informal inter-disciplinary and inter-departmental meetings - was related to the **secure design and configuration of Games-IS technical solutions**. Apart from typical ISS controls of application and system access restrictions, the prioritization of Games-IS availability and stability made imperative the need for critical asset redundancy and loose coupling of Games-IS services and business units (i.e. Olympic venues).

The need for redundancy was greatly acknowledged by all Games-IS functions, and was therefore included in the Games-IS budget and designed into the Games-IS systems and network. However, the loose-coupling of Games-IS services and venues was appreciated to a lesser extent by the various non-ISS Games teams. This was proposed via a series of ISS network and network area segregation controls, and the implementation of network traffic restrictions. Such controls had not yet been designed and implemented by the Games-IS Network team, nor could the Games-ISS

team fully provide detailed requirements as there was still poor understanding of 'ordinary/normal' activity within the Games-network. Therefore, this was identified as an area of ISS risk that was greatly unknown and unobservable during this project phase, but with expectations to become increasingly known and controllable through a process of testing and operational rehearsals. Thus, it was stressed that over the next project stages of preparation considerable efforts would have to be made in order to understand 'normal' and acceptable Games-network traffic, implementing not only controls of IS redundancy, but also loose service and venue coupling.

Closely related to the risk signals communicated by the creation of the Games-ISS operational policies and procedures and the specification of technical ISS design and configuration requirements, was the risk signal associated with the need for **ISS assurance controls**. Throughout all key Games-ISS planning and design documents it was communicated that a lack of ISS assurance controls would lead to inefficient ISS control enforcement, incomplete knowledge of the Games network ISS posture, and inefficient ISS problem detection and resolution. A lack of adequate ISS assurance controls would compromise the efficiency of other ISS management efforts, since it would not be possible to monitor these and verify their levels of performance. That would respectively compromise ISS risk decision making and efficient incident management. Therefore, it was recommended that ISS guidelines, policies and procedures should act as compliance audit checklists, while the combined utilization of ISS metrics and an integrated ISS monitoring solution (i.e. a SIM solution) would operate as a further means to ISS assurance.

Given that ISS assurance controls were still in their design phase and had not yet been implemented in the Games-IS environment, no particular feedback was provided by other Games-IS teams. Games-IS top management had overall expressed their interest in the findings and effect of such controls, but other technical Games-IS staff were rather indifferent towards these controls and identified area of risk.

Finally, as venuisation preparations intensified, the Games-ISS Risk Manager increasingly stressed the need for efficient and effective **ISS incident management processes** and structures. Similarly, the *Games-Network ISS Strategy* and the Games-ISS operational policies and procedures highlighted that ISS management did not only involve activities of proactive risk management, but also effective containment of ISS incidents that would prevent the compromise of the Games network availability and stability. Thus, it was identified that an ISS incident management procedure, team structure and escalation process would have to be defined and aligned to the - wider in scope - Games-IS problem resolution procedure.

This direction was met encouragingly by the Games-IS Operations group that acknowledged that the scale and complexity of the Games-network made it likely that not all risks would be known to the Games-IS experts prior to the Games, or that there could be unforeseen last minute changes and new risks. During the particular project phase, however, the rest of the Games-IS functional groups were more preoccupied with the timely design and implementation the Games-IS infrastructure necessary for the first round of Test Events (i.e. in August 2003), than with the mechanisms and procedures of incident containment. Therefore, beyond the Games-IS Operations team and Games-ISS Team, the intensity and prioritisation of activities during the particular project phase operated as factors *attenuating* the importance of containment controls.

4.3.2.4 Organizational ISS reliability and operational preparedness

Given the above ISS activities, contextual noise and process of ISS risk identification and message interpretation during the 'Analysis and Design' phase of the Games-ISS project, the researcher also examined their impact on levels of organizational reliability and operational preparedness.

A high reliability questionnaire was developed by the researcher as in Appendix-A10, and was repeatedly completed by a number of ATHOC Admin-network and SchlumbergerSema Games-network professionals that represented different organizational functions. They were all requested to assess the level of organizational ISS maturity with regards to reliable organizational design, culture and operational management. The responses to this questionnaire are examined below, while the growth rate of ISS reliability maturity levels is summarised in Appendix-A10: Table A10.2.

From these findings it is evident that during the period of intense Games-ISS design activities (i.e. April to June 2003) all questionnaire respondents agreed that the majority of Games-ISS controls of **reliable organizational design** were in place, yet had not yet matured and were not Games-IS universally applied.

During this period it was also evident that the majority of the Games-IS project management team and Operations team also identified a number of ISS controls that were either non-existent or they were unaware of their status. This could possibly indicate that during the particular project phase the Games-ISS team primarily collaborated and coordinated efforts with other technical functions, but not the

management structures as yet. Communication channels between the ISS experts and other Games-IS functions had not yet developed fully.

It is interesting to note, however, that during the period immediately prior to venuisation and the first Operational Rehearsals (i.e. August 2003) a positive progress is overall observed with regards to the maturity of the existing controls. This is probably explained by the approval of Games IS and ISS designs during that period, as well as the start of the Games-ISS project 'Implementation' phase.

In addition, as time progressed less reliable ISS organizational design controls were identified whose status was unknown to the questionnaire respondents. This indicates the increasing levels of communication and collaboration between various functions - and in particular with the Games-IS Technical teams - and the transfer of knowledge and expertise among them. The IT-Helpdesk team, on the other hand, remained uninformed with regards to the status of several ISS organizational design controls.

Therefore, from April to June 2003 the number of non-existent ISS organizational design controls was reduced, while control maturity improved. By July 2003 all identified ISS organizational design reliability controls were in place, yet their maturity levels - although improving - remained poor. In addition, perceptions seem to have converged as time progressed, indicating increasing levels of effective ISS risk and control management communications.

With regards to ISS controls of **reliable operational management**, an agreement is observed across Games-IS functions that the majority of these were non-existent or lacked substantial maturity prior to venuisation. Interestingly, the persons least knowledgeable of the ISS operational management controls were members of the Games-IS Operations functions. This finding falls in line with observations during the particular project phase where ISS communications were primarily with the Games-IS Technical groups in order to define the acceptable ISS baseline and designs. ISS operational management controls had not yet been developed and the associated communications with the Operations functions had not yet been made.

As venuisation preparations peaked prior to the first Test Events (i.e. August 2003) ISS operational management controls improved. Nonetheless, the majority of Games-IS functions seem to have remained unaware of these developments and still perceived such controls to be greatly non-existent. The only exception to this observation was the Games-IS Technical team. This finding is compatible with the researcher's observation made during that phase, where the Games-ISS team was

primarily interacting with the Technical teams, defining acceptable ISS designs and ways of working. Other ISS communications had not yet matured. Similar to controls of reliable ISS organizational design, the persons least knowledgeable of the Games-ISS operational management controls were those that had an operational focus.

Therefore, over time, ISS operational management controls improved (i.e. Appendix-A10: Table A10.2), yet were still largely non-existent, and were not communicated to the majority of Games-IS functions.

In relation to ISS controls of a **reliable organizational culture**, prior to venuisation findings demonstrate that the distribution of maturity estimates ranged from non- to greatly-existent, indicating that different controls presented different levels of maturity.

An analysis of the questionnaire responses suggests that the most mature control of reliable ISS culture was related to the clear decision making structures and the existence of formal and informal communication structures and mechanisms. The least mature or non-existent controls were related to the availability of ISS training and incident response capabilities. These findings can be justified by the fact that during the particular Games-ISS project phase the focus was on the definition of an acceptable ISS baseline and designs, and not on operations and formal ISS training. ISS work was mostly coordinated via informal processes of mutual adjustment and the gradual standardization of IS and ISS work processes via the delivery of documented strategic and design guidelines.

With the Operational Rehearsals approaching, the majority of Games-IS functions identified a small improvement of reliable ISS organizational culture controls. Action had been taken to implement such controls - for example the delivery of ISS training, although these remained greatly immature.

Yet, it is interesting to note that with venuisation an increased number of questionnaire respondents identified organizational ISS culture controls whose status remained unknown to them. This potentially points to the fact that with the approaching venuisation there was a greater recognition of the presence or absence of such controls. The lack of visible and mature controls may have acted as a stress factor for the non-ISS functions that identified several unknown control areas.

Apart from classifying reliable ISS controls into categories of organizational design, operational management and organizational culture, these can be also classified into anticipation- and containment-focused controls.

Therefore, with regards to ISS controls of **reliable anticipation**[157], prior to venuisation all Games-IS functions agreed that the majority of such controls were either non-existent or very immature and with no uniformity across the Games-IS environment. In addition, the Games-ISS experts identified that the status of ISS anticipation controls that were not directly under their direct jurisdiction, remained unknown to them.

With venuisation the majority of ISS anticipation controls were implemented; however they were still greatly immature. It is worth noting that all Games-IS functions agreed that the maturity of ISS communication controls across teams had improved, along with the identification of Games-IS technical requirements and interdependencies. However, formal training and publication of ISS operational policies and procedures remained greatly undeveloped.

The status of **reliable ISS containment**[158] controls demonstrated little maturity prior to venuisation. Games-IS operational functions seem to have been the ones least aware of the ISS containment controls in place, indicating a lack of communication between the expert Games-ISS team and the Operations team. This can be partly justified by the preoccupation of the Games-ISS team with design activities during this project stage.

Similarly, the Games-ISS expert also identified a set of controls whose status he was unaware of. These involved Games-IS design and implementation controls, such as the existence of single points of failure in the Games-network. This indicates a lack of adequate communication with the Games-IS Technical teams.

With venuisation, some positive progress was observed in relation to ISS containment controls across all Games-IS functions, however these still lacked uniformity. The most confident function with regards to the implementation of containment controls

---

[157] According to Weick and Sutcliffe (2001, 2007) *reliable anticipation controls* focus on activities prior to the occurrence of an (ISS) incident, and cover three areas, namely a pre-occupation with failure, a reluctance to simplify and normalise, and a sensitivity to operations (i.e. section 3.3.2.2).

[158] According to Weick and Sutcliffe (2001, 2007) *reliable containment controls* focus on activities after the occurrence of an (ISS) incident, and cover two areas, namely a commitment to resilience and a deference to expertise (i.e. section 3.3.2.2)..

seems to have been the Games-IS Technical one. This can be potentially justified by the intense Games-IS design and implementation activities of the Technical teams during venuisation preparations. Otherwise, ISS containment controls remained invisible outside the Games-ISS team.

Therefore, between April and June 2003, as venuisation preparations were initiated, ISS containment controls improved. Yet, the status of several of these controls remained unknown outside the confines of the Games-ISS team and the closely collaborating Games-IS Technical teams[159].

Some further observations of interest were made during this project phase with regards to the findings from the '*Maturity of Reliable ISS Organization*' questionnaire. When assessing the maturity level of ISS reliability controls within a particular Games-IS area, it seemed that members of the same team, or closely collaborating teams, assigned similar scores. Furthermore, it was observed that laypersons often provided similar scorings.

Finally, it was observed that persons and teams whose activities focused on a particular functional area, allocated higher maturity scores to the associated controls than laypersons did. Therefore, it could be argued that during the 'Analysis and Design' stage of the Games-ISS project either ISS control experts operated as risk attenuators, or that ISS control laypersons operated as risk amplifiers.

[159] As indicated in Appendix-A7, the various functions of the Technical group included: the Network, Windows 2000, Unix and Databases teams.

4.3.3. A2004 Games-ISS project 'Implementation and Testing'

Following the period of Games-ISS 'Analysis and Design', which provided some clarity with regards to the A2004 Games-ISS needs, priorities and vision, the implementation of the Games-ISS controls started with the shift to venuisation, a couple of months prior to the first Test Events (i.e. TE-1: August 2003).

The objective of the Games-IS(S) 'Implementation' phase was to configure the IT infrastructure as designed and agreed during the earlier project stage, while 'Testing' - over a series of operational and non-operational phases of the project - the reliability, stability and security of the Games-IS.

At this point, it is worth noting that the implementation activities of the rest of the A2004 Games-IS project had commenced almost ten months earlier, primarily with the implementation and testing of the Games-IS applications and the associated systems and network that supported these. As stated by the Games-ISS Architect

> "the design and implementation of the Games-ISS controls are conducted at a stage in the greater project when other decisions have been long made. In many cases we have to find ways around existing infrastructure in order to make the Games network secure. [...] It is not always easy, or cheap" (i.e. Appendix-A3:41).

Therefore, between June and July 2003 the Games-ISS team was intensely involved in the implementation of ISS controls as defined and designed during earlier project stages. From August 2003 onwards - when the Test Events (TEs) commenced - the controlled trial and error operations acted as a feedback mechanism to the previously defined Games-IS(S) infrastructure designs, policies and procedures. This led to a series of negotiations, control changes and improvements.

In addition, the increased Games-ISS workload of the project 'Implementation and Testing' phase resulted in new members - of specific expertise - being added to the Games-ISS team (i.e. Table 4.8).

4.3.3.1 Games-ISS deliverables, controls and incidents

Most of the Games-ISS 'Implementation and Testing' project phase activities were repetitive and spanned across the particular project phase.

Overall, a number of observations can be made with regards to the Games-ISS activities and risk events during the 'Implementation and Testing' phase. Firstly, the Games-ISS team became increasingly disengaged with the activities of ATHOC's Admin-ISS team. The increasing workload of the Games-ISS team and the inefficient decision-making process of ATHOC resulted in SchlumbergerSema formally suggesting the recruitment of independent ISS experts/consultants to help out ATHOC with its Admin-ISS planning and implementation activities.

Instead, the Games-ISS team increasingly interacted and collaborated with other Games-IS functions, IT partners (e.g. SWATCH, KOEP), and IT customers (e.g. broadcasters).

In addition, the Test Events raised awareness with regards to new ISS risks (i.e. Table 4.12) and stressed the need to coordinate the implementation of Games-ISS controls with other functions. The Test Events also raised awareness with regards to the levels of operational complexity and uncertainty, often leading to new negotiations and tensions between teams.

One of the lessons learned from the progressive 'Implementation and Testing' activities was that a number of changes and Games-IS(S) reconfigurations would have to be implemented. These would have to be controlled via change management and ISS assurance procedures.

Finally, it was observed that as this project phase came to an end (i.e. end of January 2004), increased pressure was put on all Games-IS functions to proceed with implementing the IS(S) controls that had been negotiated throughout 'Implementation and Testing'. Decisions were reached, action was taken, and the Games-IS(S) environment became increasingly stable. Any further tests beyond that point would focus on the impacts of increased operational scale and complexity.

4.3.3.2 *Contextual noise - organizational politics, culture and project phase challenges*

While during the 'Analysis and Design' phase of the Games-ISS project it was observed that the Games-ISS team operated either in relative independence from the other Games-IS functions, or in a relatively stress-free environment of collaboration, things changed during the 'Implementation and Testing' phase of the project.

Approaching venuisation demanded that Games-IS functions work with one another more closely and within tight timeframes. The interdependence of deliverables across teams became more apparent, and effectively coordinating efforts was critical to the success of the 'Implementation' stage. In addition, the significance of timely and accurately sharing information with regards to new requirements and configurations was also made evident.

Thus, the 'Implementation' stage of the Games-IS(S) projects required a different set of skills to the previous 'Analysis and Design' project phase. However, the swift change in the ways of working that came with venuisation did not always allow enough time for the Games-IS(S) staff to adjust. Stress levels increased and differences surfaced with regards to the ways of working and task priorities. While in the previous project phases Games-IS teams had created a positive environment of team-working, the Games-ISS Risk Manager suggested that venuisation "is a time when we have to learn to say 'no' to some requests. We have to prioritise. We cannot keep everyone happy, and we will have to do some things on our own too" (I.e. Appendix-A3:54).

Moving towards venuisation also created a number of frictions internal to Games-IS teams, including the Games-ISS team. While existing staff retained their roles and responsibilities as before, venuisation implied that they would also have to take on some new roles and responsibilities specific to the operational Test Event phases. This often led to tensions within teams as decision-making structures appeared to change. Similarly, when new team members joined the existing Games-IS(S) teams, older members often felt threatened by the lack of hierarchical structures within the increasingly operations-focused teams.

Apart from such matters of internal team power struggles, levels of job satisfaction dropped during the 'Implementation' phase of the project. Games-IS staff complained not only of increased stress levels, but also of great frustration due to the increasing complexity of operations and the great extent of required changes. Members of the Games-ISS team - as well as other teams - suggested that the

continuously changing environment and the repetitive revision of implemented controls left them with a reduced sense of achievement. According to the Games-ISS Network Analyst frustration was caused by a further factor:

> "it is impossible to get complete and accurate information. This leads to wrong assumptions and wrong configurations; and wrong configurations lead to many errors, many corrections, and many changes. And all of this seems never ending" (i.e. Appendix-A3:72).

In fact, the Games-IS Chief Integrator suggested that

> "during the 'Implementation and Testing' phase of the project planning skills are not as important as during 'Analysis and Design'. During this stage the most valuable staff is that which has strong technical skills or good communication skills - ideally one has both. [...] During 'Implementation' and 'Operational Rehearsals' staff across the various teams can develop strong relationships that are not necessarily related to organizational position and role. And these relationships are very important when things go wrong because you know who you can trust; and you will trust someone who is competent in what they do, or one that you know you can communicate with" (i.e. Appendix-A3:74).

A further observation made during the 'Implementation and Testing' phase of the Games-IS(S) projects was that the repetition of activities and constant revision of deliverables also led to increased levels of boredom. In fact, boredom was also observed during operational Test Event phases; especially so at the competition venues, where workload was usually less to that of TOC-based staff.

Aside from the above changes in the working environment of the Games-IS(S) groups caused by the venuisation of operations, a further observation during this period was the intensification of intra- and inter-organizational negotiations. While the Games-ISS team became increasingly disengaged with ISS activities of the Admin-network, they interacted more with other teams and organizations, communicating their ISS design and procedural requirements as well as incorporating other groups' requirements into their ISS management solutions.

Such interactions, however, often led to tension, disagreement and - occasionally - blame attribution. Tension was least observed with Third Parties (i.e. broadcasters), as their operational demands were of the highest priority to the Games-IS organization. Although the Third Parties repeatedly demonstrated non-compliance

with the Games-ISS device configuration, connectivity and procedural requirements, such incidents were relatively tolerated and it was accepted that ISS controls would be gradually implemented.

Negotiations internal to the Games-IS organization, on the other hand, were less compromising. The Games-ISS team repeatedly had intense disagreements with the Games-IS Operations groups[160] and the Games-IS Network group. These were related to the non-compliance of the Operations groups with the Games-ISS procedures, and the non-compliance of the Network group with the *Acceptable Usage* and *Secure Network* operational policies, as well as the network ISS design and configuration requirements. These tensions peaked with the debate over the implementation of Access Control Lists (ACLs) on the Games network. The Games network performance problems observed after the implementation of ACLs during the TE-2, led to the teaming of the Operations and Network groups, blaming the Games-ISS team and the ACLs for the poor network performance. The Games-ISS team responded to such accusations by stating that the problematic implementation of ACLs was due to the incorrect build and configuration of devices across venues by the Operations groups, and the poor ACLs and network configuration by the Network group. The Games-ISS team stressed the criticality of ACLs on the Games network, yet it appeared that the particular control had been *stigmatised*. The Games-ISS Network Analyst suggested that

> "it is convenient for the Network team to blame the Security one. The Operations team management, on the other hand, is not at all technical to be able to understand what the real problem is. [...] Nobody likes to be told that they cannot be trusted and restrictions have to be put in place. Implementing any type of security control at the perimeter of the Games network is easier than implementing a control inside the network" (i.e. Appendix-A3:72).

Eventually, by the end of the Games-IS(S) 'Implementation and Testing' phase, ACLs were partly implemented. This was greatly due to the increasing pressures to stabilize the Games network by the end of the particular project phase, and the commitment from Games-IS project top management with regards to ISS management. In addition, it was agreed that the Games Network team would recruit more engineers to assist with the improvement of the Games network design and configuration, including the implementation of ACLs.

[160] As indicated in Appendix-A7 the Games-IS Operations function included the following teams: Venue Management; IT-Helpdesk; Software Distribution; PC-Factory, etc.

The commitment to Games-ISS by SchlumbergerSema (and later Atos Origin) top management was not only demonstrated by their support of implementing the ACL controls. The Games-ISS project was one that received great publicity and promotion during the preparation stages of the project, since it was viewed as a business area that could strategically benefit not only the A2004 Games but also the IT sponsor's corporation. Therefore, top management demonstrated particular interest towards the choice and functionality of the SIM solution, as well as the ISS metrics framework and dashboard. However, such interest was not encountered within the Games-IS organization, where most teams - and even most Games-ISS team members - worked independently of the SIM and ISS metrics initiatives.

Specifically, aside from the Games-ISS Risk Manager and ISS Risk Analyst, the rest of the team members did not demonstrate any interest in the ISS metrics dashboard and findings, although they knew of their existence. Similarly, apart from the Games-ISS Risk Manager and the Games-ISS Systems Analyst who was working on the customization of the SIM solution, no other team member demonstrated any particular interest in the technology. Instead, they were using other technologies and tools to manage and monitor ISS in the Games network environment. The Games-ISS Architect repeatedly stated that

> "I do not know why we are implementing the SIM solution on the Games network. Surely it can be useful, but by the time it is ready to use, it will be too late. In the meantime we are doing all the monitoring with our existing devices" (i.e. Appendix-A3:69).

Likewise, the Games-ISS Risk Analyst suggested that

> "we currently cannot use the SIM solution. It generates too many security events and it is impossible to make any sense out of it. There is a lot of customization that still needs to be done. [...] Perhaps the implementation of such a great and complex security solution is not best suited for an environment like ours, where everything changes the entire time and we are short of time. [...] For these Games, the greatest benefit from the SIM solution will be a marketing one. So far it has not affected how the team works and monitors the environment; but it seems that it is all we are advertising" (i.e. Appendix-A3:68).

Finally, the last few issues that seemed to have affected the organizational context during the Games-IS(S) 'Implementation and Testing' project phase were related to the changes in corporate management, namely the take-over of SchlumbergerSema's

Major Events division by Atos Origin, and the subsequent resignation of the Games-ISS Risk Manager. Both events created considerable speculation with regards to the project's future and priorities, and the role and responsibilities of the remaining Games-ISS team's members. However, despite the temporary distraction from daily project activities, activities continued as planned, top management commitment to ISS seemed unchanged, and the duties of the resigning ISS Risk Manager were smoothly handed over to his replacement.

4.3.3.3 Parameters and mechanisms of ISS risk amplification

During the 'Implementation and Testing' phase of the Games-ISS project the focus of ISS activities was on the installation and configuration of ISS technological controls, and the communication and enforcement of procedural and awareness/training ISS controls.

The 'Implementation' of ISS controls and the ISS events and incidents experienced during 'Testing' pointed to the presence of risks or risk events, communicating messages about their nature and the effectiveness of the implemented controls.

As earlier in this study, utilizing the SARF conceptualization of the risk communication and amplification processes, the researcher identified twenty areas of Games-ISS risks that were detected and communicated during the 'Implementation and Testing' project phase (i.e. Table 4.12). Some of these were also identified in prior stages of the project (i.e. Table 4.11). This is to be expected as the risk communication process is often one of repetition and feedback. In fact, the trial and error processes of the A2004 IS Test Events provided further feedback with regards to ISS risks, leading to a series of negotiations, control changes and improvements.

Table 4.12: *Games-ISS risks identified and communicated during the 'Implementation and Testing' project phase.*

	Games-ISS Risk Area
1	A lack of prioritization of **secure configuration** requirements among Games-IS functions.
2	Unknown **physical security** at venues, implicating ISS management decisions with regards to the appropriateness of logical ISS controls.
3	Problematic ISS practices of **Admin network**.
4	Inadequate consideration of **ISS containment and incident management** controls.
5	Inadequate organizational appreciation that ISS is a **common responsibility** with regards to both ISS risk anticipation and containment.
6	Inadequate consideration of **Third Party connectivity** ISS requirements and practices; potentially compromising the 'closed network' principle of Games-network.
7	Lax **access and authorisation controls** of Games applications and systems for Games-IS internal users.
8	Inadequate controls managing and monitoring **unauthorised devices** on the Games-network.
9	Internal threat is evident - **unauthorised activity** on the Games network. Internal communications are not controlled and restricted.
10	Inefficient allocation of **ISS incident management resources** and efforts.
11	Lack of means to adequately **assess** and understand the location, extent and impact of a detected **ISS vulnerability**. Poor **containment** controls.
12	Necessity, yet ISS risk mitigation inadequacy of **malicious software protection** controls - particularly for **laptops**.
13	Inadequate consideration of **IT volunteers** as an ISS threat source.
14	**ISS alerts are too many** and, thus, not manageable.
15	Inadequate incorporation of ISS into the procedures and controls of the **Operations team** functions.
16	Inadequate incorporation of ISS function into the **change management** procedures.
17	Inadequate **customization of ISS** management and monitoring **devices**.
18	**Lack of** a centralized and accurate **information repository** with regards to the configuration of Games systems and the 'ordinary' communications within the Games network.
19	Lack of **mechanisms to standardise configurations** across the Games network.
20	Inadequate and ineffective means to **measure** and monitor the **performance of ISS controls**.

From the early stages of the Games-ISS 'Implementation and Testing' phase it was made evident to the Games-ISS team that the **secure configuration of the Games systems and network** had not been - thus far - a priority among the Games-IS Technical function. Technical teams had inconsistently and inadequately addressed ISS issues, with the greatest ISS awareness indicated among individuals that had worked in previous Olympic event projects.

Towards the end of the 'Analysis and Design' stage, and throughout the 'Implementation and Testing' stage the members of the Games-ISS teams closely collaborated with the various Technical teams communicating that the secure configuration of the Games-IS devices was critical to the reliability of the Games network operations. Such communications were made via formal and informal meetings, documented ISS policies and ISS design requirements. However, the extent of the risk and the significance of risk mitigation controls were not stressed until after the first Test Events (TE-1). During TE-1 a series of ISS incidents indicated that compliance to secure configuration policies was poor, while further guidelines had to be communicated by the Games-ISS experts. Informal and formal communications stressed that it could be no longer assumed that the Games network was a closed one, nor could it be assumed that authorised Games users would not abuse their access and other privileges. The risk message was not only communicated to the Technical teams but also senior project and SchlumbergerSema corporate management. It was suggested that Games systems had to be urgently **security hardened**. Omitting to do so could lead to the realization of catastrophic, uncontrollable and unknown risks on the Games-IS infrastructure.

The use of a worm scenario attack and the simulation of a related hacking exercise convincingly *framed* the risk and SchlumbergerSema senior management authorised the costly - yet necessary - system security upgrades. Any hesitation by the Games Integration and Games Application Development teams due to increased project costs and testing man-hours was removed, and by early October 2003 it was agreed that all Games systems would be security patched and hardened[161]. The timeframe for the implementation of all these controls was defined as the end of the calendar year (December 2003), while responsible parties were identified across teams that would coordinate with the Games-ISS experts the required control implementations.

[161] The security hardening and patching of all Games systems included: (a) an upgrade with the latest security fixes; (d) the hardening of Games-IS device BIOS settings by removing all unnecessary device services; and (c) the implementation of stricter user access controls.

Similarly, it was suggested that Games network connections and communications had to be further restricted and monitored. The great number of Games network unauthorised connections and communications during the August 2003 Test Events demonstrated to the Games-ISS experts the urgency of implementing tighter network ISS controls and access restrictions such as port security and ACLs.

Thus, over a series of formal and informal meetings, as well as via a number of formal risk assessment reports, it was communicated that Test Events demonstrated that security on the Games network was very poor and violations of acceptable activity and behaviour too numerous. In fact, it was communicated that **violations were so numerous** that they were impossible to monitor and contain, thus uncontrollable. In addition, it was suggested that unless the specified network ISS controls were implemented, there would be no other means to reduce the associated risks effectively, while other ISS controls - such as the hardening of Games systems - would be cancelled out.

The response to the above communications with regards to Games network ISS was one of alarm with regards to the Games-IS project management who had assumed that the Games network would be a closed one. Also, for those who had been previously involved with the SL2002 Olympic event, the communication of a vulnerable, not-closed Games network was also alarming. However, the rest of the Games-IS Technical teams - the majority of which did not have any prior Olympic experience - appeared to be *attenuating* the associated risk. Both during and after the TE-1, when the Games ISS experts communicated the need to secure the network and restrict **unauthorised network activity**, Technical teams - and in particular Network engineers - ignored expert ISS directions. The Games-ISS Network Analyst - who prior to joining the Games ISS team was a member of the Network team - suggested that

> "partly they are security ignorant and partly they see this as a game. They control the entire network and they do not like to be told what they can and cannot do. It is a power thing. It happens everywhere. They do not necessarily mean harm, but they do enjoy toying with us" (i.e. Appendix-A3: 63).

Thus, although management commitment was present with regards to securing the Games network, the compliance of Games engineers was not easily achieved. The associated risks had to be repeatedly communicated and a number or ongoing negotiations had to take place in order for Games network security to improve. The Games Network team suggested that ISS network controls were unnecessary -

particularly the internal network communication restrictions, that the Games-ISS team had provided inadequate or inaccurate ISS guidelines, or that the proposed ISS controls negatively impacted the performance of the Games network. Therefore, the Games Network team appeared to act as a *risk attenuating social station*, while negatively *marking* the network ISS controls proposed by the Games-ISS team.

The debate between the Games-ISS and Network teams peaked during the second round of Test Events when the poor performance of the Games network was blamed on the implementation of related ISS controls (i.e. ACLs). The Operations team, which oversaw and managed the operations at the TOC and venues during the Test Events, sided with the Network team during the TE-2. The lack of adequate time to investigate in detail or fix the reasons for the poor Games network performance led to a decision by the Operations team management where the ACLs were removed from the network. In addition, it was decided that port security would be partly deactivated, thus allowing uncontrollable connection of Third Parties onto the Games network. It was thus evident that during operational phases ISS risk decisions were greatly *affected* by the organization's immature containment controls and procedures, as well as the *emotional factor of time-pressure*.

Although the ISS risks of not implementing strict ISS controls - both at the perimeter and internally to the Games network - were known and repeatedly communicated, it was not until the later stages of the 'Implementation and Testing' project phase that their implementation commenced. This was greatly due to the increased corporate and management pressure to resolve the issue and secure the network, as well as the management decision to recruit additional network experts that would specifically work on the standardization of ISS network design and controls. It was agreed that significant efforts had to be made with regards to identifying and creating mechanisms that would standardise the Games network's configuration.

Furthermore, the increasing maturity of effective Games network and system ISS controls by the end of the 'Implementation' project phase was also an outcome of continuing efforts by the Games-ISS team to **analyse and document 'ordinary' activity** within the Games-IS infrastructure.

The first Test Events (TE-1) and the numerous ISS events and incidents that occurred during these due to the great number of unauthorised devices and Games network communications also pointed to a further ISS risk; the, thus far, low prioritization of **ISS containment controls**. Similar to the risk identified during the 'Analysis and Design' Games-ISS project phase (i.e. Table 4.11:12), it was identified that ISS

incident management controls and processes were still immature and inefficient. ISS incidents were not correctly identified and labelled, thus leading to their misallocation with regards to the responsible ISS incident resolution and containment party.

A further factor contributing to the poor ISS incident management and containment efforts was the **lack of adequately customized ISS monitoring tools** and the **lack of adequate knowledge with regards to the build of Games devices** and the 'ordinary' Games network traffic. With vast amounts of information to process and a lack of means to assess and prioritise this information, the Games-ISS experts - as well as the IT-Helpdesk and Games Operations team - were often observed to allocate their incident management resources inefficiently. There were inadequate means to assess and understand the location, extent and impact of a detected ISS vulnerability. For example, it was impossible to assess accurately the potential ISS impact of an unauthorised device connecting on the Games network, or the detection of a virus infected device.

In addition, it was observed that ISS containment controls and processes were often ineffective due to the **poor decision making of non-experts.** In times of operational crisis, decisions were often left to senior operational management, rather than seeking the expertise of technical engineers. Such an instance was during the first Test Events when the ATHOC ISS team detected some Admin-network devices that were virus infected. Although the Admin and Games networks were two virtually separated networks with their interface protected by a series of network design and ISS management and monitoring controls, the Games Operations manager on shift hastily decided to shut down the connection between the two networks. Although he was advised by the Games-ISS team that there was no need to do so, the associated risk was *amplified* by the decision making non-expert and the communication between the two networks was terminated. It was not until several hours later, when the Games-ISS Risk Manager was called on shift and all necessary virus infection checks had been completed on the Games network, that the link between the two networks was reactivated.

The particular incident demonstrated to the Games-ISS team that the Games system and network interdependencies, as well as the associated ISS controls, were not adequately understood by all teams involved in the ISS incident management process, thus impacting the efficiency of ISS risk containment activities. In addition, it demonstrated that ISS decision making was not always delegated to where expertise lay, particularly *in times of emergency*.

Thus, following the TE-1, the Games-ISS team increasingly sought to closely collaborate not only with the Games Technical teams, but also with the Operations team, thus establishing efficient incident management procedures.

However, prior and during the TE-2 the efforts made in order to improve the ISS incident management process and interactions with other Games-IS teams, did not have an immediate effect. A number of ISS incidents took place during that period, where the Operations team violated Games-ISS policies and best practices[162]. Such ISS incidents indicated that the Games-ISS experts were inadequately involved in Games-IS decision making, while ISS laypersons had not fully appreciated their role in maintaining secure Games-IS operations.

In fact, it was the repeated trial and error process of Test Events that demonstrated to Games-IS teams - particularly the Games Technical and Operations teams - that the Games-ISS team had to be involved in technical, operational and change management decisions. In addition, the Test Event trial and error process also demonstrated that IS and ISS decision making had to be delegated to where expertise lay, particularly in times of emergency.

Thus with the Games-ISS team stressing the need to improve ISS containment controls and the various ISS incidents underlining this message, there was eventual change in decision making behaviours and operational IS and ISS procedures. Ineffective ISS incident and change management procedures had been proven to lead to risks unknown to those exposed, that were often uncontrollable and with potentially dreadful consequences.

In addition, the above developments and ISS incidents had communicated a further message, namely that ISS anticipation and containment was not the sole responsibility of the Games-ISS team, but in fact the **common responsibility** of all Games-IS functions and partners.

Among others, this also included **Third Parties** who required connecting onto the Games network in order to obtain and broadcast sport event results data. Throughout the TE-1 and TE-2 it was made evident that Third Parties had been inadequately addressed by the Games-IS organization, including the Games-ISS team. Few preparations had been implemented with regards to their connection to the Games network. No network ISS connectivity, device secure build and configuration

[162] E.g. the Operations team proceeded with device configuration changes, or authorised the removal of ACLs from the Games network without first consulting with the Games-ISS team.

requirements had been provided to them, nor had any formal discussions taken place between Third Parties and the Games-ISS team. Furthermore, the A2004 broadcasters had not received any Games IS(S) training. As such, during the TE-1 it was quickly identified that Third Parties posed a great ISS risk to the Games network, since no port security had been implemented yet. In addition, Third Party devices - which connected onto the most critical of all Games-network VLANS - were not security audited and hardened prior to connecting onto the Games network. However, it was not only the logical ISS controls that were lacking; no ISS operational procedure had been established to address the necessary steps that Third Parties, the Operations/ IT-Helpdesk and Network teams had to comply with.

The non consideration of the ISS risks and issues associated with Third Parties by the various Games IS(S) teams prior to the TE-1 is perhaps surprising given the significance of Olympic broadcasters. When questioned about it, the Games-ISS Risk Manager suggested that

> "prior to the August (2003) Test Events we were all focused on the internal-facing Games-IS preparations that we had to do. We had considered how to protect the perimeter of the Games network and how to secure it from other non-trusted or semi-trusted networks. But we neglected to consider what happens with Third Parties that bring their devices into our trusted environment. [...] This is possibly the highest ISS risk management priority for us now. We need to understand their needs and we need to make them understand our ISS requirements" (i.e. Appendix-A3:60).

Therefore, it appears that the intense preparations and heavy workload prior to venuisation did not allow the Games IS(S) teams to identify the Third Party connectivity risk issue. In addition, focus on the perimeter of the Games network led the Games-IS and ISS teams to overlook the insecure connection of Third Parties within the trusted Games network environment. The ISS risks related to Third Parties were *hidden*.

As soon as the Games-ISS Risk Manager identified the Third Party risk issue during the TE-1, he communicated to the Games IS Operations, Network and management teams that the impact of the identified risk could be catastrophic with grave consequences for the Games-IS operational reliability and security. He quickly proceeded with drafting a set of *Third Party Connectivity Requirements* which were communicated to all Third Parties, ATHOC, SWATCH and the SchlumbergerSema Games Operations and Network teams. ISS controls were not implemented until the next round of Test

Events in October/November 2003, when port security was applied. Yet, compliance to the *Third Party Connectivity Requirements* remained patchy until the end of the Games-ISS 'Implementation and Testing' phase. This was partly due to the delayed creation of a *Third Party Connectivity* policy and procedure (i.e. not until January 2004) and the gradual compliance of Third Parties to the provided ISS connectivity requirements. Given that the facilitation of broadcasting was a key operational aspect of the Games network, when A2004 broadcasters were not compliant to the ISS requirements the Games IS(S) teams did not disallow these connections. The Games-ISS Risk Manager argued that

> "we cannot threaten broadcasters that they cannot connect to the Games network during Test Events because they are not meeting our security requirements. In a sense, within the Olympic context if you do not broadcast a result you also do not have a result. Making things easy for our broadcasters is our top priority; but we also need to ensure that the network also remains stable and secure. [...] We do not negotiate with Third Parties during Test Events; we cannot afford to. However, after the Test Events we have several meetings with them when we try to explain to them what it is we need and why we need it. We tell them that if their connection onto the Games network is not secure not only could they compromise the network's reliability and the quality of information that they get, but they can also affect the quality of results information that other broadcasters get; and we cannot allow that. Nor can our other broadcasting partners. We tell everyone the same, and eventually they will all comply with our requirements" (i.e. Appendix-A3:66).

Indeed, by the end of the Games ISS 'Implementation and Testing' phase the majority of Third Party connectivity risk issues had been satisfactorily addressed.

In addition to Third Parties, ISS risks were identified in relation to a further group of Games-IS workers, namely **IT volunteers**. The risk signal was an IT volunteer related incident that took place during TE-1. An IT volunteer, who was located at one of the competition venues, worked as an IT-Helpdesk Assistant. During his shift and when there was little venue IT-Helpdesk activity, the volunteer accessed through his workstation the database that supported the entire Admin and Games networks incident management system and stored all user credentials and incident information. His unauthorised activity was detected by the SchlumbergerSema IT Helpdesk Venue Manager, who warned the volunteer to refrain from such unauthorised behaviour. The volunteer, however, persisted and attempted accessing

and extracting information from the database. The incident was detected again by the Venue IT-Helpdesk Manager who raised the issue with the central IT-Helpdesk operations at the TOC, without however notifying the volunteer. The central IT-Helpdesk decided to lock the volunteer's account, claiming technical problems. The volunteer logged a ticket reporting account connection problems, which was escalated to ATHOC IT. The latter group investigated the issue with regards to the reported technical problems and identified that the volunteer's account was instead locked because of his unauthorised activity. Circumventing SchlumbergerSema Operations management and without notifying the IT Helpdesk, the ATHOC IT Manager called the volunteer, apologized to him for the inconvenience, informed him of the true reason for his account's deactivation, and finally congratulated him for his interest in security. He then demanded of the IT Helpdesk to reactivate the volunteer's account. This was when the incident was escalated to the Games-ISS Risk Manager.

The particular incident escalated to a major political debate between ATHOC IT and SchlumbergerSema as well as internally to the latter organization. The Games-ISS Risk Manager sent one of his team members at the venue to investigate further and discuss with the IT volunteer, who appeared impenitent and suggested that if he were to be given access to the Games network he would repeat his unauthorised activity, considering it his obligation to hack the Games system and identify its ISS vulnerabilities. Alarmed by this response, the Games-ISS team demanded that the IT volunteer's account be not re-activated. ATHOC IT strongly disagreed with this decision suggesting that IT-literate volunteers were a precious commodity for the A2004 Olympic project, and they could not afford questioning their sense of volunteering. They eventually blamed SchlumbergerSema of inappropriately dealing with this entire incident, while the IT volunteer remained at the venue idling. The Games-IS Operations team, on the other hand, shifted blame to the Venue IT-Helpdesk Manager who had detected the volunteer's unauthorised activity in the first place, while the Games-ISS team suggested that the incident should have been brought to their attention sooner than it did. All this resulted in the Venue IT-Helpdesk Manager resigning and suggesting to the rest of his SchlumbergerSema colleagues that the Games-IS management and ISS teams did not support their own people when they faced difficult and emergency situations.

The above incident communicated a number of ISS risk messages not only for IT volunteers, but also in relation to the efficiency of incident management and escalation procedures, and with regards to the incident detection mechanisms.

With regards to IT volunteers, the incident demonstrated to the Games-IS functions that IT volunteers could not be trusted and they should not be placed in critical IT positions unless the appropriate logical ISS controls had been first implemented. Such controls included the restriction of application and system access privileges, the implementation of strong password policies and user-specific access privileges, and the segregation of duties. In addition, the incident raised awareness with regards to the need to conduct background checks of volunteers, and the need to train them in Games-ISS policies and procedures. Replacing volunteers at critical IT positions with paid personnel was considered by SchlumbergerSema but eventually rejected as a very costly solution.

The above incident, on the other hand, was clearly interpreted differently by ATHOC IT, which suggested that IT volunteers were a critical resource for the A2004 Olympics, and therefore should be treated with particular leniency from the various Games-IS project functions. Following the incident, ATHOC IT did not wish to discuss the matter further with SchlumbergerSema, and throughout the rest of the project IT volunteers were not considered an ISS risk source to them. This was in clear contrast with the perceptions of Games-ISS experts who communicated the exact opposite view both internally to the Games-IS organization and externally - such as to the press. Therefore, ATHOC IT clearly acted as a *social station of risk attenuation*.

In addition to the risk messages communicated in relation to IT volunteers, the above incident indicated to the Games-IS Operations (including IT-Helpdesk) and ISS teams that ISS incident management and escalation procedures were problematic and had to be further formalised. The volunteer incident was escalated to the Games-ISS team only after it had become a crisis and tension had already been created between SchlumbergerSema and ATHOC IT management. It was not identified from the early stages of incident detection that this had to be reported to the Games-ISS team. Thus, following the incident, the Games-ISS Risk Manager and Analyst initiated a number of meetings with the Games Operations and IT-Helpdesk teams to discuss what had gone wrong and what could be improved in future cases. These meetings were important not only in terms of improving future incident management performance, but also in minimizing the negative impact of the incident on the morale of SchlumbergerSema employees. The Games-ISS Risk Analyst argued that

> "you could say that this incident turned into a bit of a scandal within SchlumbergerSema. Everyone found out about it and the Game-ISS and Operations teams were accused of not supporting their people when needed. [...] We cannot allow such accusations. We do not want people to think that

we are interested in such blame-game. If this goes on, they will not report any of the errors and security incidents that they observe" (i.e. Appendix-A3:59).

Eventually, the Venue IT-Helpdesk Manager retrieved his resignation and intra-organizational tensions were relieved. Yet, it was understood among Games-IS functions that the ISS risks related to IT volunteers were a sensitive matter that could not be openly discussed with ATHOC, which perceived this as an Olympic *value-threatening and ideological hazard*[163].

A further risk identified by the researcher at that stage, which however seemed to be considered as relatively unimportant across the Games-IS teams, was associated with the evident levels of **boredom** during Test Event phases. It was not only the IT volunteer that was bored during TE-1 and opted to spend his time hacking the Games systems. The researcher observed that during Test Events and in particular during periods of little event and incident activity, the Games-IS(S)employees, partners and volunteers were bored and distracted by other activities that not only were not related to the Games-IS operations, but also were irrelevant to their job descriptions. Thus, at a period when Games-IS workers were required to give their full attention to operations, they were observed playing electronic games, watching television or observing the sport events. This phenomenon was aggravated at venues, where Games-IS monitoring activity was less than that at the TOC. Venue Games-IS workers often left their positions and desks and idled around the venue premises, watching the sport events or chatting with others. This observation of boredom and routinization was also captured in the responses to the researcher's *Maturity of Reliable ISS Organization & Operations* questionnaire, where all respondents acknowledged that to some extent their teams were indeed bored during operational phases. The greatest levels of boredom were recorded among IT-Helpdesk personnel operating at competition venues.

When this observation was discussed with a number of Games-IS managers, they all acknowledged that this was indeed inappropriate, yet was acceptable as long as logged incidents were resolved within the SLA-specified time. The Games-ISS Risk Manager, on the other hand, disagreed. He suggested that

[163] According to Kasperson and Kasperson (1991) highly attenuated risks represent 'hidden hazards'. *Ideological hazards* remain hidden because they lie embedded in a societal web of values and assumptions that attenuates consequences, elevates associated benefits, or idealizes certain beliefs. Value-threatening hazards alter human institutions, lifestyles, and basic values.

> "this is unacceptable - especially when entire functional teams are distracted with issues that are not related to their operational roles and responsibilities. We all need to be in front of our monitors looking out for any suspicious activity. We cannot just wait for an incident to be logged and then respond to a ticket. [...] The extent to which each team consciously focuses on operations has to do with the team's attitude as well as the monitoring technologies that they have in place. If your technology allows you to look for activity that is out of ordinary, then there is more that you can do. If, however, your monitoring technology will only tell you that something is wrong after it has gone wrong, then you just wait for something to go wrong in order to get to work" (i.e. Appendix-A3:62).

However, little was done to address this risk issue. The Games-ISS Risk Manager reprimanded any Games-IS workers in the TOC that did not seem focused on their operational responsibilities, yet the state of each individual's mental alertness was difficult to detect and accordingly readjust. Thus, during the particular phase, no considerable control was implemented with regards to avoiding routinization and boredom.

A further ISS risk that was identified during the 'Implementation and Analysis' stage of the Games-ISS project was related to the lack of adequate and effective means to **measure the performance of ISS controls** and compliance to ISS operational policies and procedures. This ISS issue had been identified by the Games-ISS Risk Manager prior to the commencement of the Test Events, yet was vividly demonstrated when during the Test Events there were limited means to prioritise ISS risks and know with certainty which of all specified ISS controls had been implemented or not. Therefore, the risk profile of each Games-IS asset, venue and communication was either unknown or uncertain.

However, the collection of all necessary information with regards to the performance of and compliance with the specified ISS controls required the collaboration and input from other Games-IS functions and technologies. This input had not been provided prior to the TE-1 as the various Games-IS functions were more concerned with implementing as much as possible prior to the operational phase. In addition, the Games-ISS team had not adequately specified the ISS areas where assurance and control performance information had to be collected for.

Following the TE-1 though, priorities changed. The Games-ISS Risk Analyst worked almost full time on defining more formal ISS operational policies and procedures, and

collaborated with other Games IS functions - such as the various Technical and Operations teams - in order to identify means to collect the necessary ISS metrics information. Incrementally, she also conducted a series of monthly ISS compliance audits with regards to ISS policies and procedures. On the other hand, the Games-ISS Network Analyst reviewed the implementation of the Games network ISS controls and provided guidance as to future directions. Similarly, the Games-ISS System Analyst collected information on the build of Games devices and guided other teams on implementing systems' ISS controls. All the above information was gradually incorporated into the Games-ISS Metrics Dashboard that was communicated to most Games-IS project management team members. Finally, by the end of the 'Implementation and Testing' phase, the Games-ISS team recruited an ISS Systems Tester to commence vulnerability assessments on the Games system configurations, thus verifying the level of residual ISS risk.

Overall, throughout the various efforts to collect and analyse Games-ISS performance and compliance information, the Games-ISS team communicated that this process aimed to identify the areas of non-compliance and poor performance in order to either release more resources towards the management of the identified ISS risks, or re-assess the level of residual ISS risk. All Games-ISS members stressed that this was not a process of blame allocation, but one of collaboration and effective risk management. Lack of the necessary assurance would lead to poor ISS risk decision making and possibly the realisation of uncontrollable and dreadful risks.

One last area of ISS risk to be identified during the 'Implementation and Testing' phase of the Games-ISS project was related to the **physical security** of venues and Technology Secure Areas (TSAs). Similar to previous project phases, venuisation did not adequately improve the physical security of venues. The majority of A2004 Olympic venues were still being constructed and as such physical security controls were minimal.

In order to create the risk and threat profile of the various Games systems, the Games-ISS team required to know where each of the Games devices would be located, and what the physical security controls would be. This information - owned and managed by ATHOC that was also responsible for the construction and physical security of venues - was not readily provided. This was partly due to the unavailability of this information, and partly due to ATHOC's reluctance to provide this in hope that the SchlumbergerSema Games-ISS team would assist them with the Admin network ISS issues.

Under these conditions, the Games-ISS team had to make assumptions with regards to the physical security of venues. Given ATHOC's delays in most other areas of event preparation and venuisation, the Games-ISS Risk Manager chose to assume that physical security would not be tight until the last stages of the project. This implied that logical ISS controls had to be tightened, creating additional reasons for Games devices to be securely configured and stripped off any unnecessary and insecure device services (e.g. deactivation of removable media). This message was communicated to all Games-IS Technical and Operations teams that had to implement strict device access and network connectivity technical controls and operational procedures. They did not have to be convinced of the need to do so as a response to poor physical security, since they could all witness in person the problems in this area. In addition, they were all aware of ATHOC's project preparation delays, which created further distrust with regards to the timely implementation of adequate physical security controls.

Overall, during the Games-ISS 'Implementation and Testing' project phase venuisation and the trial and error process of Test Events further verified ISS risks that had been identified during earlier project phases. In addition, the Test Events signalled new ISS risks that had previously not - or inadequately - been considered.

From the above analysis it is evident that processes of ISS risk amplification or attenuation took place, not only affecting ISS risk perceptions, but often creating ripple effects and impacting the ways in which the Games-IS organization managed risk. Risk perceptions often differed between ISS experts and laypersons, thus determining the risk communication tactics that the ISS risk experts chose.

Therefore, risks relating to the secure configuration of Games systems and network were *amplified* by the Games ISS experts, communicating messages of dread, uncontrollability, and operational disaster. This was in direct response to the risk *attenuation* tendencies of the Games-IS Operations and Technical teams. In addition, it was observed that senior and corporate management commitment to Games-ISS assisted towards the gradual implementation of the ISS controls proposed by the Games-ISS experts.

Other ISS risks, on the other hand, often seemed to be *attenuated* by the Games-ISS experts. This was particularly evident for ISS risks that were not related to the deliverables and operations internal to the Games-IS organization. Therefore, ISS risks associated with Third Parties (i.e. Olympic broadcasters) connecting onto the Games network were indeed considered critical, yet the associated communications

and negotiations were less controversial and the Games-ISS team willingly agreed to address the related ISS risks in a step-by-step approach.

Similarly, another external-facing risk that was consciously attenuated by the Games IS(S) organization was that related to IT volunteers. Given ATHOC's intensely risk *attenuating* behaviour towards the particular issue, SchlumbergerSema chose not to make any further risk communications towards ATHOC. Instead, they focused on the logical and procedural ISS controls that they could implement in order to mitigate the risk to an acceptable level.

On the whole, it can be argued that during the Games-ISS 'Implementation and Testing' phase ISS risks that were directly related to the operations of the Games-ISS team were in their majority neither amplified nor attenuated. ISS risks that were related to the operations of other Games-IS functions were often *amplified* by the ISS experts and *attenuated* by the other functions, while ISS risks that were related to parties external to the Games-IS organization were often *attenuated* with regards to external communications, although they were commonly acknowledged within the Games-IS organization.

Finally, the repetitive nature of the Test Events and the trial-and-error process of implementation provided increasing clarity over the nature of ISS risks. As examined below, this supported the effectiveness of ISS risk communications, as well as facilitated increasing and maturing levels of organizational and operational ISS reliability and preparedness.

4.3.3.4 Organizational ISS reliability and operational preparedness

Similar to the 'Analysis and Design' phase of the Games-ISS project, a number of individuals, who represented the various Games-IS functions, were requested to score the levels of organizational ISS reliability and operational preparedness across various stages of the project's 'Implementation and Testing' phase. The findings of these questionnaires (i.e. Appendix-A10) were often discussed with the questionnaire respondents, requesting further justification of their assessments.

Prior to the August 2003 Test Events (TE-1)

From the data collected it is evident that during the period leading up to the first Test Events (TE-1: August 2003), all identified Games-ISS controls of **reliable organizational design** had been implemented, although the majority of these

controls demonstrated poor maturity levels, with patchy implementation. All questionnaire respondents identified that the organizational design control ranking highest during this phase was related to the implementation of redundancy for all critical IT assets. The lowest ranking controls, on the other hand, were related to the adequacy of resource buffers, the duplication of ISS controls and the loosely-coupled design and configuration of the Games network. The lowest ranking score during this period was provided by the members of the Games-IS Operations team - particularly the IT-Helpdesk - demonstrating perhaps the poor communication with the Games-ISS team.

With regards to the maturity of the Games-ISS controls of **reliable operational management**, this also demonstrated an improvement from previous project phases - in fact greater to that of the organizational design controls. This could be probably explained by the venuisation that took place during late July 2003, and the increasing demand for decentralised Games-IS operations. Thus from July to August 2003, ISS controls of reliable operational management improved from immature and non-existent, to significantly consistent. The highest ranking controls were related to the clear communications from management with regards to the operational and ISS priorities, as well as the need to give undivided attention to operations. The lowest scores were allocated to the existence of diverse ISS error detection and reporting mechanisms, and the existence of formal mechanisms to enhance ISS learning. Overall, the Games-ISS team members scored lower the maturity of ISS operational management controls to the rest of the Games-IS functions. This perhaps suggests that the intensifying venuisation preparations created a false confidence among ISS laypersons that attenuated the associated ISS risks.

The controls related to the **reliable ISS organizational culture** demonstrated the greatest improvement of all, with the vast majority of related controls considered to be mature and consistent. Across the various respondents, the highest ranking controls were related to the clear communications from management with regards to the organizational priorities, and the communication between diverse groups and organizations with regards to the resolution of ISS problems. The lowest ranking controls were related to the efficient identification and classification of ISS events and incidents, and the clear communication and awareness of the operational ISS policies and procedures.

It is also interesting to note that the Games-ISS experts gave the lowest scores with regards to a mature and reliable ISS organizational culture. When questioned about this, the Games-ISS Risk Analyst suggested that

> "this is probably because the other groups have not yet realized the full significance of ISS and how it affects their roles and responsibilities. They know that some ISS controls are in place, they have done their ISS training, and they probably think that this is all to it. But I am less optimistic. [...] The security culture has not yet matured in the organization" (i.e. Appendix-A3:59).

Overall, during the 'Implementation' period prior to the TE-1 both **anticipation** and **containment** ISS controls were assessed to have improved by a similar rate, demonstrating increasing levels of maturity and consistency (i.e. Appendix-A10). In addition, the team that seems to have observed the greatest improvement of both ISS anticipation and containment controls during this period is the Operations team and its IT-Helpdesk function. However, the IT-Helpdesk function also remained the only one to demonstrate complete lack of awareness with regards to some of the ISS reliability controls.

Nonetheless, it is observed that with venuisation the gap in ISS reliability perceptions between various Games-IS functions narrowed down. This finding is compatible with the above mentioned improved score of mature and consistent ISS communications between Games-IS experts and laypersons.

Prior to the October 2003 Test Events (TE-2.1)

The August 2003 Test Events (TE-1) was the first occasion when IS and ISS controls were put to the test operationally and problems with regards to the Games-ISS culture, policies, procedures and technical design and solutions were made apparent.

With regards to the maturity of **reliable ISS organizational design** it appears that that TE-1 and the ISS issues identified after these operated as a *risk amplification mechanism*, raising awareness over the nature of ISS risks and the effectiveness of ISS controls. Both Games-ISS experts and layperson suggested a drop in the improvement rates of reliable Games-ISS controls.

From discussions with the Games-IS Chief Integrator, Technical Manager and IT Integration Manager, it was evident that the great number of unauthorised devices and activity on the Games network during the TE-1, as well as the related ISS risk assessment reports that were generated in September and October 2003, all indicated that the Games network was still lacking in terms of a secure organizational and IT infrastructure design controls. Characteristically, with the communication of the ISS risk assessment results, all questionnaire respondents -

including the Games-ISS team - lowered their scores with regards to the non-existence of single points of failure across the network. In addition, out of all functions the Operations Team Manager demonstrated the greatest drop in his assessments of reliable ISS organizational design controls suggesting that

> "we now realise that that ISS management is a more complex issue than we first appreciated. [...] We are now working closer with the Games-ISS team to define secure operational procedures; and this does not only relate to the management of ISS incidents and problems, but also how we build and patch our systems, how we configure devices prior to shipping them to the venues" (i.e. Appendix-A3:65).

Unlike controls related to reliable ISS organizational design, controls of **reliable ISS operational management** improved over the period following the TE-1, although this improvement was relatively small, yet consistent across Games-IS functions. It is worth noting that a new low ranking control was related to the duplication and overlap of IS and ISS personnel where operations were critical. Over discussions with the Games-ISS Manager, the Operations Manager and IT-Helpdesk Manager, they all agreed that the TE-1 demonstrated that IT volunteers could not be trusted and were not suitable for critical IT and operational positions. Yet, due to the project cost implications of recruiting and training more Games-IS personnel at the current project phase, all above parties were pessimistic with regards to fully mitigating this risk in future Test Events.

Assessments with regards to the maturity of a **reliable ISS organizational culture** after the TE-1 were more or less similar to those prior to the TE-1. The groups that scored the reliability of the organizational ISS culture lower than before were the Technical and Operations groups, indicating their management's appreciation of the cultural ISS problems existing within their teams, which were demonstrated by a series of ISS incidents both during and after TE-1. Across all Games-IS functions, it was commonly agreed that the most recent ISS incidents had demonstrated that ISS roles and responsibilities were not fully appreciated by the various Games-IS functions and individuals, while the IT-Helpdesk Manager highlighted that IT volunteers had been completely neglected thus far with regards to receiving any Games-ISS training. Therefore, once again, ISS incidents seem to have operated as signals of ISS risk, demonstrating that prior assessments of ISS control efficiency had been exaggerated.

Overall, in the period following the TE-1 and prior to the October 2003 Test Events both **anticipation** and **containment** ISS controls demonstrated a slow down in terms of their maturity. All Games-IS functions identified that perhaps they had overestimated the effectiveness of these controls prior to the TE-1. The groups to demonstrate the greatest reduction in their maturity assessments were the Technical and Operations (including the IT-Helpdesk) groups, where most ISS incidents were observed. This reduction in maturity estimates resulted in more consistent ISS reliability scorings across all Games-IS functions, including the ISS experts.

Prior to the December 2003 Test Events (TE-2.2)

Subsequent to the August 2003 Test Events (TE-1), the next phase of 'Implementation and Testing' (and operational rehearsals) was that of the October/November 2003 Test Events (TE-2.1). Following these and in preparation for the December 2003 Test Events (TE-2.2), the maturity of reliable ISS **organizational design** controls demonstrated no change. While some ISS controls had been implemented, the majority of these were postponed such as the implementation of ACLs and the secure connection of Third Parties. Thus, single points of failure persisted in the Games network, while it was demonstrated that the Games network had serious design and configuration problems that would have to be resolved. The groups allocating the lowest scores with regards to the maturity of reliable ISS organizational design controls were the Operations and IT-Helpdesk teams.

In relation to controls of **reliable ISS operational management**, these also demonstrated minimal improvement, with a consensus in scorings across the Games-ISS functions. All groups identified that ISS management priorities were becoming increasingly clear, while operational ISS policies and procedures were frequently updated and accordingly communicated to the necessary parties.

Controls of **reliable ISS organizational culture** were the ones that demonstrated the greatest improvement during the particular project stage, although this was relatively moderate. Once again, the teams allocating the lowest scores with regards to the maturity of the organization's ISS culture were those of the Operations and IT-Helpdesk teams. Persisting problems with Third Party connectivity and a lack of clarity over the associated procedures were blamed for these relatively low scores.

Overall, during the period prior to the TE-2.2 both ISS **anticipation** and **containment** controls demonstrated only a small improvement. The groups that provided the lowest maturity scores in either case where those of the Operations and IT-Helpdesk

teams. All other teams appeared to converge with the Games-ISS experts. The above findings support prior observations with regards to the increasing tensions between the Games-ISS and Games Operations teams, while also demonstrating the poor maturity of operational ISS procedures.

With the completion of the Games-IS(S) project 'Implementation and Testing' phase

The last stage of the Games-IS(S) project 'Implementation and Testing project phase was the one subsequent to the December 2003 Test Events (TE-2.2).

As considered earlier in this study, during this period implementation activities of ISS controls were intensified. Supporting such observations, the scores provided by all Games-IS functions with regards to the maturity of **reliable ISS organizational design** controls increased over this period. However, all teams identified that although progress was evident, considerable work had to be done with regards to the complete elimination of single points of failure in the Games network and the improvement of the network's design and configuration.

Controls of **reliable ISS operational management**, on the other hand, did not demonstrate any improvement over the particular period. Across all teams decentralisation of decision making during operational phases was still not optimal, while formal mechanisms that facilitated learning from trial and error activities seemed to have become more lax.

With regards to controls of **reliable ISS organizational culture**, all teams suggested that there was no improvement during this period. The only exceptions to this were the Games-IS Operations and IT-Helpdesk teams that suggested that such controls had improved. The latter groups suggested that with the formalisation of a number of ISS procedures - and in particular the Third Party connectivity procedure - ISS roles and responsibilities were more clearly communicated and understood, while any associated problems could now be easily identified and allocated to the appropriate party for resolution.

On the whole, controls of ISS anticipation and containment demonstrated a small improvement during the last stages of the project 'Implementation and Testing' phase. The groups identifying the greatest of these improvements were the Operations and IT-Helpdesk teams that had now clarified ISS operational procedures and had improved their understanding with regards to operational ISS roles and responsibilities.

4.3.4. A2004 Games-ISS project 'Operational Rehearsals'

The Games IS(S) project phase of 'Operational Rehearsals' was distinguished in two parts. The first - between August 2003 and January 2004 - overlapped with the 'Implementation and Testing' project period. During that phase a series of Test Events took place[164] with the Games IT infrastructure supporting a limited number of operational venues and sport events. The aim of that first phase of 'Operational Rehearsals' was to implement the designed IS and ISS controls, testing that design assumptions and directions had been correct, while implemented solutions and controls were effective, acceptable, secure and reliable.

The ISS deliverables, implemented controls and incidents that took place during the first stage of the 'Operational Rehearsals' were examined in the previous section of this study (i.e. section 4.3.3). The current section will consider the ISS deliverables, controls and incidents that were observed during the second phase of the Games IS(S) 'Operational Rehearsals'.

4.3.4.1 Games-ISS deliverables, controls and incidents

The objective of this second phase was to increase gradually the number of operational venues and sport events per each round of remaining Test Events, thus increasing the operational scale and complexity that the Games IS(S) solutions had to support. The appropriateness of the Games IS(S) designs and implemented controls was expected to have been already established from the first rounds of Test Events (i.e. TE-1 and TE-2). Thus, further Test Events aimed to test performance, reliability and operational preparedness levels in an environment of increasing operational demands.

The Test Events that took place between February and June 2004 (i.e. TE-3 to TE-4) were also complemented by two rounds of Technical Rehearsals (i.e. TR-1 and TR-2). The latter tests did not involve actual sport events, but simulated ones. The Technical Rehearsals aimed to run a series of 'what-if' scenarios and evaluate the levels of IS stability, reliability and security. They also aimed to evaluate the levels of organizational and operational preparedness in case of a crisis.

The complete schedule of Test Events and Technical Rehearsals that took place between August 2003 and June 2004 is summarised below in Table 4.13.

[164] I.e. TE-1 to TE-2:2.1-2.3.

Table 4.13: *The A2004 Olympics Test Event and Technical Rehearsal clusters.*

Phases of Operational Rehearsals		Dates of Operational Rehearsals	No. of Operational Competition Venues	No. of Sports Events
TE-1	-	6 - 30 August, 2003	6	7
TE-2	TE-2.1	20 October - 2 November, 2003	2	2
	TE-2.2	15 - 31 December, 2003	2	2
	TE-2.3	14 January - 1 February, 2004	2	3
TE-3	TE-3.1	4 - 22 February, 2004	4	4
	TE-3.2	12 - 28 March, 2004	9	11
TR-1	-	29 March - 1 April, 2004	9	9
TE-3	TE-3.3	15 - 30 April, 2004	3	5
	TE-3.4	15 - 30 May, 2004	2	2
TE-4	-	4 - 12 June, 2004	4	4
TR-2	-	15 - 17 June 2004	17	35

Overall, it is observed that during the second phase of 'Operational Rehearsals' (i.e. February to June 2004) Games-ISS activities were particularly focused on ISS assurance and control fine-tuning. Games-ISS technical and procedural controls were regularly revised and communicated to other Games-IS functions, partners and customers.

The significance of change and configuration management procedures was made evident as the organization grew steeply in size and operational complexity, and coordination activities became increasingly challenging. A number of ISS incidents and re-occurring errors also demonstrated a need for effective coordination mechanisms within and across teams.

Similarly, the Games-ISS team expanded in size during the particular project phase. Two further ISS specialists were recruited to focus on Games systems and applications security testing, while during 'Technical Rehearsals' the ATHOC Admin-network ISS experts gradually joined the operations-focused Games-ISS team. This new team that operated from the TOC was renamed into the 'TOC-SEC' team.

4.3.4.2 *Contextual noise - organizational politics, culture and project phase challenges*

Similar to the 'Implementation and Testing' project phase, venuisation and 'Operational Rehearsals' required of the Games-IS functions and partners to collaborate more closely and coordinate their activities. Increasing levels of stress were identified prior to and during the project milestones such as the final round of TE-3 and the TRs.

The increased stress levels and demand for operational preparedness and reliability often led to intense arguments between Games-IS functional groups, such as the between the Games-ISS and Games Technical teams. Arguments often led to the allocation of blame, the stigmatization of technologies, groups or individuals, the increased levels of frustration and the loss of job satisfaction.

As operations expanded, so did operational complexity and a great number of configuration changes were continuously required. The great number of such changes, as well as their frequency often led to errors and miscommunications that aggravated the tense working environment.

In order to avoid such errors as well as to gradually stabilise the Games-IS environment, groups were increasingly requested to document all change requests, while impact assessments had to be carried out. However, this change in working practices often led to aggravated tensions. This in fact was one of the reasons for intense arguments between the Technical and Games-ISS teams, with the latter denying any changes without first receiving all necessary documented information. Such tension was partly overcome by the support provided by senior project management.

In addition to the above changes in the working environment, the increasing size of the organization represented further challenges for the Games-IS functions. Certain teams - such as the Network, Venue-IT Managers (VITM), and IT-Helpdesk teams - demonstrated great and continuous increases in their man-force, without however providing the new team members with adequate - if any - induction and roles and responsibilities training. Similarly, new team members did not receive consistent training on the incident management procedures or the Games-ISS policies and requirements. This resulted in poor incident management practices across the Games-IS organization[165].

[165] E.g. wrong incident profiling and delayed problem resolution.

Closely related to the above observation is the patchy performance of Venue-IT teams, and the concern expressed by the Games-ISS team after TR-1 and TR-2 with regards to not having adequately skilled persons at venues in order to efficiently and effectively resolve any ISS issues. Therefore, it was observed that IS and ISS venue incidents were often directly assigned for resolution to the TOC teams, rather than venue teams attempting to resolve these. This behaviour increased the workload for the Games IS(S) teams operating at the TOC. Meanwhile, Venue-IT teams were often observed to either be too relaxed and bored, or too stressed and lacking clear thinking.

At this point, it is significant to note that following the TE-4, TR-2 and the delivery of the audience-specific Games-ISS trainings, ISS operations at venues improved considerably. Among others, compliance of Third Parties to the Games-ISS requirements significantly improved after the completion of the training sessions. The Games-ISS Risk Analyst attributed this improvement to the training of Venue-IT Managers (VITMs) and IT-Helpdesk operators, who began enforcing the Games-ISS Third Party secure connectivity procedure.

The growth in Games-IS organizational size also affected the Games-ISS team. Two new Games-ISS members were added to the team, while from the TR-1 onwards ATHOC Admin-ISS team members started joining the Games-ISS team to form the TOC-SEC operational group. This growth in size was often problematic, with the Games-ISS team members suggesting that they had a relatively limited understanding of the activities of each team member, especially so for the two new Games-ISS experts (i.e. the Games ISS Application and System Testers). ISS risks identified by each Games-ISS team member were not communicated across the team, and it appeared that the Games-ISS Manager was the only person to be aware of most of those risks. In addition, there was no Games-ISS risk registry. The *Games ISS Risk Management* document[166] included incomplete information. This was partly due to the increasing frequency of TEs and TRs that did not provide Games-ISS experts with adequate time to record and communicate their findings to their colleagues. In addition, it appeared that the significance of such a Games-ISS risk information repository was inadequately stressed across all Games-ISS team members.

[166] The *A2004 Games ISS Risk Management* document operated as an information repository where all Games-ISS risks, controls, vulnerabilities, test-scenarios and audit/ISS-metrics findings were supposed to be logged. This document was regularly updated and it was expected to operate as a tool that would assist ISS risk management decision making during Games-time. The document was owned and updated by the Games-ISS Risk Analyst.

The formation of the TOC-SEC operational team presented a few more challenges to the Games-ISS team which soon appreciated that there was inadequate knowledge of each team's respective requirements and solutions. This led to a series of TOC-SEC cross-training sessions, stressing the need to operate in line with a unified ISS incident management procedure. Indeed, from TR-1 to TR-2 TOC-SEC performance improved, although certain problems remained, such as the over-utilization of the Games-ISS Analyst experts.

One further issue that required the Games (Atos Origin) and Admin (ATHOC) ISS teams to collaborate more closely was the problematic venue physical security. Physical security issues were not perceived by Atos Origin as their responsibility, yet they affected the quality of their deliverables and the associated ISS risk levels. The problems identified by the Games-ISS team were repeatedly reported to the ATHOC ISS Section and ATHOC IT Department, yet little seemed to change from one round of operational rehearsals to the next. Involvement of the ATHOC ISS team into the venue ISS audits, demonstrated to ATHOC first hand the problems encountered, and the problems were thus escalated to senior ATHOC management. However, once again, improvements were relatively small.

Finally, similar to the previous project phase, during 'Operational Rehearsals' the Games-ISS Risk Analyst faced difficulties collecting information for the Games-ISS Metrics Dashboard, since the rest of the Games-IS(S) members did not consider this a priority and did not provide adequate assistance. Indeed, the significance of ISS metrics seemed to lose momentum during the second phase of 'Operational Rehearsals'; these were only communicated to senior project management. The Game-ISS Risk Analyst attributed this to the organizational prioritization of operational preparedness and potentially to the change of Games-ISS team manager in January 2004.

However, the corporate structure of the Games-IS organization remained committed to and interested in Games-ISS practices, continuing the related promotional efforts. In fact, the Games-ISS Manager was increasingly involved with press and customer communications, promoting the Atos Origin Games-ISS risk management model and the newly developed SIM solution. This significantly contradicted priorities among the Games-ISS team members who did not - so far - utilise the SIM solution, as this was still under development and new to them.

4.3.4.3 Parameters and mechanisms of ISS risk amplification

During the second round of Games IS(S) 'Operational Rehearsals' the focus of ISS activities was on fine-tuning ISS technological controls, policies and procedures. This fine-tuning process was a highly interactive and repetitive one, incrementally increasing the levels of operational scale and complexity. It was based on trial and error mechanisms and aimed to deliver mature levels of ISS operational preparedness and organizational reliability prior to the August 2004 Olympic Games. Therefore, this was the period when the Games-ISS team had to ensure that ISS communications were effective, thus contributing to the optimisation of the ISS technological and procedural controls.

As in the previous project phases, the researcher utilized the SARF in order to capture the areas of ISS risk identified and communicated by the Games IS(S) project organization during the second phase of 'Operational Rehearsals'. These ISS risks are summarised in Table 4.14 below. Once again, similarities are identified with regards to ISS risks detected during earlier stages of the Games IS(S) projects (i.e. Tables 4.11 and 4.12).

Therefore, following the completion of the TE-2, one of the first ISS problems to be identified by the Games-ISS team was the **poor levels of compliance with ISS policies and procedures**. In fact, all Games-ISS team members acknowledged that during the particular project phase there were very few mechanisms in place to verify ISS compliance levels. The Games-ISS Manager noted that

> "we do not know where we stand. We need to start implementing more ISS assurance controls that will verify our level of ISS posture" (i.e. Appendix-A3:75).

As such, from February 2004 onwards the Games-ISS team invested considerable amounts of their time and resources creating ISS checklists, audits and test scenarios, frequently interacting with other Games-IS functions and partners. In addition, two new members were added to the team in order to conduct Games systems and applications ISS testing respectively. The Games-ISS Risk Analyst suggested that the presence of ISS assurance controls operated as a feedback mechanism to the ISS management and communication processes, informing the update of ISS policies and procedures, technical controls and further communications. However, she also noted that the implementation of ISS assurance mechanisms was not always supported by all Games-IS(S) personnel, who seemed to consider it a low priority relatively to the logistical and device installation activities

required prior to each round of operational rehearsals. This, however, was to change as further rounds of Test Events indicated that incidents - such as mis-configurations - were often repetitive and caused by the inadequate existence of ISS assurance controls and checks (i.e. Appendix-A3:81).

Table 4.14: *Games-ISS risks identified and communicated during the 'Operational Rehearsals' (February to June 2004) project phase.*

	Games-ISS Risk Area
1	Patchy **compliance with ISS policies and procedures**.
2	Inadequate knowledge of the **Games-ISS policies and procedures** content by many Games-IS workers and partners.
3	Security vulnerable **Games systems and applications**.
4	Persisting unauthorised **Games network communications**.
5	Inconsistent compliance of **Third Parties** with the Games network secure build and connectivity policy and procedure.
6	Insecure build of Games **laptops**; they are also inconsistently updated with anti-virus definitions.
7	**Mis-configurations of ISS** management and monitoring devices and ISS controls.
8	Inadequate/non-existent information on the **physical layout of venues** and the physical placement of Games IT devices.
9	**Ineffective communication between Games ISS team and Venue workers**.
10	**Incorrect configuration of IT devices** at venues and absence of any configuration checks by venue IT teams.
11	**Poor physical security** of venue IT areas and devices
12	Poor performance of **Games ISS monitoring platform**
13	**Mis-configuration and disconnection** of Games ISS devices generating **inadequate alarms**.
14	Poor **incident management collaboration** between **Venue-IT** workers and TOC-SEC team
15	Poor **incident management collaboration** and coordination **within the TOC-SEC** team
16	Problematic **incident profiling and resolution assignment** of IS(S) incidents by non experts
17	**Inadequate duplication of TOC-SEC team skills**, resulting in inefficient incident management practices.
18	Problematic update of Games ISS **anti-virus solution**, negatively impacting the **performance of OVR** systems.

Once further ISS assurance controls were established it was made evident to the Games-ISS team that poor **ISS policy and procedure** compliance was greatly due to the **inefficient communication** of these across the various Games-IS functions and

partners. As suggested in an *ISS Venue Audit Report* completed by the Games-ISS Risk Analyst and communicated to the Games-IS management team, "not everyone seems to be aware of the presence or content of ISS policies and procedures. This is especially the case for persons working at competition venues". The cause of the problem was partly the mechanism of ISS policy and procedure communication. Until April 2004, each Games-IS function manager was sent an electronic copy of the Games-ISS policies and procedures that were relevant to their team's activities. Beyond that point, each function manager was responsible of communicating the content of these policies to their team members. However, these communications usually were nothing more than a mere announcement that new ISS policies were released and that each individual was responsible of familiarizing themselves with its contents; most individuals did not.

In addition, as Games-IS functions increased in scale, the new team members were often not informed of the Games-ISS requirements. This partly explains a further ISS risk observation with regards to the **poor communication of ISS policies and procedures to Venue workers.** The majority of new Games-IS workers were employed to man the Games-IS team across the competition and non-competition venues. They were therefore located across the various, decentralised Olympic venues and did not have daily face-to-face communication with their colleagues, function management and Games-ISS team. Thus, the *Games-ISS Venue Audits* demonstrated that Games-IS employees, volunteers and partners operating from venues had the poorest knowledge and understanding of ISS polices and procedures. The significance of ISS requirements had not been attenuated by them, it had been inefficiently communicated to them.

Following the identification of the particular problem by the Games-ISS team, the latter communicated more closely with the management of other Games-IS functions in order to raise their awareness over the particular problem. In addition, during ISS audits the Games-ISS experts would communicate the content of the ISS policies and procedures to the persons and teams audited. Furthermore, Venue-IS workers were requested to refer to the Games-ISS policies and procedures when in doubt, or to directly contact the Games-ISS team. More importantly, however, the Games-ISS Risk Analyst commenced the preparation of audience-specific Games-ISS manuals, checklists and trainings. The preparation of this work was coordinated with the Games Operations team, while the training presentations were delivered from May 2004 onwards to small-sized audiences, encouraging questions and interaction. The Games-ISS training presentations did not only address the audience-relevant ISS

policies and procedures, but also raised awareness over ISS threats and best practices. Presentations concluded with a message of collaboration, stressing that secure IS practices were a common, organization-wide responsibility. Overall, these presentations were well received, particularly so where the ISS training presenter encouraged interaction and asked or gave real, A2004 Games-IS examples.

However, reception of Games-ISS training messages was occasionally problematic. During periods of intense negotiations between the Games-ISS team and other teams - such as the Technical ones - members of the training audience would react negatively. Such reaction was not as much directed towards the content of the training presentations, but more towards the training presenter and the Games-ISS team in general.

The ISS risk that created the most intense of arguments and negotiations during the 'Operational Rehearsals' phase was related to the implementation of network access controls. Throughout operational rehearsals it was identified that **Games systems and applications had several ISS vulnerabilities.** These were either detected during the various rounds of 'Operational Rehearsals', or by the Games-ISS experts that conducted security tests. The Games-ISS team collaborated with the various Games Technical teams to mitigate as many as possible of the system and application ISS vulnerabilities, however not all could be addressed within the remaining project timeframe. They, therefore, suggested that the implementation of Games network security controls was imperative in order to mitigate or contain the security vulnerabilities. However, the constantly changing ISS requirements and the growing size of the Games Network team implied that the implementation of ACLs was very problematic, with several configuration errors impacting the operational performance of the network. Such problems and errors were identified during Test Events and under conditions of *time pressure*, when it appeared difficult to coordinate a secure solution. Therefore, the ACLs were repeatedly removed and - as in the Test Events conducted during earlier project phases - they were *stigmatised.* ACLs were labelled as unnecessary and dangerous, and a cause of operational disasters. The Games-ISS team on the other hand, was labelled as paranoid and regimental.

The truth of the matter was that **network communications** within the Games network **remained undisciplined**, and several unauthorised activities were repeatedly observed. In addition, the implementation of ACLs was often the only technical means to contain a system or application security risk. The tension between the Games-ISS and Technical/ Network teams was overcome to a great

extent with the engagement of senior project management in the debate. The support they demonstrated towards the activities of the Games-ISS team led to the increased coordination between the various teams. In addition, the Games- ISS team Manager instructed his network ISS experts to conduct more checks themselves with regards to the correct implementation of ACLs and not leave this activity entirely to the Network team engineers. Where mis-configurations were identified, the Games-ISS team Manager personally raised the issue with the Network or Technical Team Manager and oversaw the problem's resolution. Thus, this added level of authority appeared to ease the intensity of arguments, and gradually the Games ACLs were correctly implemented across venues. Furthermore, the Games-ISS team delivered a relevant training to all Games Network engineers, familiarizing them with the Games-ISS network requirements and procedures.

Another persisting ISS problem identified during the second round of 'Operational Rehearsals' was that related to the **secure connectivity of Third Parties** onto the Games network. Once again, this problem was evident during Test Events, when Third Parties connected onto the Games network. Despite direct communications between the Games-ISS team and Third Party representatives with regards to ISS requirements, Third Parties consistently did not comply with these. Third Parties, therefore, appeared to *attenuate* the associated ISS risks. The Games-ISS team proceeded with defining a few more Third Party secure device build and connectivity checklists, policies and procedures, and the Games-IS Chief Integrator suggested that these are communicated via ATHOC. It was hoped that adding this level of communication formality would convince Third Parties that ISS was not an issue to be considered lightly. However, compliance to the related ISS requirements remained low. Later, during venue ISS audits, it was identified that this was partly due to the poor knowledge of the related policies and procedures by Games-IS venue workers, who had to conduct the related compliance checks. This problem was greatly overcome by implementing a number of ISS controls. Firstly, the Games-ISS team provided to each Venue-IS team a *Third Party Secure Device and Connectivity Checklist*. In addition, rather than completely delegating the responsibility of these checks to the Venue-IS workers, the Games-ISS team was also centrally involved in this process. Finally, a set of ISS trainings to Third Parties and the various Venue-IS experts also seemed to significantly improve the levels of compliance.

A further ISS risk that persisted during this project phase was related to the **insecure build of Games laptop devices**. Throughout the various rounds of Test Events it was made evident that laptops connecting onto the Games network were not always built

according to Games-ISS requirements. In addition, these Games devices were not always updated with the latest anti-virus definitions.[167] These problems were not detected via any specific ISS incident, but rather via Games-ISS monitoring activity during operational rehearsals. Given the mobility of such devices, it was considered imperative by the Games-ISS team that all users connecting their laptops onto the Games network were identified, and the devices were securely configured. Thus, the Games-ISS team took action by first identifying all Games-IS workers, partners and Third Parties that were using a laptop. Once this was done, a newly drafted *Secure Laptop Policy and Procedure* were communicated via email to all laptop users and the Operations team. Accompanying these was a *Secure Laptop Checklist* that was utilised by the various organizations to securely build their devices, while the IT-Helpdesk and Games-ISS teams used these to conduct device audits. However, the uptake of this policy and associated process was overall slow, and it was not until before TR-2 when compliance levels improved. This was greatly due to the inefficient communication of the *Secure Laptop Policy* and *Procedure* to the Venue-IS workers. As identified earlier, Venue-IS workers were often not aware of the Games-ISS policies and procedures applicable to their roles and responsibilities, and thus did not apply the necessary ISS assurance checks. However, as soon as the Games-ISS training sessions commenced, a considerable improvement was evidenced with regards to secure laptop compliance levels.

The secure build and connection of Games laptops was not the only security issue concerning these devices. Most **physical security** incidents were also related to the theft of laptop devices; clearly the mobility of these contributing towards the ease of theft. This problem was partly addressed by distributing K-locks to Games laptop users. Other than this control, however, the overall level of physical security at the Olympic venues remained relatively poor, although some improvement was witnessed as venue construction preparedness matured.

Another ISS risk that was related to Atos Origin's dependence on the deliverables of ATHOC IT was related to the provision of adequate and accurate information with regards to the **physical layout of venues** and the **physical location of Games IT devices**. This is a problem that persisted from previous project phases. Since no particular improvement was evident, the Games-ISS team chose to overcome this

[167] On a daily basis the Games anti-virus servers pushed the latest definitions to all Games devices at a specific time during the day. If laptop devices were not connected onto the Games network during that particular time of the day, they would not be updated with the latest anti-virus protective controls.

problem by identifying themselves the venue physical security controls. This was done during the Venue ISS Audits, which indicated that physical security controls were poor thus far; both in terms of robust venue construction and access controls. The issues were raised with the ATHOC-ISS team that was encouraged to participate in the venue audits. The problems were eventually escalated to ATHOC Senior IT Management, while the requested information with regards to the physical IT device layout at venues became gradually available before TR-2. However, by that time the Games-ISS team had already chosen to strengthen the logical ISS controls of Games IT devices, thus leading to an overall more costly solution.

The collaboration between the Games-IS and ATHOC IT organizations was also problematic when the Games-ISS and Admin-ISS teams were joined into one operational team, the TOC-SEC group. Due to the inadequate number of Games-ISS experts that would cover all necessary shifts during operational phases - and later Games-time, the Admin-ISS team was gradually integrated into the Games-ISS one. However, the addition of new ATHOC-ISS team members initially created great operational confusion and **poor ISS incident management practices**. This was greatly attributed to the lack of ATHOC-ISS training on the Games-ISS incident management process, requirements and controls. Therefore, prior to TR-2 the relevant training was delivered to all TOC-SEC members, and indeed ISS incident management performance improved.

However, poor ISS incident management practices were identified to be caused by a number of additional reasons. The Technical Rehearsals demonstrated that Games-IS functions and the IT-Helpdesk often **classified and assigned ISS incidents inaccurately**. In addition, ISS incident management **collaboration between the TOC-SEC group and the Venue-IT groups** was mostly poor, with little communication between them. Both these ISS issues were addressed during the ISS training sessions, when the Games-ISS team members had the opportunity to present in person the ISS policies, procedures, incident management process, roles and responsibilities. These sessions were often interactive, and the training audience was encouraged to raise questions and give examples from their personal experience. During these sessions it was also possible for the Venue-IT workers to meet various members of the Games-ISS team, which was suggested to have improved communications between the TOC-SEC and Venue-IT teams. According to the Games-ISS Risk Analyst,

> "after the security training presentations the Venue-IT teams can put a face to a name. The next time that they have a security problem, they will be less hesitant to call us and directly communicate with us. It is good for us too,

since we also get to meet the people that are working at venues. The security training presentations and the occasional venue audits that we do are the only ways for us to meet the people working at the competition venues. [...] When you are on the phone with someone from a venue and you are trying to resolve a problem, it makes things a bit easier if you have actually met before the person you are talking with. Knowing what the venue looks like also helps" (i.e. Appendix-A3:85).

However, there was one problem with regards to ISS incident management performance that the Games-ISS team did not seem to address. This was related to the **inadequate duplication of TOC-SEC team skills and responsibilities**, particularly with regards to the management of Games-ISS network controls. Each of the three TOC-SEC shift teams covered three roles, namely the TOC-SEC Duty Manager (1-per-shift), the Games-ISS and Admin-ISS Administrators (2-per-shift), and the Games-ISS and Admin-ISS Incident Analyst (2-per-shift). However, as seen in Table 4.15 below, the expertise of the Games-ISS experts was not well distributed and duplicated among shift teams. This resulted into the poor allocation of team workload and ISS incident management activities - especially so when there were multiple and simultaneous ISS incidents that needed to be investigated and resolved. The outcome was that certain shift members were stressed while others were too relaxed, and ISS monitoring was often neglected. Possibly more important, however, was the fact that ISS network and system problem management skills were not duplicated. As such, during TR-2 it was demonstrated that Shift-#3 could not resolve any network ISS problems. Instead, they had to either wait for the next shift, or had to keep another ISS Administrator on-call.

Although the above problems were made evident across all Test Events and Technical Rehearsals, no substantial action was taken by the Games-ISS team; even after the Technical Rehearsal Officers' (TRO) Manager documented and communicated to senior Games-IS management that the structure of the TOC-SEC team needed to be revised. The Games-ISS Manager suggested that "*there is little we can do and change now. We do not have enough time to train everyone in everything. But this should not be a major issue. By Games-time the entire environment will be fixed and stable. We do not expect any major network and system security configuration changes*" (i.e. Appendix-A3:88).

Table 4.15: *Games ISS experts, roles and responsibilities of the A2004 TOC-SEC shift teams.*

TOC-SEC Role & Responsibilities		Skills of TOC-SEC Members		
		Shift #1	Shift #2	Shift #3
ISS Duty Manager	ISS incident response management	Experienced	Some experience	Minimal experience
	External team communication & escalation	Experienced	Some experience	Minimal experience
	ISS network & system problem management	Some experience	No experience	No experience
ISS Administrator	ISS network & system problem management	Experienced in *network* problem management	Experienced in *network* problem management	Experienced in *system* problem management
	ISS incident response	Some experience	Experienced	Minimal experience
	Intrusion detection monitoring	Experienced	Experienced	Some experience
ISS Incident Analyst	Intrusion detection monitoring	Some experience	Some experience	No experience
	ISS incident response	Some experience	Experienced	Minimal experience
	Update on ISS alerts & vulnerabilities	Experienced	Experienced	Minimal experience

Further ISS risks that were identified were related to the **wrong configuration of ISS and Games IS devices.** The continuous operational changes, new IS(S) requirements and significant logistical operations prior to each round of Test Events and Technical Rehearsals led to a number of errors and omissions, often causing stress and tension within and between teams. This was aggravated by the lack of adequate device configuration checks by the Venue-IT teams, resulting in the eventual creation of Venue-IT configuration checklists, as well as the creation of related checklists for the Games-ISS team at the beginning of each operational shift.

As examined earlier, the problematic configuration of ISS devices and controls escalated to its worst with regards to the implementation of ACLs, leading to the *stigmatization* of the ISS technology and Games-ISS team. Meanwhile, the real ISS risks - namely the problematic and uncoordinated configuration of ACLs by the

Games Network team and the lack of adequate ACL version control and assurance checks by the Games-ISS team - were *attenuated.*

In addition, during the Technical Rehearsals it was identified that the mis-configuration and disconnection of Games-ISS devices generated **inadequate ISS monitoring alerts**. Thus, the Games-ISS team decided to formally add regular checks in the shift activities of both the TOC-SEC and Venue-IT teams. These checklists were communicated across the necessary persons and groups via email communications and formal training sessions.

Finally, the various rounds of operational rehearsals pointed to a few performance problems of the Games-ISS devices. Specifically, the **Games-ISS monitoring platform repeatedly failed**, impeding the Games-ISS team from monitoring communications both within and at the perimeter of the Games network. This was considered to be a significant problem for the operations of the Games-ISS team, not however directly affecting the reliability and performance of the Games critical services. Technical tests were defined in collaboration with the technology provider and eventually this problem was fixed.

An instance, however, where a Games-ISS technical control directly impacted the performance and reliability of Games-IS critical services was in relation to the **interaction of the anti-virus technology and the OVR** (On-Venue-Results) system. From the early stages of the TE-3 it was identified that whenever the anti-virus server pushed new definitions to all Games-IS devices, OVR devices failed and stopped working. The OVR devices had to be manually restarted to operate normally again. This was quickly identified as a problem that could not be fixed, and it was therefore agreed that OVR devices would have a dedicated anti-virus solution, where the related server would push new anti-virus definitions on a weekly basis only after a Change Request was raised and agreed with the OVR system owners. As such, operational and performance problems would be avoided, and definition updates would be restricted to periods when the systems were not supporting a Games sport event. It was also agreed that following TR-2 no further anti-virus updates would take place on the OVR systems, unless an emergency was identified and a Change Request was approved.

Overall, during the period of 'Operational Rehearsal' the process of trial-and-error considerably assisted the process of ISS risk identification, indicating that ISS communications and management became increasingly problematic as soon as the organization moved to a decentralised operational model. In addition, as the

organizational operations and structure became greater in size and complexity, continuous changes were required with regards to the ISS management controls, in order to accommodate a dynamic environment. This high degree of repetition and change often led to errors and omissions, raising stress and/or frustration levels which created tense inter- and intra-organizational relations and interactions. Hence, this organizational environment frequently led to the amplification or attenuation of ISS risks. Direct communication of the Games-ISS experts with their target audience, and the direct involvement of the ISS experts in assurance activities and processes often assisted with the improvement of the overall ISS management levels and practices. However, even ISS experts demonstrated to be prone to biased judgements and occasionally downplayed or amplified ISS risks.

4.3.4.4 Organizational ISS reliability and operational preparedness

The findings from the organizational ISS reliability and operational preparedness questionnaire during the second phase of 'Operational Rehearsals' are considered in more detail below (i.e. Appendix-A10).

Up to TR-1: February to March 2004

Following the completion of the TE-2 in January 2004 and the end of the 'Implementation and Testing' phase of the Games IS(S) projects, no improvement was observed with regards to levels of **reliable organizational ISS design**. All related ISS controls demonstrated partial and immature implementation, with the IT-Helpdesk Manager allocating the lowest scores out of all his colleagues, suggesting that his team had a very poor understanding of the Games-IS interactions, ISS needs and status of implemented controls. The highest ranking control across all questionnaire respondents was related to the implementation of component redundancy for all critical IT assets.

However, with the approaching first Technical Rehearsals (TR-1: March to April 2004) and their completion, some improvement was suggested by most Games-IS groups. The Games-ISS group, however, did not consider any improvement to have taken place. The persisting ISS problems with the secure Third Party connectivity, the secure build of Games-IS devices, and the Games network configuration problems, indicated to the Games-ISS team that the implementation of the necessary organizational ISS design controls remained inconsistent. The only other

organizational role that did not consider any improvement to have taken place by the completion of TR-1 was the IT-Helpdesk Manager.

Contrary to controls of organizational design, the controls of **reliable ISS operational management** demonstrated a steady improvement during the period leading up to the TR-1, and an overall greater level of maturity. The role that suggested the greatest improvement was that of the IT-Helpdesk Manager, who observed an increasing collaboration and coordination between his team and the Games-ISS team with regards to the enforcement of the Games-ISS operational procedures.

However, controls of **reliable organizational ISS culture** did not fare as well as those of operational management. Instead, throughout the period leading up to the TR-1, a deterioration was observed. This was attributed by all Games-IS members to the increasing number of organizational employees and the lack of any ISS training and communication controls to integrate them into the existing organizational ISS culture. Questionnaire respondents identified that Games-IS employees - particularly those operating from venues or the newly-joined ones - were often bored or did not feel confident to make any decisions. In addition, the Games-ISS team members identified that the ISS policies and procedures were still poorly understood by all Games-IS groups and external partners, with compliance levels remaining relatively low.

During the same project phase, both **ISS anticipation** and **containment controls** did not demonstrate any particular improvement. This was a period of continuous changes and updates of existing controls, with Games-IS(S) team members often perceiving no change in levels of organizational and operational maturity and stability.

Prior to TR-2: April to June 2004

During the last rounds of TE-3 and prior to TE-4 (June 2004) the maturity of **reliable organizational ISS design controls** improved significantly. The end of the TE-3 signalled for the various Games-IS teams the need to finally achieve some level of stability, with ISS technologies, policies and procedures, and communications becoming increasingly consistent and clear. The only related control that continued to demonstrate low maturity was related to the elimination of single points of failure. Such risks were identified by the Games-ISS team members to be both technological and procedural, such as the insecure build of devices and the non-compliance of Third Parties with the Games network secure connectivity procedure.

In addition, the IT-Helpdesk Manager identified that his team was still lacking adequate understanding with regards to the interactions, criticality and ISS controls of the Games network and applications. This was greatly due the increasing size of his team during this period, and the lack of any formal ISS - or otherwise - training. Indeed, it was not until late May of 2004 that the Games-ISS team started delivering a series of audience-specific ISS trainings.

On the other hand, the maturity levels of the **reliable ISS operational management controls** remained overall stable during this period, with a considerable number of related controls demonstrating maximum maturity, especially so with regards to the maturity of the Games ISS policies and procedures and the establishment of mechanisms that supported learning via mechanisms of trial and error.

With regards to controls of **reliable organizational ISS culture**, these also demonstrated an improvement, especially so during the period just prior to TR-2. All questionnaire respondents identified such an improvement, greatly attributing this to the delivery of formal ISS training. In addition, levels of routinization appeared to have dropped as operations picked up pace and Games-IS workers were better informed and prepared with regards to there IS(S) responsibilities.

Overall, throughout the project phase leading up to TR-2 both **ISS anticipation** and **containment controls** improved considerably, especially so as the final round of the TE-3 was completed and the Games-IS project management team demanded organizational and operational stability.

After TR-2: June 2004

Following TE-4 and TR-2 all ISS controls of organizational reliability and operational preparedness demonstrated increasing levels of maturity.

Once again, the **organizational ISS design control** that demonstrated the highest level of maturity across the questionnaire respondents was related to the presence of component redundancy built into the IT infrastructure for all critical assets. In addition, all teams demonstrated improved levels of understanding with regards to the interactions, criticality and implemented ISS controls of Games applications, systems and network. The most notable improvement was that recorded for the IT-Helpdesk team. Therefore, perceptions of organizational ISS design reliability levels converged.

Similarly, and in fact demonstrating even greater levels of maturity, the operational **ISS management controls** improved significantly by the end of the 'Operational Rehearsals' period, with all Games-IS functions agreeing on their assessments. The lowest score was given by the Games-ISS Risk Analyst who suggested that the decentralisation of decision-making authority remained problematic as venue operators often hesitated to resolve problems themselves and re-assigned their resolution to the central TOC teams.

With regards to **controls of a reliable organizational ISS culture**, these also demonstrated increasing levels of maturity and consistency, with the members of Games-ISS team allocating the highest scores and the Games Operations and IT-Helpdesk teams allocating the - relatively - lowest ones.

Finally, both **ISS anticipation and containment controls** demonstrated improvement, resulting in similar levels of maturity.

4.3.5. A2004 Games-ISS project 'Event-time'

With the completion of the A2004 Games IS(S) 'Operational Rehearsals' project phase in June 2004, the project organizational environment entered a final period when the status of operational IS(S) settings and controls were verified. Olympic competition and non-competition venues were gradually security 'locked down', while functional teams gradually moved to a fully operational work mode of shifts.

As the A2004 Games-time approached (13th - 29th August, 2004), there was decreasing emphasis on the activities, deliverables and controls anticipating ISS risks. Instead, there was an increased attention towards the efficient containment of IS(S) incidents, and the capture of all relevant information required for the effective real-time risk and incident management decision making.

Games-time was a period when operational Games IS(S) scale and complexity reached their peak, and all related preparations were put to the test. As the focus of the organization shifted towards the management and containment of IS(S) incidents, so did the researcher's attention.

4.3.5.1 *Games-ISS deliverables, controls and incidents*

With the completion of the Games-ISS 'Operational Rehearsals' the ISS testing activities did not entirely terminate. Various ISS tests and checks were conducted at this stage of the project by the Games-ISS team in collaboration with a number of other Technical and Operational Games functions[168]. In addition, some further Venue-ISS Audits and ISS training sessions were conducted.

As for ISS incidents that were detected during this period, these demonstrated significant similarity to problems detected at earlier project phases. Prior to the Games, most ISS incidents were in fact change requests of ISS-device configurations, while some mis-configurations were also detected and corrected. In addition, Third Parties and Games-IS partners also demonstrated non-compliance to certain Games-ISS policies and procedures. With the assistance of the Venue-IT teams, these problems were - in their majority - timely addressed.

Finally, the Games-ISS incidents that were detected during Games-time did not have any severe impact on the Games-IS services, and were overall contained. These are summarised below in Table 4.16.

Table 4.16: *Games-ISS incidents during A2004 'Event-time' (13^{th}-29^{th} August, 2004).*

Type of Games-ISS Incidents	No. of Games-ISS Incidents/ No. of Total Games-ISS Incidents
Severity 2 (major impact) Games-ISS incidents	1/101 (1%)
Severity 3 (minor impact) Games-ISS incidents	38/101 (38%)
Severity 4 (investigation-only) Games-ISS incidents	62/101 (61%)
ISS control configuration change/correction	29/101 (29%)
Unauthorised/out-of-ordinary Games network traffic	22/101 (22%)
Account management policy errors & violations	21/101 (21%)
Wrong Games device configuration and build	8/101 (8%)
Unauthorised device disconnection/connection	5/101 (5%)
ISS hardware malfunctioning	5/101 (5%)
Physical security violations	5/101 (5%)
Games network intrusion/spoofing attacks	2/101 (2%)
Accreditation policy violations	1/101 (1%)
Other	3/101 (4%)

[168] E.g. some technical test were conducted to ensure the correct configuration of Games-ISS ACLs, the security of several critical Games applications and systems, and the secure build and BIOS settings of Games-IS devices.

4.3.5.2 *Contextual noise - organizational politics, culture and project phase challenges*

During the period immediately prior to the A2004 Games and during the 17 days of the event the Games-IS(S) organization experienced an almost complete shift from functional organizing to venue and operational organizing. Games-IS operations were completely decentralised, while the operating environment reached its greatest scale and complexity, yet demonstrated relative stability (i.e. Table 4.9).

The Games-ISS team continued some of its functional activities during early July 2004, yet by the end of the same month it was joined by the Admin-ISS experts and was completely transformed to a 24-by-7 operational structure of three TOC-SEC shift teams (i.e. Table 4.15). Its operations were not decentralised to the same extent as for other Games-IS functions, since the TOC-SEC monitored all ISS activity centrally from the TOC. However, the Games Technical and Operational experts operating from the competition and non-competition venues acted as TOC-SEC assistants with regards to installing and configuring Games-ISS devices and controls at venues. In addition, they were greatly delegated the compliance monitoring of ISS operational policies and procedures, such as the *Third Party Connectivity Procedure* and the *Secure Laptop Policy*.

The physical lock-down of Olympic venues from mid-July 2004 onwards, signalled that security controls were becoming stricter, and coincided with increased levels of compliance with the *Secure Third Party Connectivity* policy and procedure. Yet, the lock-down of venues and the increased ISS alertness of Venue-IT teams also raised the TOC-SEC's attention to a further risk with regards to the non-compliance of Olympic IT Partners (i.e. SWATCH) with the *Secure Laptop* policy[169].

The immense logistical project of preparing within a matter of a few days the IT infrastructure of all A2004 Games venues also led to several errors and omissions, with IT devices being shipped to the wrong venue, or IT devices (including ISS devices) being wrongly built and configured.

Therefore, during the period immediately prior to the A2004 Games, as well as during the Games, the majority of ISS problems were related to the incorrect build of

[169] In brief, SWATCH had assumed that since they were a Games-IS trusted partner, they did not have to comply to the Games-ISS *Secure Laptop* policy. This led to some last minute tension and negotiations between Atos Origin and SWATCH. They finally agreed that some of the *Secure Laptop* checks would be implemented, while non-compliance to some of the secure-build requirements would have to be accepted since there was inadequate time to change all of these.

Games devices by the Software Distribution team[170], which had inconsistently security hardened Games devices and inconsistently implemented device BIOS restrictions. In addition, mistakes with regards to the incorrect configuration of ACL and port security controls on the venue switches by the Network engineers persisted.

Overall, what appeared to significantly improve prior/during the A2004 Games was the compliance level of the procedural ISS controls. Technical and configuration errors appeared impossible to completely eliminate. Yet, these errors did not create tension between the TOC-SEC team and the other functional/operational teams as had happened previously. Problems were resolved in a collaborative and mostly efficient manner. The urgency of the 'live' Games did not allow for such political arguments.

Instead, during the particular project period tensions seemed to increase *within* operational teams, whether that was the various Venue-IT and TOC-IT teams. Similarly, increased tension was observed within the TOC-SEC team, particularly between different shift teams. Team loyalties seemed to shift from a functional (i.e. Games-ISS team) level to an operational (i.e. TOC-SEC shift team) level.

TOC-SEC team #2 and #3 (i.e. Table 4.15) often expressed their frustration with regards to the inequitable distribution of Games-ISS skills and administrative privileges. They both expressed that

> "the TOC-SEC shifts had to be rearranged and all shifts should have administrative access to all Games-ISS management platforms. But it seems that all [the Games-ISS Manager/TOC-SEC team-#1 Duty Manager] cared about was to keep the best security engineers on his team" (i.e. Appendix-A3:94).

In addition, arguments were often observed between individuals across TOC-SEC teams, especially between persons that held the same role across shifts. Relationships between shift-teams became more competitive and it appeared that - to one extent or another - they all wanted to avoid being blamed for any ISS problems and poor ISS incident management practices. The Games-IS Chief Integrator later noted that

> "this is normal behaviour. Some shift teams will always be stronger than others, and none of them wants the extra workload or responsibility. Keep in

[170] The A2004 Games Software Distribution team was a function of the Games-IS Operations, Central Operations group (i.e. Appendix-A7), along with the IT-Helpdesk, PC-Factory, and IT-Training.

mind as well that for most Games-IS workers their employment contract will end by the end of the Games, and if they are to get a contract renewal they have to ensure that nothing happens on their watch. They are all competing for a future job against their colleagues" (i.e. Appendix-A3:96).

It thus appears that in terms of their future job security each Games-IS(S) worker was more threatened by their teammates, than by the members of other teams.

The sense of competition between the Games-ISS TOC-SEC members was particularly evident with regards to the several Atos Origin Games-ISS marketing and promotional presentations that took place during this period. The Games-ISS members competed with one another for an opportunity to make one of these press presentations/interviews and thus also promote their own contribution to the project.

Furthermore, both during Games-time and later in the completed *A2004 ISS Risk Management* document[171] it was made evident that the members of the TOC-SEC team attenuated the ISS risks and problems caused by their own operations, and amplified the errors and ISS risks caused by other operational groups, or beyond the TOC-SEC team's jurisdiction - for example, the physical security problems. Such behaviour was particularly driven by the Games-ISS Manager.

Finally, during this period it is worth noting that significant levels of routinization, boredom and tiredness were observed both at competition venues and the TOC, particularly during the evening/early hour shifts (i.e. 19.00-7.00). IS(S) monitoring and checks often did not take place and after 12-hours on shift teams were often keen to leave than stay behind and ensure thorough shift hand-over. Routinization was greater for the less skilled TOC-SEC members that relied on their more experienced and skilled colleagues to carry out all necessary ISS management and monitoring activities. Such routinization often led to a delayed incident management response.

4.3.5.3 Parameters and mechanisms of ISS risk amplification

The 'Operational' phase of the A2004 Games-IS(S) project was a time when the focus of every Games-IS function was on the logistical preparations of the 60 operational Olympic venues and the smooth execution of the 'event'. The goal was for the

[171] I.e. footnote #164.

Games-IS(S) infrastructure to invisibly and reliably support the A2004 Games. Therefore, the majority of ISS risk signals that were witnessed during this period were originated from Games-time ISS events and incidents (i.e. Table 4.16). These Games-time ISS incidents also signalled to the Games IS(S) organization the extent to which their event preparations were adequate and their prior ISS risk perceptions valid. The areas of ISS risk identified during this project are summarised below in Table 4.17.

Table 4.17: *Games-ISS risks identified and communicated during the 'Operational' (July to August 2004) project phase.*

	Games-ISS Risk / Incident(s)
1	**Mis-configured Games ISS** technical controls.
2	ISS vulnerabilities and design flaws of critical **Games applications**.
3	Problematic **ISS incident allocation and escalation** procedures among ISS non-experts.
4	Problematic **physical security** despite some improvements after venue lock-down.
5	Non-compliance of SWATCH with the Games ***Secure Laptop* Policy**.
6	Violations of Games ISS **account management policies**.
7	Problematic **TOC-SEC incident management communications** and coordination.
8	Inadequate **duplication of skills** and administrative privileges across TOC-SEC shift teams.
9	Lack of adequate **ISS assurance checks** with regards to the correct configuration of the Games-ISS technical controls.
10	Attempts to connect **unauthorised devices** onto the Games network.
11	**Unauthorised disconnection** of Games devices.
12	**Performance problems**/ malfunctioning of Games-ISS technical controls.

All of the above ISS risks were identified both prior and during the A2004 Games, although often during Games-time there was a different urgency to their management. The same ISS risks that were tolerated to an extent during the project's preparation phase, were *amplified* during Games-time and had to be urgently managed. For example, the **mis-configuration of Games-ISS controls** by either the Games-ISS team or the Technical teams was a common problem, yet this was far less tolerated during Games-time.

In fact, such ISS problems led to tensions between or within teams. While during the project preparation phases entire functional teams were responsible of implementing

and configuring a particular IS(S) control, during Games-time this responsibility became the responsibility of specific individuals, according to their operational roles. Thus, errors and omissions often led to personal arguments during Games-time.

In addition, there appeared to be a tendency across the various functional or operational teams to hide any IS(S) risks identified at the last minute, in knowledge of the inability to change the IT infrastructure and in fear of being blamed for any omissions. This phenomenon was exposed after the Games, when Games-IS employees felt less threatened from admitting to errors and 'hidden' IS(S) risks.

Therefore, ISS risks related to the **poor design practices of Games applications**, or the **inconsistent or wrong implementation of Games network ISS controls** were attenuated during Games-time, in hope that any related incidents would be quickly detected and contained. Even within the TOC-SEC team knowledge of ISS risks was greatly departmentalised, and it was only after the completion of the *A2004 ISS Risk Management* document and the completion of the A2004 Games event that a more complete picture of ISS problems was available.

This departmentalised knowledge of Games IS(S) problems and controls also had an impact on the efficiency and effectiveness of **incident management practices**, via the slow detection of problem causes, the slow resolution of incidents, and the inadequate or excessive allocation of Games-ISS incident management resources.

However, the interaction between Venue-IT experts and the TOC-SEC team improved during Games-time, demonstrating a close coordination and collaboration in the detection and resolution of ISS incidents. This resulted in improved ISS incident management practices. The TOC-SEC team was better equipped to identify centrally problems related to the **configuration of Games-ISS network controls**, the **unauthorised connection of devices** on the Games network, the **violations of account management policies**, and the **performance problems of Games-ISS devices**. On the other hand, the decentralised Venue-IT teams could locally detect any non-compliance problems to **procedural and physical ISS controls**. Furthermore, the Venue-IT teams played a key role in verifying any ISS problems detected by the TOC-SEC team, and containing or resolving these locally. Therefore, the Venue-IT teams often acted as an effective ISS communication channel to the various IS partners and customers at the venue.

The contribution of Venue-IT teams to the enforcement of ISS management controls was particularly useful in detecting and managing the ISS problem related to the last-minute device connectivity requirement of IT Partner, SWATCH. Although **SWATCH**

had been communicated and trained on all Games-ISS operational policies and procedures - including the *Secure Laptop* policy - they had mistakenly assumed that they could connect their laptops onto the Games network without prior ISS compliance checks from the ISS and Venue-IT teams. Although SWATCH put considerable pressure on the Venue-IT teams to grant them access to the Games network, the Venue-IT personnel declined their requests and timely escalated the matter to the TOC-SEC team and senior project management. The problem was finally resolved with a formal agreement between Atos Origin, ATHOC IT and SWATCH, where the latter would comply with the majority of the Games *Secure Laptop* requirements, while the Venue-IT teams would conduct all necessary and agreed compliance checks.

Apart from the above observations with regards to specific ISS risks identified immediately prior and during Games-time, a number of further observations were made by the researcher with regards to the ISS risk attention and sense-making processes. As noted earlier, attention was raised towards the ISS controls of risk containment, such as the improvement of incident management communications and practices. The *Games ISS Incident Management* policy and procedure were updated prior to the Games, in order to provide clearer guidance to the classification and escalation of Games-ISS incidents. Moreover, during Games-time it was made evident that the lack of **TOC-SEC duplicated administrative privileges on the Games-ISS controls** was creating problems with regards to the efficient management of ISS incidents. Hence, this was addressed by allowing a member of each TOC-SEC shift team to have full access to the Games-ISS management controls. The fact that this known problem was not addressed prior to the Games is perhaps indicative of the Games-ISS Manager's false confidence in the stability and correct configuration of Games-ISS controls during Games-time.

The delayed detection and resolution of several **wrong control configuration** ISS incidents can be also attributed to the false confidence that TOC-SEC members had in the skills of their colleagues and the adequacy or effectiveness of ISS assurance controls. Related ISS incidents during Games-time indicated that complacency and boredom often resulted in mistakes, which were often hidden from other teams.

It is also interesting to note here that - similar to previous project phases - boredom was acknowledged by all respondents to the researchers' *Maturity of Reliable ISS Organization and Operations* questionnaire, yet little was done to address this issue. Games IS(S) personnel were rarely reprimanded for not paying full attention to their

operational management and monitoring responsibilities. The Games-IS Chief Integrator suggested that

> "everyone gets bored at some point when on shift. Especially the night shifts. Nobody really gets told off, because we all feel bored and tired at times. [...] Yes, this can lead to problems; especially as the Games approach their conclusion and we all tend to get a bit more relaxed. On the last two days of the Games we had a few severity-1 and -2 incidents and nobody addressed them until hours later, because most people were not at their posts monitoring what is happening" (i.e. Appendix-A3:96).

Another observation with regards to ISS risks during Games-time was related to expected risks, yet their unexpected interaction. As stated earlier, all ISS risks and incidents identified during Games-time were previously known and, therefore, partly expected. What, however, was not expected was the way in which a technical risk/incident could be combined with a procedural and behavioural ISS risk, thus leading to the amplification of the total risk experience. For example, the ISS incident summarised in Appendix-A11 was a combination of a wrong Games-ISS control configuration, the poor incident management and communication practices within the TOC-SEC team, the inadequate duplication of skills and administrative privileges across TOC-SEC shifts, and the lack of adequate and effective ISS assurance checks.

ISS incidents such as these often amplified perceptions of risk or indicated that perceptions of risk had been previously attenuated. This is demonstrated in the responses to the researcher's *Maturity of Reliable ISS Organization and Operations* questionnaire considered below. For example, although overall ISS containment controls improved prior to Games-times, a number of ISS incidents raised awareness over certain risks (e.g. the lack of Games ISS skills duplication) and led to particularly low ISS reliability scorings. This can be greatly attributed to the contextual noise at the time, where the upcoming Games decreased error tolerance levels and the increased availability of ISS risk information *amplified* risk perceptions.

Similarly, although prior to the event it was acknowledged that the Games applications suffered from certain design and security flaws, these were then assessed to be overall acceptable and containable. However, after the Games and with a series of critical Games application failures, the same risks were scored higher and the reliability of application ISS controls - although no application security

incident took place - was scored lower. Clearly, the contextual noise of the Games and the realization that IS design risks can interact and compromise the availability of IT services, also *affected* assessments with regards to the security of Games applications.

Overall then, it is observed that immediately prior and during Games-time increased attention was given to the fine-tuning of ISS risk containment controls. The lack of adequate time to make any further significant changes to the Games-ISS management controls implied that newly identified risks could not be entirely corrected, but restricted.

In addition, the approaching 'Event' made the organization less tolerant to mistakes, which often led to the *amplification* of ISS risks. However, the imminence of the Games also made functional/operational teams more cooperative and any last minute problems were addressed in a coordinated, results-focused manner. The escalation of any such problems to senior project management also speeded up related decision-making.

However, tension and the allocation of blame increased *within* teams. This also applied to the TOC-SEC team, which often demonstrated an orchestrated effort to hide risks from non-experts and resolve problems internally. Such tension and any associated mistakes were often aggravated by the increasing levels of tiredness and boredom, and the inequitable distribution of responsibilities and skills within teams.

Finally, it is worth emphasizing that Games IS(S) configuration changes did not stop before or during the A2004 Games, demonstrating the constantly changing and complex business requirements, while associated errors and omissions also persisted. In fact, the interaction of various such errors and ISS risks often led to unexpected outcomes and the *amplification* of ISS incidents and risks.

4.3.5.4 Organizational ISS reliability and operational preparedness

As summarised in Appendix-A10, after the A2004 Olympic venue lock-down and the freeze of the Games IS(S) environment and soon after the completion of the A2004 Olympic Games event, a number of Games-IS(S) team representatives were asked - as previously - to score the level of organizational ISS reliability and operational preparedness.

The researcher expected that the August 2004 findings would indicate the greatest level of ISS control reliability, while the September 2004 findings would reflect ISS risk perceptions after these had been put to the test during Games-time. The actual responses to the *Maturity of Reliable ISS Organization and Operations Questionnaire* are summarised below.

Just before the A2004 Olympic Games (early August 2004)

The maturity level of **reliable ISS organizational design** controls did not demonstrate any significant change from the period following the completion of TR-2. The only improvements were suggested by the Games-ISS Architect and Games-IS Technical Team Manager who argued that after the final round of Technical Tests and controlled configuration changes, their understanding of the Games systems and network interactions, interdependencies, ISS needs and implemented controls had improved.

With regards to the maturity level of **reliable ISS operational management** controls, this also demonstrated a small improvement with a number of Games-IS functional managers suggesting that attention to operations had improved along with the degree to which decision making migrated to where expertise was.

However, it is interesting to note that during this period the Games-ISS Risk Analyst who was predominantly occupied with collecting a variety of ISS risk information and drafting the *A2004 Games ISS Risk Management* document[172], did not entirely agree with her colleagues. She suggested that the key IS(S)personnel was not adequately duplicated where operations were critical, pointing out that TOC-SEC team-#3 demonstrated a particularly poor performance with regards to ISS incident management practices. She also questioned the effectiveness of the organization's formal mechanisms with regards to enhancing ISS learning from trial and error activities. Specifically she suggested that

> "formal mechanisms are in place, but these are not always effective. For example, TR-2 demonstrated that the operational model of the TOC-SEC team needs to change, yet it has not. The TR-2 also indicated that across all shifts there must be at least one Games-ISS expert that has full access to the Games-ISS monitoring and management tools. This has not changed either" (i.e. Appendix-A3:93).

[172] I.e. footnotes 164 and 169.

Yet, the rest of her team members and organizational colleagues did not seem to acknowledge this issue as a problem.

Similar to ISS controls of reliable operational management, all Games IS(S) team representatives suggested that the maturity level of **reliable ISS organizational culture** remained overall stable prior to the Games. According to a number of respondents minimal improvement was demonstrated in areas such as the degree to which Games-IS personnel was encouraged to question normal system, network and people activity, and to elaborate on their ISS incident response capabilities.

Once again, the only questionnaire respondent that suggested that the organizational ISS culture had deteriorated was the Games-ISS Risk Analyst. She argued that the latest Venue ISS Audits had demonstrated the ineffectiveness of the Games-ISS training efforts with regards to particular target groups, such as Third Parties, IT Partners and IT volunteers.

Overall, with regards to the maturity level of Games **ISS anticipation and containment controls**, almost all respondents suggested that this had slightly improved. The only exception to this assessment was the Games-ISS Risk Analyst.

Immediately after the completion of the A2004 Olympic Games (early September 2004)

Following the completion of the A2004 Olympic Games, all respondents to the researcher's questionnaire suggested that all types of reliability ISS controls did not demonstrate any improvement during Games-time. Quite the contrary, all types of ISS reliability controls were assessed as less mature than prior to the Games, indicating perhaps that prior to the event the Games IS(S) personnel were more confident of the controls' maturity. The actual event and the problems encountered during this, either *amplified* perceptions of ISS risk or attenuated confidence in the effectiveness of ISS controls.

Thus, with regards to the ISS controls of **reliable organizational design** the majority of questionnaire respondents agreed that the clarity over the Games applications, systems and network interactions, interdependencies, ISS needs and implemented controls had been overestimated prior to the A2004 Games event. The area where the reliability of ISS controls appeared to have been overestimated the most was related to the Games applications. The Games-IS Chief Integrator suggested that:

> "prior to the Games, the technical area that we were most confident about was the Games applications. They had been used before in the Salt Lake

Winter Olympics and we did not face then any major problems. What changed the most in the Athens Games was the network architecture and design, and this was everyone's greatest concern. But it turned out that the network controls performed better than all the rest. The applications that we had trusted the most gave us the greatest trouble" (i.e. Appendix-A3:96).

It is interesting to note that during Games-time no ISS incident was experienced with regards to the Games applications, but rather there were severe problems with regards to their performance under the great load of Games-time user requests. Nonetheless, the above perception expressed by the Games-IS Chief Integrator was shared among the various Games functions and the ISS reliability levels of the Games applications demonstrated a reduction.

The above perception with regards to the poor understanding of the Games applications also explains the lower score in September 2004 with regards to the adequate component redundancy that was built in the IT infrastructure for all critical assets.

Controls of **reliable ISS operational management** also demonstrated lower levels of maturity after the Games. Questionnaire respondents suggested that during Games-time it was demonstrated that there was inadequate duplication of key IS(S) personnel where operations were critical. It was suggested that this often impacted the efficiency and effectiveness of incident management practices. In addition, the Games-IS Operations Team Manager suggested that the Games-ISS policies and procedures were not communicated to all parties as effectively as assumed prior to the Games. This assessment was made in reference to the laptop connectivity problems that were encountered at the last minute with SWATCH.

Finally, with regards to **controls of reliable ISS organizational culture** the majority of questionnaire respondents identified that the levels of routinization increased during Games-time. In fact, they acknowledged that this phenomenon often resulted in reduced vigilance and a delayed response to incident management requests.

Overall then, immediately prior to the A2004 Olympic event all ISS reliability controls - aside from the ISS containment controls - did demonstrate their greatest level of maturity. However, with the completion of the Games, although the event was considered to be overall successful from an IS(S) point of view, the problems encountered during the event led to lower ISS control reliability scores than prior to the Games. This applied to both ISS **anticipation and containment controls.**

4.3.6. A2004 Games-ISS project 'Closure'

The overall successful completion of the Games IS(S) projects was concluded with a series of After Action Review (AAR) reports and meetings that lasted a few days. Among other Games-IS topics that were addressed by this formal mechanism of learning and information collection, the performance of the Games-ISS function and TOC-SEC operational team were also considered.

All members of the Games-ISS team attended an AAR meeting and had to complete a related report which addressed a number of Games-ISS topics as considered below.

Firstly, all Games-ISS team members agreed that the implementation of the ISS controls was more challenging that initially expected. This was greatly attributed to poor activity coordination with non-ISS teams, especially the Games Network team. The Games-ISS Manager suggested that

> "the relationship with the Games Network team was very difficult. There was an unclear reporting on the status of their ongoing activities, and we often had to substitute the Network team in the investigation of difficult network issues. These problems have created tensions and feelings of injustice within the Games-ISS team".

He identified that the cause of these problems was that

> "the majority of the Network team members were not experienced, leading to many wrong configurations. Also, the decision-making and -tracking processes were very obscure" (i.e. Appendix-A3:95).

The Games-ISS team members, however, identified that their relationship with the rest of the Technical teams had been relatively good, and these teams had been very proactive in terms of ISS.

An ISS control implementation area that was identified as problematic by all Games-ISS experts was related to the **Access Control Lists** (ACLs). The Games-ISS Manager argued that

> "all ACLs at venues were implemented as planned. Nevertheless, the efforts required to define, implement and test the ACLs has been much greater than expected, requiring management attention and support to be completed" (i.e. Appendix-A3:95).

Several reasons were identified as responsible for this situation: a lack of accurate data flow requirements; the inability to test early due to the delayed readiness of venues and the late start of some applications, forcing the Games-ISS team to frequently re-deploy ACLs; and the lack of a centralised management system.

Furthermore, the Games-ISS team also addressed their **interaction with the Games IT Integration team**. The latter group was supposed to work with the Games-ISS team to determine the 'ordinary' Games traffic flow, thus determining the ACL requirements. The Games-ISS experts suggested that there was an initial disconnect between their team and the Integration team. This was identified to improve after TR-1, when joined tests were organized between the two teams. In addition, all Games-ISS members agreed that there was a gap between the technical teams and non-technical teams of the project. As stated by the Games-ISS Manager,

> "the IT Integration and Operations teams do not speak the same language as the Technical and Security teams. Cross-functional testing can definitely help in creating a common language and fine-tuning security controls" (i.e. Appendix-A3:95).

With regards to interactions with the Games IT Integration team, the Games-ISS team also considered the issue of **system and application stability**. They agreed that the application security and performance tests had been inadequate in relation to excessive legitimate traffic, resulting in the failure of certain Games systems during event-time.

In relation to the implementation of **procedural and training ISS controls**, the Games-ISS team identified that account management issues should be addressed in greater detail, while more thorough auditing procedures should be added for both technical and non-technical policy statements. They also identified that there was a need to increase the number of venue Games-ISS visits for auditing and training purposes. The Games-ISS Manager suggested that

> "communication with the Venue-IT teams is key to the success of any ISS investigation performed at venues. [...] Their training has helped strengthen their collaboration with us. More venue visits should be organized for ISS auditing and training purposes. The ISS audits should also ensure that partners' equipment is considered" (i.e. Appendix-A3:95).

During the AAR meeting the Games-ISS team also discussed the **ISS monitoring** practices during Games-time and the implementation of the SIM solution. The Games-ISS Manager suggested that

> "we aimed to implement a SIM solution in order to filter, aggregate and correlate the security alarms generated by the Games IT infrastructure. The implemented system has received approximately 5 million alarms from which it has extracted 450 high alerts and 22 critical ones. We feel that the solution has performed very well and that we have achieved our objectives. [...] A SIM solution should be definitely implemented at Games events. In the future Games we need to fine-tune the correlation rules with the help of the Technical teams" (i.e. Appendix-A3:95).

However, not all team members agreed with the above view. The majority of Games-ISS team members suggested that they rarely used the SIM solution to monitor the Games IT environment during Games-time. The reasons for this were their relative unfamiliarity with the solution and the fact that alternative IT monitoring solutions had been used throughout the project preparation phases.

During the AAR Games-ISS team meeting, the participants also addressed issues related to Game-IS operational procedures. With regards to the **change management process** they all agreed that change requests should include a section describing all interdependencies, since in several instances the Games-ISS/TOC-SEC team approved new functionality without knowing there was a resulting ISS control configuration change requirement. Furthermore, the Games-ISS team agreed that there was inadequate change management coordination after a change had been approved. No quality checks were implemented.

Similarly, the Games-ISS team also identified a number of problems in relation to the **configuration management process**. They highlighted their last minute discoveries prior to the Games with regards to the insecure and inconsistent build of certain devices, while they argued that their assurance activities were impaired by the lack of a central repository which could track versions of the different configurations they managed. The Games-ISS Manager recommended that

> "we need to implement a number of things; a central repository to store configurations; a central auditing system to check the configurations in place; and a global configuration management system. We also need to organize more system audits and tests" (i.e. Appendix-A3:95).

Following the numerous account management policy violations that took place during Games-time, the team also reviewed the **account management process**. They all agreed that there were inadequate account management controls to support the complexity of the Games environment. In addition, matters were aggravated by the fact that there were too many people who joined the organization at the last minute, with too many different roles, each requiring several types of access.

Finally, during the AAR meetings that followed the conclusion of the A2004 Olympic Games event, the Games-ISS team reviewed issues related to the **TOC-SEC staffing and shift schedules**, as well as the **collaboration with the Admin-ISS team**. All team members agreed that the 24-by-7 shift schedule with a 12-hour shift for each team was not adapted to the real level of Games activity. Night-time activity was significantly less to that of the day-time shift, therefore inefficiently utilising the team's resources.

With regards to the team's collaboration with ATHOC's Admin-ISS team, the Games-ISS Manager suggested that

> "joining the Games- and Admin-ISS teams was expected to allow the Games-ISS experts to leverage resources and improve operational effectiveness. Time was invested in training each team, yet the return was very small. The Games-ISS solution was so complex that there was not enough time to get the Admin-ISS experts up to speed. [...] The OCOG's ISS team should not be joined with the Games-ISS team in the future. Instead, Atos Origin employee volunteers should complement the Games-ISS team" (i.e. Appendix-A3:95).

Although the majority of the Games-ISS experts agreed with this view, the two members of the second TOC-SEC team suggested that they had a relatively productive collaboration with the Admin-ISS experts on their shift. They argued that bringing in Atos Origin employee volunteers at the last minute would not add any valuable expertise to the TOC-SEC team as there would be inadequate time to train them on the Games-ISS solutions. Instead, they suggested that there should be indeed greater ISS expertise duplication within the Games-ISS team; perhaps a more costly solution, but a more security effective one.

All above ISS issues and lessons learned were recorded and made available to Atos Origin's Executive Major Events organization that would proceed with organizing and delivering the next Olympic Games' IS infrastructure. The Games-ISS project was relatively successfully completed, the last goodbyes were said, and two of the seven Games-ISS team experts continued on to work in the next Olympic Games event.

4.4 Emergent issues

As presented in Chapter 3 of this study, this research focuses on understanding the organizational processes of change that establish reliable ISS operations in a major event context. This study adopts a contextualist analysis perspective which identifies vertical and horizontal levels of analysis and the interconnections between those levels through time. Therefore, the research's empirical findings have considered the Games-ISS project organization's deliverables, controls and incidents, the contextual surroundings, the identified and managed ISS risks, and the organizational reliability levels as these were identified across linearly structured project phases.

This section of the study considers any emerging patterns with regards to the above parameters of vertical analysis. It aims to horizontally and vertically summarise findings prior to proceeding to the research's *Discussion* section, where these findings are then analysed in terms of the three levels of organizational risk encounters,[173] while SARF and High Reliability Theory predictions are contrasted with actual results.

4.4.1. Emergent issues on the A2004 Games-ISS project deliverables, controls and incidents

With the commencement of the A2004 Games-ISS project two issues were dominantly evident. Firstly, the project initiated later to the related Games-IS Integration project. This implied that several of the project IT infrastructure foundations[174] had been put in place prior to the Games-ISS analysis, design and implementation activities. Secondly, it was clear that the local OCOG and the IOC had not considered previously the strategic scope and value of an Olympic ISS plan. Provisions of ISS services were not covered in the *METER* contractual arrangement between the TOC, ATHOC and their international TOP IT sponsor, SchlumbergerSema.

The above two structural and contextual factors determined the set of Games-ISS deliverables upon project commencement. Intense negotiations took place on a senior management project level, defining an Olympic ISS Strategy and the interactions between the Games- and Admin-ISS teams, as well as the Games-ISS

[173] As presented in all previous chapters of this study, the concept of 'organizational encounters with risk' is introduced by Hutter and Power (2005b), and it refers to the ongoing process of organizational risk identification, sense-making and re-organization.

[174] E.g. the Games application's design requirements and the Games network architecture.

expert and the rest of the Games-IS Integration project functions and organizational structure.

Efforts were made by the Games-ISS expert to jointly address Olympic ISS issues with ATHOC. Yet, the lack of adequate leadership and coordination mechanisms from ATHOC's side, and the lack of binding contractual agreements between ATHOC and SchlumbergerSema led to a shift in project focus, and the Games-ISS expert concentrated on the ISS practices of the Games systems and network, which was also considered of greater criticality.

The need to do so was stressed further by the visible implications the late involvement of a Games-ISS expert had on the Games-IS Integration project. The lack of strategic consideration of ISS issues within the Games-IS infrastructure had led to increased project costs and/or a compromised solution security and reliability.

Therefore, the deliverables and controls implemented during the Games-ISS project 'Initiation' and 'Analysis and Design' stages changed from an Olympic-wide focus to a Games-network one. Planning and design activities - the majority of which were implemented only once - dominated the early Games-ISS project phases, while interactions with the Games-IS functions increased. The implementation of any Games-ISS controls during the early stages of the project was conducted by Games-IS Technical teams with the guidance of the Games-ISS experts. However, no ISS assurance controls were yet implemented and no operational ISS policies were yet created and provided.

It was with the expansion in size of the Games-ISS team and its shift towards a project implementation mode that the Games commenced implementing Games-ISS management controls, ranging from ISS policies and procedures, to an ISS metrics framework and Games network ISS technical controls. The implementation of Games-IS(S) controls peaked prior to the first A2004 Games operational rehearsals and was greatly dependent on the construction readiness of the Olympic competition venues, which was problematic. A delay in venue readiness, implicated the timing of control implementation and the opportunity to conduct adequate tests prior to operations.

The majority of the Games-ISS deliverables and controls that commenced during the project 'Implementation' phase continued throughout the 'Operational Rehearsals' too. The increased interactive complexity and the involvement of additional organizations in the Games IS(S) preparations implied that ISS controls had to be continuously revised. The late delivery of competition venues also implicated the extent to which tests could be conducted and assurance controls timely

implemented. In addition, the operational rehearsals operated as a mechanism of ISS risk attention, raising awareness over ISS issues that had previously not been considered, planned for and managed.

Interactions with other Games-IS functional groups and organizations became more tense as the operational rehearsals activities moved to their second phase of Technical Rehearsals, and operational and organizational size and complexity increased. The heavy workload of every function implied that prioritization was not always similar for all involved parties. Mutual adjustment mechanisms were no longer adequate to coordinate activities, nor was the standardization of processes. ISS assurance controls aimed to verify the standardization of outputs. This was particularly difficult to achieve with a lack of centralised management controls, such as system and network configuration systems. Also, the increasingly decentralised organization structure implicated the extent to which the Games-ISS team could manage ISS behaviours, processes and technologies across competition venues. Reliance on the Venue-IT teams increased, while training and audit ISS controls proved significant tools in establishing a working relationship with them.

The second phase of the Games-IS 'Operational Rehearsals' also meant the gradual integration of the Games- and Admin-ISS experts into one TOC operational team. This change in organizational structure primarily aimed to allow the Games-ISS experts to leverage resources and improve operational effectiveness. However, the effectiveness of this control was later debated. The great operational complexity of the Games-IS(S) environment impaired the effective transfer of knowledge to the Admin-ISS experts that had no practical experience with regards to the management of the Games network and ISS controls.

Games IS(S) operations peaked during the Games 'Operational' phase, when interactive complexity was relatively high, yet stable. However, although the Games-IS(S) project 'Operations' phase was meant to coincide with a 'freeze' of the Games network/IS environment, IS(S) tests and last-minute configuration changes continued, as well as a number of ISS assurance checks.

During Games-time, ISS project deliverables were reduced to a minimum, while no new Games-ISS controls were implemented, merely updated as required. The 'Event' project phase was a period when almost full attention was given to the efficient and effective management of Games IS(S) incidents.

The ISS incidents experienced and identified during this period were greatly similar to events experienced during the project's 'Operational Rehearsals' phase, indicating

two things. Firstly, the prolonged period of operational testing and technical rehearsals was indeed an effective process to identify Games IS(S) problems. Secondly, the fact that these ISS incidents were repeated, yet contained during Games-time, indicated that certain ISS risks were hard to manage and eliminate. Nonetheless, their effective containment during Games-time avoided any major ISS disaster[175].

Overall, Games-ISS planning and baseline-definition project deliverables reached their peak during the project 'Analysis and Design', and 'Implementation and Testing' phases. The Games-ISS planning deliverables that were revised most frequently and throughout the project's lifecycle were related to the Games ISS incident management requirements and processes.

On the other hand, Games-ISS management controls were mostly implemented during the project's 'Implementation and Testing', and 'Operational Rehearsals' phases. The latter phase, was greatly dominated by the implementation and fine-tuning of Games-ISS controls that were dependent on the work activities and behaviours of other Games-IS functions and collaborating organizations. This inter-dependency and need of coordination often created tensions and the delayed or patchy implementation of Games-ISS management controls. This was the project period when ISS assurance controls and processes were of critical importance.

Finally, Games-ISS project incidents took place throughout the Games-ISS 'Operational Rehearsals', often leading to significant breaches of security and a compromise of the Games network IS services' reliability and availability. Games-ISS incidents continued into 'Games-time', yet problems were overall contained - although with varying levels of effectiveness and efficiency. The ISS incidents that took place indicated that perhaps the greatest challenge for this project was the coordination of Games-ISS management activities with other groups, and the adequacy of ISS assurance controls.

[175] The same could not be wholly argued for the rest of the Games-IS project, since a number of high severity incidents during Games-time did impair the performance, reliability and availability of certain Games-IS services. However, this is not discussed here as it is not within the scope of this study.

4.4.2. Emergent issues on the A2004 Games-ISS project contextual noise

Across the A2004 Games-ISS project lifecycle it was made evident that the evolving organizational structure, culture and politics often determined the outcome of ISS management efforts, and vice versa.

Firstly, the poor appreciation by the IOC and ATHOC with regards to the strategic need and value of ISS management implied that this was not a Games-IS deliverable that was explicitly included into the METER contract[176]. This resulted in the relatively delayed involvement of an ISS expert in the Games-IS Integration project and the **delayed initiation of the Games-ISS project**. This was aggravated by the numerous initial negotiations with regards to the budget to be allocated to the Games-ISS project, as well as which organization would cover this cost.

In addition, when the project was initiated there was an unclear definition of ISS management roles and responsibilities within SchlumbergerSema, as well as between ATHOC and SchlumbergerSema. As such, considerable time and resources were spent during the early stages of the Games-ISS project in order to create an Olympic-wide ISS strategy and clearly allocate roles and responsibilities across and within organizations.

Furthermore, the relatively late initiation of the Games-ISS project implied that Games-ISS design and configuration requirements were provided after most Games-IS applications, systems and network had been implemented, or their design foundations had been set. This often resulted in the delayed implementation of Games IS(S) solutions that were often costly, or with compromised security levels.

Aside from the implications of the late project initiation, the Games-ISS project was greatly dependent on the collaboration and coordination of its experts and activities with various other groups and organizations.

With regards to the collaboration of the Games-ISS project function with **ATHOC** and the Admin ISS experts, this evolved throughout the project's lifecycle. Despite initial intentions by the Games-ISS experts to coordinate the various Olympic ISS initiatives with their ATHOC colleagues, it was soon made clear that this would not be possible. The relatively poor skills, work coordination and leadership practices of ATHOC delayed ISS management decision-making. Hence, once the Olympic ISS Strategy was

[176] The *METER* contractually bound the TOP Olympic sponsors to the IOC, requiring the TOP sponsors to provide a set of free Olympic services in exchange for corporate and solution marketing opportunities generated from the Olympics.

defined between ATHOC and SchlumbergerSema, the Games-ISS experts became increasingly disengaged with the activities of the Admin-ISS team.

Yet, the Games-ISS project remained dependent - to an extent - on the deliverables and organizational culture of ATHOC. For example, ATHOC never provided the Games-ISS experts with their business ISS requirements and Games-IS asset criticality assessments. This resulted in the Games-IS organization basing their decisions on related assumptions. In addition, ATHOC was responsible for the timely preparation of the competition venues and their physical security controls. The delayed delivery of Olympic venues implied that there was less opportunity to test Games IS(S) systems at the venue. In addition, with less time to install and configure the Games IS(S) controls at venues, SchlumbergerSema's/Atos Origin's venue logistical preparations were made harder, often leading to errors and omissions. Little time was left to conduct all necessary checks prior to (test) operational phases.

Furthermore, the last minute enforcement of Olympic venue physical security controls meant that the Games-ISS experts often had to make assumptions with regards to these. With a '*no space for error*' approach, the Games-ISS experts opted to assume poor physical security and hence strengthen the logical security of Games IS(S) systems. This was clearly a more costly option.

The Games-ISS experts also expected ATHOC's support with regards to the communication of operational ISS policies to Third Parties and other IT partners. It was hoped that this approach would add a greater degree of formality to these communications, and thus improve compliance levels.

Finally, ATHOC was responsible for the timely provision of appropriately skilled Games IS volunteers. Delays in the identification and provision of such volunteers meant that several of them did not receive any Games-IS(S) training, nor did they have desktops at the venues to work from. As an effect they often had to share Games-IS credentials with other users in order to be able to do their job.

The groups, however, that the Games-ISS team had to collaborate with the most were the other **Operations, Technical and Integration** functions of the Games-IS Integration project. While interactions were initially informal and within an environment of relaxed team-working, this changed as the Games-ISS project entered its 'Implementation and Testing' phase. Teams had to collaborate closely and timely coordinate their deliverables as they were greatly dependent. As the first Test Events approached, venuisation led to an increased workload for all teams, each of which had different priorities. Stress levels increased and often tensions developed

between teams. The lack of adequate and accurate information often led to errors and operational problems.

Such tensions were aggravated as the Operational Rehearsals progressed and further Games-ISS controls and restrictions had to be implemented. Negotiations extended beyond the accurateness and necessity of Games-ISS controls. They often became political debates of power and blame allocation between teams.

Thus, the Games Integration team did not particularly collaborate with the Games-ISS team until the later stages of project preparation as they assumed that their re-used applications were secure and reliable. The Games Operations team, on the other hand, collaborated with the ISS experts just before the commencement of 'Operational Rehearsals', when organizational focus shifted towards operations. This was frequently a problematic relationship as the Operations professionals did not always appreciate the need for various technical ISS controls and the reasons behind any operational ISS problems. In addition, the problematic configuration and change management processes also generated various miscommunications and coordination problems. These issues also affected interactions with the Technical teams, which varied across project phases and across Technical specialists. The interaction with the Games Network team was the most problematic, particularly as the latter group grew in size and new uncoordinated, inadequately skilled and trained engineers joined the team.

Tensions, however, were often overcome after issues were escalated to senior project management, which was overall committed to Games-ISS. In addition, the introduction of further ISS assurance controls also helped towards timely detecting errors. As for tensions across Games-IS teams during Games-time, the urgency and criticality of the Event meant that there was little opportunity to allocate blame, and focus shifted to the efficient and effective resolution of a crisis.

Apart from collaborating with Games-IS functional teams, the Games-ISS experts also had to coordinate Games-ISS controls with **Venue-IT teams** during project operational phases. The implementation of Games-ISS technical and procedural controls across the Olympic venues was solely dependant on the Venue-IT teams, none of which had any particular ISS skill and experience. As such, the collaboration with these teams was often problematic, particularly so with regards to the management of ISS incidents and the implementation of ISS assurance controls. There was poor decentralisation of ISS problem solving practices, which increased

the TOC-SEC team's workload and left them with little time to conduct any ISS monitoring.

However, the above changed over time as further practical experience was obtained by the Venue-IT teams and role-specific ISS training was delivered to them. In addition, the venue ISS audits improved collaboration between the Games-ISS experts and the Venue-IT workers, raising their overall technical and procedural ISS awareness.

In addition to the various Games-IS Integration project teams, the Games-ISS experts also had to collaborate with a number of external organizations, such as other IT partners (e.g. SWATCH) and IT customers (e.g. broadcasters).

Collaboration with **IT Partners** was occasionally problematic as they had their individual practices and greatly retained their organizational and operational autonomy. IT Partners were involved in all Games-ISS meetings and communications that were relevant to their activities and deliverables, while they also joined in the various rounds of 'Operational Rehearsals'. However, as demonstrated earlier, coordination was not always ideal. ISS incidents occasionally indicated poor communication between organizations and a wrongly assumed level of trust. They also indicated that Games-ISS assurance controls with regards to IT Partners had been more lax throughout the project lifecycle.

Collaboration with **Third Parties** was even more problematic, particularly during the project preparation phases when they repeatedly did not comply with the Games-ISS secure device connectivity and build requirements. This was greatly due to a relatively lax enforcement of these requirements by the Games-IS(S) organization, which was concerned with dissatisfying the Olympic revenue providers. In addition, the lack of adequate checks from the Venue-IT teams also aggravated the problem. However, by Games-time compliance levels improved significantly and no problems were identified.

From the above it is evident that **venuisation** and the approach of the Games added momentum to the delivery of Games-ISS controls. There was a greater incentive to make and coordinate decisions, and efficiently resolve problems. In addition, venuisation changed Games-ISS communications and collaboration patterns across teams and organizations.

In fact, venuisation and the Games also altered collaboration patterns within the Games-ISS team. A change from a functional (Games-ISS) to an increasingly

venue/operational team structure of shifts (TOC-SEC) created new roles and responsibilities, often distracting the team members from their work and reducing their motivation levels. Therefore, during the early phases of venuisation, stress levels increased and difficulties were experienced with regards to prioritizing Games-ISS tasks. Further on, as operational rehearsals progressed and operational complexity increased, so did the number of changes and levels of associated frustration. Finally, during Games-time, internal Games-ISS tensions were not reduced, especially so as the inequitable distribution of skills and administrative privileges aggravated these. It was observed that Games-ISS colleagues were increasingly competitive and did not acknowledge their mistakes. Concerns of future job security increased as the project approached its end.

A further observation made during operational phases and Games-time was the existence of boredom and tiredness, particularly during the night shifts. As examined in section 4.3.5 these two phenomena often led to errors and omissions. In addition, the logistical scale and complexity of preparing the IT infrastructure across the venues before the Games also led to a number of errors, which were detected throughout the Games 'Operational' project phase. However, in most cases, such errors did not create tension between teams during Games-time. Problems were resolved collaboratively and relatively efficiently. The urgency of the 'live' Games did not allow for political arguments.

Finally, it is worth noting that the **sudden and great increase in Games-IS employees** also affected the organizational culture and the effectiveness of Games-ISS communications. During the second phase of project 'Operational Rehearsals', numerous new employees joined the organization in order to support IT operations at venues. Such employees often had little appreciation of the organizational culture, the operations of the centrally based project functions such as Games-ISS, and the centrally managed policies and procedures. This phenomenon increased the work coordination challenges both within Games-IS functions and in between functions[177]. The growing number of involved IT volunteers from TR-2 onwards, further increased challenges with regards to the creation of an organizational ISS culture, the delivery of operational IS(S) training and the implementation of account management controls.

[177] This was particularly demonstrated with the Games Network team and the Venue-IT teams, which lacked efficient mechanisms to deal with the quick expansion in workforce.

As indicated in the case of the Admin-ISS experts who joined the TOC-SEC team from TR-2 onwards, the transfer of tacit knowledge and experience was impossible within tight timeframes and with the operational complexity of the Games IS(S) solution. The identification of ISS risks and the resolution of related problems remained activities almost exclusively conducted by the more experienced Games-IS(S) team members.

Overall, the horizontal analysis of the Games-ISS contextual noise indicates that the event organization's activities, size, and operational complexity all affected the Games-ISS interactions and communications. Evolving political debates and dynamics affected the effectiveness of Games-ISS management controls, the patterns of work coordination and communication.

4.4.3. Emergent issues on the parameters and mechanisms of A2004 Games-ISS risk amplification

Throughout the preparation and 'live' stages of the A2004 Games-ISS project a number of ISS risks were identified, assessed and managed. This section aims to summarise all the ISS risks formally identified throughout the project's lifecycle (i.e. Table 4.18) and examine (a) how these progressed over time, and (b) the extent to which these were reliably managed during Games-time.

During the 'Initiation' of the Games-ISS project no ISS risks per se were identified. However, from past experience (i.e. SL2002) the Games-ISS expert made a number of Games-ISS project recommendations. Firstly, ISS was an issue that had to be dealt strategically and holistically. It was communicated that ISS attacks were common and these could compromise the reliability of the Games-IS operations. Therefore, Games-ISS objectives should be aligned to business requirements, while the initiation of such a project should not be delayed as this could lead to costly solutions or the compromise of overall Games security.

From the Games-ISS 'Analysis and Design' stage until the 'Closure' of the project a number of ISS risks were identified and formally communicated[178] within the Games-ISS team and across the Games-IS organization. The vast majority of these ISS risks were repeatedly identified across various stages of the Games-ISS project, and their

[178] *'Formally communicated'* refers to ISS risk communications made within and outside the Games-ISS team in formal decision-making meetings, ISS training sessions, ISS documents and ISS bulletins. 'Informal communications' would consist of daily, spontaneous discussions among Games-IS(S) members.

reliable management was often not achieved until Games-time. Achieving the desired levels of Games-ISS risk anticipation and containment required a series of repetitive and evolving efforts. These have been considered in more detail in section 4.3 of this study.

Table 4.18 below summarizes the ISS risks that were identified by the Games-IS(S) organization, and tracks when these were formally (i.e. X) and informally (i.e. x) acknowledged. Observations with regards to the patterns of ISS risks that were repeated, formally and informally communicated, and effectively and reliably managed are considered below.

One of the first Games-ISS risks to be identified in the A2004 environment which also persisted throughout the project's lifecycle was related to the lack of adequate and effective Olympic venue and TSA **physical security** controls(i.e. Table 4.18:4). This was an ISS risk that was consistently and formally identified and amplified by Games-ISS experts. The minimal improvement from one project stage to the next, and the fact that this was an issue outside the Games-ISS team's jurisdiction, led to its *amplification* in order to raise attention and motivate change. Yet, during 'Closure' the risk was not considered. It was not perceived as a lesson to be learned since it was outside the Games-IS(S) organization's jurisdiction. Hence, after Games the risk was *attenuated*. It is therefore evident that at different stages of the project the same risk was either amplified or attenuated. The reliable management of this ISS risk and associated controls was the responsibility of ATHOC, yet it affected (a) the logical Games-ISS controls chosen, (b) the cost of the Games-ISS solutions, and (c) the establishment of Games-ISS procedural controls (e.g. the Venue ISS audits). Thus, the dependency on another organization was acknowledged by the Games-ISS experts from early on. The risk was anticipated and alternative ISS controls were designed and implemented to contain it.

Table 4.18: *A2004 Games-ISS risks formally (X) and informally (x) identified and communicated throughout the A2004 Games-ISS project lifecycle*

	Identified ISS Risk	Analysis & Design	Implementation & Testing	Operational Rehearsals	Event	Closure
1	Lack of an **Admin and Games networks ISS strategy**.	X	-	-	-	-
2	Lack of a **holistic approach to managing ISS**. Games-ISS addressed as a purely technical issue.	X	-	-	-	-
3	Lack of adequate **Admin network ISS management** efforts & controls.	X	X	-	-	-
4	Lack of adequate and effective Olympic venue and TSA **physical security controls**.	X	X	X	X	-
5	Lack of a centralised, integrated, and resource-effective ISS monitoring solution - **SIM monitoring capability** required. Too many and unmanageable **ISS alerts**.	X	X	-	-	X
6	**Delayed involvement** of Games-ISS experts in Games-IS 'Analysis and Design', and 'Implementation' project phases.	X	-	-	-	X
7	Lack of adequate **Games network ISS management technical controls**. **Unauthorised activity** on the Games network. Internal communications not controlled and restricted.	X	X	X	X	-
8	Lack of a **Games network ISS architecture** identifying different levels of trust.	X	x	-	-	-
9	Inadequate appreciation of **Games-ISS roles and responsibilities** across the Games-IS organization. Not appreciated as a **common responsibility** with regards to both ISS risk anticipation and containment. Lack of audience-specific ISS operational policies and procedures.	X	X	x	x	X
10	Lack of **clear ISS technical requirements** covering concerns of critical asset and service redundancy and loose-coupling.	X	x	x	-	-

	Identified ISS Risk	Analysis & Design	Implementation & Testing	Operational Rehearsals	Event	Closure
11	Lack of adequate **ISS assurance controls**. Inadequate and ineffective means to measure and monitor the performance of ISS controls.	X	X	X	X	X
12	Lack of ISS **containment incident management controls** and processes.	X	X	-	-	-
13	Inadequate attention to the **secure configuration** of Games systems and network devices by various Games IS (Technical & Operational) functions.	-	X	X	X	X
14	**Unknown physical security** controls at venues, implicating ISS management decisions with regards to the appropriateness of logical ISS controls.	-	X	X	-	-
15	Lack of adequate **Third Party** secure connectivity and device build requirements.	-	X	X	-	-
16	Lack of strong **access and authorisation controls** for internal users on Games applications and systems.	-	X	x	X	X
17	Inadequate controls managing and monitoring **unauthorised devices** on the Games-network.	-	X	x	-	-
18	Inefficient allocation of **ISS incident management resources**.	-	X	x	x	X
19	**Inadequate means to assess** and understand the location, extent and impact of a detected **ISS vulnerability**. Poor containment controls.	-	X	x	-	-
20	Inadequacy and problematic implementation of **malicious software protection controls**.	-	X	x	x	-
21	Inadequate consideration of ISS threat posed by **IT volunteers**.	-	X	x	-	-

	Identified ISS Risk	Analysis & Design	Implementation & Testing	Operational Rehearsals	Event	Closure
22	Inadequate incorporation of ISS controls into Games-IS **Operations team** activities and procedures.	-	X	x	-	X
23	Inadequate incorporation of Games-ISS function into the Games-IS **change management procedure**.	-	X	x	x	X
24	Inadequate **customization of Games-ISS management and monitoring devices**, leading to too many ISS incidents and false-positive alerts.	-	X	x	-	-
25	Lack of a centralized Games-IS **configuration management process and tool/database** that would support accurate ISS risk decision-making and a means to standardise Games-IS configurations.	-	X	x	x	X
26	Inadequate knowledge with regards to the **ordinary communications** within the Games network.	-	X	x	x	X
27	Inconsistent **compliance to ISS policies and procedures**. Poor communication and enforcement of ISS policies and procedures.	-	-	X	X	X
28	Inadequate **ISS hardening** of Games systems and applications.	-	-	X	X	-
29	Inconsistent **compliance to Third Party** secure connectivity and device build requirements.	-	-	X	-	-
30	Insecure build and ISS management controls of **laptop** devices connecting legitimately onto the Games network.	-	-	X	X	-
31	Inadequate **device configuration checks**, resulting in many misconfiguration errors.	-	-	X	X	X

	Identified ISS Risk	Analysis & Design	Implementation & Testing	Operational Rehearsals	Event	Closure
32	Ineffective Games-ISS communication and incident management coordination practices with **Venue-IT workers**.	-	-	X	-	X
33	Problematic **performance of Games-ISS monitoring platform**.	-	-	X	-	-
34	Inadequate **alarms generated by illegitimately disconnected and misconfigured Games-IS devices**.	-	-	X	x	-
35	Poor **ISS incident management** collaboration and coordination within the **TOC-SEC team**.	-	-	X	X	X
36	Inadequate **duplication of Games-ISS expert skills** within TOC-SEC shifts.	-	-	X	X	X
37	Problematic **ISS incident profiling and resolution assignment** by non-ISS experts.	-	-	X	X	-
38	Problematic **performance of Games OVR systems** interacting with the Games-ISS anti-virus management controls.	-	-	X	x	-
39	Problematic compliance of Games-IS **IT partners** to Games *Secure Laptop* policy.	-	-	-	X	-
40	Problematic **coordination of ISS control implementation** activities with other Games-IS functions.	-	-	-	-	X

A further ISS risk that persisted across the project's stages was related to the lack of adequate **Games-network ISS management technical controls**. Throughout the project it was acknowledged that unauthorised activity (i.e. not business related and approved) took place on the Games-network (i.e. Table 4.18:7). This was in fact anticipated by the Games-ISS experts who designed and implemented Games network service segregation and traffic restriction controls. However, this risk was *attenuated* by the Games-IS Technical and Operations teams, that often translated such controls as proof of a distrusting, and overly-suspicious work environment. The implementation of related restrictions was often interpreted emotionally, leading to tensions between the Games-ISS experts and other Games-IS functions. The Games-ISS team, on the other hand, did not particularly amplify the risk as they did not wish to worsen tensions. Commitment from senior and executive project management was key in easing these tensions and indicated that such controls were necessary. After the Games and during the AAR meetings, this ISS risk was only indirectly acknowledged (i.e. Table 4.18:40). This indicates that risk amplification/ attenuation phenomena that were related to mechanisms of (dis)trust and the effectiveness of ISS communications throughout the project were hesitantly - if not at all - addressed.

Another persistent ISS risk was the inadequate appreciation of **Games-ISS roles and responsibilities** across the Games-IS organization. It was not appreciated that ISS was an organization-wide/common responsibility with regards to both ISS anticipation and containment (i.e. Table 4.18:9). It appears that the persistence of this risk was greatly related to the continually growing size of the Games-IS organization, as well as the degree of venuisation. Prior to the operational rehearsals of the project, this risk was greatly *attenuated* by the Games-IS Operations team and functions that had little interaction with the Games-ISS experts. In addition, the Technical teams, which acknowledged that ISS management was not the sole responsibility of the Games-ISS function, did not uniformly appreciate the criticality of this issue and addressed this as a secondary priority. Senior management commitment was required to stress the criticality of coordinating ISS management control efforts across Games-IS(S) teams. In addition, the tacit knowledge obtained through venuisation also improved risk appreciation levels.

The lack of adequate **ISS assurance controls** (i.e. Table 4.18:11) was another ISS risk that was repeatedly identified throughout the project's lifecycle. However, despite the fact that this risk was consistently acknowledged, it was greatly *attenuated*, not only by Games-ISS laypersons, but also by the majority of Games-ISS experts. This was particularly evident among experts of a strong technical background. Although ISS incidents of identified errors and omissions raised awareness of this ISS risk, the

high workload of the Games-IS(S) staff often left them with little time to do adequate checks. Also the findings of the *ISS Metrics Dashboard* were only communicated to senior project management, and even then this was not done consistently. The ISS metrics were not even communicated internally to the Games-ISS team. Neither were the detailed results of ISS policy compliance and Venue ISS audits. Priority was always given to further technical control customization, not assurance of their accuracy, relevance and uniformity. However, this ISS risk was greatly acknowledged after the completion of the Games, when it was observed that during Games-time the majority of ISS incidents were related to errors and omissions that could have been prevented if ISS assurance controls were more effective. This ISS risk was *amplified* after the Games, stressing that this is a common responsibility across the organization.

Related to the lack of effective ISS assurance controls, was the persistently inadequate attention to the **secure configuration** of Games systems and network devices by other Games-IS functions (i.e. Table 4.18:13). Attention to this risk was raised after the first Test Events, when the Games-ISS experts *amplified* related ISS incidents and requested a uniform security upgrade of all Games systems. However, the problem persisted. The continuous configuration changes caused by an evolving understanding of business needs and 'ordinary' Games-IS activity, led to a secondary prioritization of ISS by Games-IS teams. Thus, the risk was *attenuated* by Games-ISS laypersons. On the other hand, the Games-ISS team often assumed that Games-IS technologies were indeed securely configured/built. The 'Operational Rehearsals' indicated that this was not the case. ISS testers were recruited on the ISS team, yet the tests were not exhaustive. The lack of an automated means to check system security configuration resulted in inaccurate results, which were greatly dependant upon what the various Games-IS teams expected, not what they knew for certain. The risk was *amplified* again after the Games, since there were many misconfiguration ISS incidents - including within the Games-ISS team.

A further ISS risk that was repeatedly identified in the Games-ISS environment was the lack of **strong Games-IS access and authorisation controls** (i.e. Table 4.18:16).This was a risk that was consistently *attenuated* by the Games-ISS experts and laypersons. Although the risk was identified from the early stages of 'Testing' and 'Operational Rehearsals', the Games-ISS team delegated responsibility of its management to the IS Integration team and various Technical team functions. The Games-ISS experts did not conduct checks on this until the later stages of the 'Operational Rehearsals', when little time was left to fix the majority of related vulnerabilities. In addition, there was no overarching, centralised ISS policy on this

issue, but rather it was addressed individually per technical system group. The reasons for this risk attenuation can be perhaps traced back to the fact that the A2004 Games IS applications had been successfully used in previous major events. It was, therefore, assumed by the entire Games-IS organization that they were reliable. In reality this was not the case. Furthermore, the prioritisation of Games systems' availability had an impact on the extent to which confidentiality and integrity security controls were adequately considered.

The inefficient **allocation of ISS incident management resources** was an additional ISS risk that was repeatedly identified throughout the project (i.e. Table 4.18:8). The role of effective ISS incident management practices was considered significant for the Games-ISS experts and operations-focused Venue-IT and IT-Helpdesk teams. However, it was not addressed until venuisation and operational rehearsals commenced. In addition, the first Test Events *amplified* this risk and demonstrated that ISS incidents were often incorrectly identified and allocated to the wrong party for resolution. This problem improved throughout the 'Operational Rehearsals' phase, indicating that the risk's presence was greatly due to the inadequate levels of tacit, experience-based knowledge. However, the problem was not completely eliminated. As the organization grew in size and the new members did not receive any formal ISS incident management training until prior to TR-2, the risk persisted. Despite this and the worrying findings of venue ISS audits, which indicated that ISS training was a contributing factor to poor decentralised ISS incident management practices, the Games-ISS experts inadequately addressed this. They relied on experienced Games-IS members to mentor the new ones on the Games-ISS policies and procedures. The risk was *attenuated* as the event preparations workload increased and focus was put on ISS anticipation controls. The problem was once again formally acknowledged by the Games-ISS team after TR-2 and the Games. During these phases it was made particularly evident that Games-ISS laypersons as well as the majority of Games-ISS experts had so far focused their efforts on ISS anticipation controls, attenuating the significance of the existing ISS incident management policies and procedure. By the end of the Games, the Games-ISS team formally acknowledged that consistent and thorough ISS incident management procedures and communications with Venue-IT staff significantly reduced this risk.

Another ISS risk that persisted across project phases was related to the inadequate and problematic implementation of **malicious software protection controls** (i.e. Table 4.18:20). This risk was formally identified during Test Events, when it was made evident that the anti-virus solution (a) caused performance problems on the OVR systems, and (b) was inconsistently implemented on laptop devices connecting

onto the Games network. The risk was addressed quickly by the Games-ISS team by creating a dedicated anti-virus solution for the OVR systems that would not interrupt their operations, and by establishing a *Secure Laptop* policy. Yet, beyond establishing a set of ISS anticipation controls, the respective containment controls were not that effective. ISS assurance checks were limited or their findings inadequately communicated[179]. The need to consistently monitor this risk was *attenuated* by the Games-ISS experts. As an effect, ISS containment controls and checks were also neglected by ISS laypersons[180]. Despite the fact that this ISS risk was experienced during Games-time it was not addressed in the After-Action-Review (AAR) meetings. The lack of adequate attention by the Games-ISS experts was *attenuated*, thus avoiding the allocation of blame.

The inadequate incorporation of **ISS controls into the Games-IS Operations** team activities and procedures (i.e. Table 4.18:22) was a further ISS risk that was repeatedly acknowledged. This was an issue that was not addressed until venuisation. In addition, the first rounds of Test Events also demonstrated that procedural Games-ISS controls had been *attenuated* and inadequately considered by the Operations team. This risk was gradually addressed as communication and coordination activities improved between the Games-ISS experts and Operations team staff, and operational rehearsals demonstrated the nature of the problem. Therefore, the management of this risk was gradually addressed through a learning process of continuous feedback.

Closely related to the above ISS risk was the inadequate incorporation of the Games-ISS function into the Games-IS **change management procedure** (i.e. Table 4.18:23). Initially, the Operations team *attenuated* the impact of change management decisions on the activities of the Games-ISS function. As above, this was a risk that was also addressed gradually, where venuisation and operational rehearsals supported a process of learning and fine-tuning. However, even during Games-time it was made evident that the overall change management process was problematic, often having an impact on the Games-ISS team's functions. Thus, this risk was also formally acknowledged by the Games-ISS team after the end of the Games.

Another persistent procedural ISS risk which was related to the activities of the Games-IS Operations team, was the lack of a **centralised Games-IS configuration management process and tool** (i.e. Table 4.18:25). During the initial stages of

[179] E.g. ISS metrics, Venue ISS Audits.

[180] E.g. Venue ISS staff, IT partners and Third Parties.

'Testing' and 'Operational Rehearsals' it was made evident that Games systems and network devices were not securely configured and this had to be urgently addressed. The risk was then *amplified* by the Games-ISS experts via a Risk Assessment exercise, and was later delegated to the various Technical and Operations teams to address. Throughout 'Operational Rehearsals' it was made evident that configuration errors persisted and security controls were inconsistently implemented. Regardless, a centralised Games-IS configuration process and tool were not implemented. The risk was *attenuated* as it was expected that the trial-and-error process of 'Operational Rehearsals' and the existing ISS assurance controls would suffice to detect any problems. The ISS risk was once again formally identified after the Games, since several misconfiguration errors during Games-time raised awareness within the Games-ISS team. Allocating the blame on the lack of a centralised configuration management tool was also convenient for the Games-ISS team which did not want to accept that their ISS assurance controls had been ineffective. However, it is worth noting that where automated controls were present, compliance to ISS policies was indeed easier to check and problems were usually timely identified.

Closely related to the above ISS risk, are the inadequate **device configuration checks**, resulting in many misconfiguration errors (i.e. Table 4.18:31). Several of the Games device misconfiguration problems detected during the early stages of 'Testing' and 'Operational Rehearsals' were later *attenuated* by the Games-ISS experts because they expected that the Games Technical teams would have addressed these. It was assumed that since the Technical and Operations teams had been communicated what they should do, they simply would. The great workload of the Games-ISS team led them to delegate this responsibility, while not conducting adequate ISS assurance checks. With the completion of the Games, the ISS experts acknowledged the persisting risk, since during Games-time several ISS incidents were related to poor device configuration checks. Once again, this was an issue of poor ISS assurance procedures and controls. It appeared that, given the high project workload, such checks should have been automated as much as possible.

One more ISS risk that persisted throughout the project was the inadequate knowledge of **ordinary communications** within the Games network (i.e. Table 4.18:26). This was an ISS risk that affected the accuracy of ISS technical controls and generated great tensions between the Games-ISS experts and the Technical and Operations teams. It was a risk that was *amplified* by the ISS experts, blaming system owners of not knowing what communications their systems generated. On the other hand, the ISS laypersons - particularly the Technical team staff - consistently *attenuated* this risk, since the implemented ISS controls restricted their

communications and available services to what was strictly business-necessary. In addition, the ongoing changes in the Games-IS infrastructure meant that defining 'ordinary' Games network traffic was not an easy task. Great coordination was required, which clearly was missing since not all teams - especially the Operations and IS Integration teams - could not appreciate the ISS and network traffic implications of a configuration change. This risk was formally acknowledged by the Games-ISS team during the AAR meetings, since during Games-time a few ISS incidents were related to previously unknown 'ordinary' Games-network traffic. The fact that several of these incidents were caused by the departmentalised knowledge of 'ordinary' traffic within the Games-ISS team was not discussed and, therefore, *attenuated*.

The inconsistent **compliance to ISS policies and procedures** (i.e. Table 4.18:27) was another ISS risk repeatedly identified by the Games-ISS team. The ISS policy compliance and venue ISS audits identified that the reasons behind this was the inadequate training and communication of Games-IS functions and IT Partners with regards to the ISS policies. The problem was particularly intensified with increasingly decentralised operations and a growing organizational size. However, the findings of these audits were *attenuated* within the Games-ISS team that was primarily concerned with implementing and fine-tuning technical ISS controls. Compliance levels improved after the delivery of Games-ISS training, yet the problem was not completely removed. For example, the non-compliance of SWATCH to the *Secure Laptop* policy immediately prior to the Games, indicates that coordination, communications and ISS assurance checks had been ineffective. Although the SWATCH incident was not addressed after the Games - hence *attenuated* - it was nonetheless acknowledged that in the future greater and more frequent efforts should be made to effectively communicate and check compliance to ISS policies and procedures.

Finally, two more ISS risks that persisted throughout the project were related to the poor incident management **collaboration and coordination within the TOC-SEC team** (i.e. Table 4.18:35) and the inadequate **duplication of Games-ISS expert skills** within the TOC-SEC shifts (i.e. Table 4.18:36). During 'Operational Rehearsals', particularly from TR-1 onwards, it was made evident that the TOC-SEC team encountered problems with regards to collaborating and coordinating efforts in relation to ISS incident resolution. This was partly due to their inadequate knowledge of the related procedures, as well as due to the problematic duplication of Games-ISS expert skills within the TOC-SEC shift. Problems were intensified as additional Admin-ISS team members joined the team. Team-internal training sessions and TR-

practice helped to identify any problems and provide future recommendations. Yet, by the time that these problems were identified[181] there was little that could change in the operating model of the TOC-SEC team. Acknowledging that, members of the TOC-SEC team - particularly the Games-ISS Manager who had defined the structure and composition of the various TOC-SEC shifts - *attenuated* the associated ISS risks. This resulted in a number of problems during Games-time, which created tensions within the team. However, even after the Games, this issue was only briefly discussed and once again *attenuated*, thus avoiding the allocation of blame on the Games-ISS team or any of its members.

Having considered the ISS risks that persisted across the Games-IS(S) project, it is also worth making a few more observations. Firstly, the vast majority of persistent ISS risks were related to procedural controls of ISS management. Even ISS risks that had a stronger technical or ISS culture element to them also had a significant procedural element, which was often attenuated and neglected.

In fact, several of the ISS risks that were procedural in nature required time and practical experience to be effectively managed; a learning process was required[182]. In addition, the majority of persisting risks could have been resolved or better contained if more effective ISS assurance controls were in place.

Another observation made is related to the nature of ISS risks identified across different project phases. Therefore, the first round of Testing/Operational Rehearsals (i.e. TE-1) stressed the inadequacy of technical ISS controls. As more TEs/TRs took place a number of procedural issues were also made evident. Further on, as the organization grew quickly in size and there were increasing organizational work and communication/coordination problems, it was also identified that several ISS culture and communication problems were present[183].

In addition, apart from the persistent ISS risks identified above, a few more risks were also amplified/attenuated. For example, the poor **ISS design of the Games applications** was inadequately and too late addressed. This risk remained hidden

[181] I.e. a couple of months prior to the Games.

[182] E.g. the problematic ISS incident management practices.

[183] E.g. coordinating work and communicating ISS messages to growing Network and Operations/Venue-IT teams

until the later stages of the project, while it was not addressed at the end of the Games, despite the Games-time performance problems.

Furthermore, the fact that **ISS training** was not effective during the 'Operational Rehearsals' period[184], was not adequately acknowledged either. Yet, this risk caused various problems and was related to various other ISS risks[185].

The late detection of the **SWATCH** devices that were not compliant to the **Games-ISS *Secure Laptop* policy** (i.e. Table 4.18:39) was another problem that remained hidden and was not addressed during the AAR meetings. This was an incident indicating that the communication and coordination with SWATCH had been inadequate, while lacking effective and timely ISS assurance controls.

Another ISS risk that experienced contradicting amplification and attenuation forces was related to A2004 **IT-volunteers**. After the initial detection of this risk during TE-1 and the departure of the first Games-ISS Risk Manager, this was never again considered. Although the TE-1 incident led to the *amplification* of the risk by the Games-ISS Risk Manager, this was greatly *attenuated* by ATHOC and senior Games-IS project management. This was an ideological hidden risk, where the Games-IS and ATHOC organizations did not wish to question the motivation of A2004 IT-volunteers. IT-volunteers were a rare commodity, while the Olympic project was greatly dependant on them. As such, no further formal ISS checks and controls were established to anticipate and contain such risks. The fact that no additional IT-volunteer related ISS incidents were detected during Games-time further attenuated this risk.

Boredom and routinization was another ISS risk that was acknowledged, yet not addressed by any of the Games-IS teams. This problem was considered to be unavoidable and it was therefore *attenuated*, despite the fact that it led to several important errors and omissions.

Finally, it is worth noting that upon project 'Closure' the Games-ISS team greatly *attenuated* the fact that the **SIM solution** was greatly not used during Games-time due to the team's technology unfamiliarity. Instead, during the AAR meetings, the implementation and use of the SIM were recorded as a success story.

---

[184] I.e. almost a year went by for ISS trainings to be repeated.

[185] E.g. inconsistent compliance to ISS policies by Venue-IT teams.

4.4.4. Emergent issues on the A2004 Games-ISS project organizational reliability and operational preparedness levels

Within a project environment where there was no "*space for errors*", the objective of the Games-IS Integration and Games-ISS projects was to provide highly reliable operations during Games-time. The process of change from project 'Initiation' to project 'Event-time' was one that aimed to ensure that during Games-time unexpected incidents could be both anticipated and contained, thus not compromising the availability of the Games-IS infrastructure.

As such, apart from closely observing the daily activities and interactions of the Games-IS(S) organization, the researcher also questioned representatives of various Games-IS project functions with regards to their assessments of the organizational and operational levels of Games-ISS reliability (i.e. Appendix-A10). The questionnaire was perhaps not exhaustive but aimed to investigate over time how perceptions of ISS reliability changed across the Game-IS organization. The longitudinal findings of these questionnaires, which were often further discussed with the respondents, are summarised below.

Firstly, with regards to the levels of **reliable ISS organizational design**, these improved over the project's lifecycle from non-existent to relative maturity and reliability. The only two periods when reliability levels appeared to decrease were after the first Test Events[186], and with the completion of the Games. Questioning the respondents of such assessments indicates that major operational rehearsals and/or the A2004 Games signalled to various persons and functions that the reliability of several ISS organizational design controls had been overestimated. Examples where this happened are related to the extent to which various functions clearly understood the Games-IS technological interactions, ISS needs and implemented controls, and the extent to which they understood the various single points of failure and IT infrastructure component redundancy requirements.

Controls of **reliable ISS operational management** were the ones that demonstrated the steadiest of improvements over the project's lifecycle. Great rates of improvement were demonstrated during the earlier stages of the project, when little operational activity was evident. However, as 'Operational Rehearsals' took place, the reliability growth rate was more stable since constant changes and fine-tuning activities took place. As for the A2004 Games event, it demonstrated to the questionnaire respondents that several necessary ISS policy and procedure

[186] i.e. August 2003.

communications had not been made, while operational personnel and skills were not always adequately duplicated.

The controls of **reliable ISS organizational culture** were the ones that demonstrated the greatest levels of fluctuation throughout the project. Prior to the first Test Event, when Games-ISS control implementation activities were initiated, assessments of a reliable ISS organizational culture dropped. This perhaps indicates that the project shift from 'Analysis and Design' to 'Implementation and Testing' created tensions between Games-IS functions that were reflected in the questionnaire responses. Increased levels of work and requirements of greater coordination indicated that not all Games-IS functions had the same ISS priorities. This low in levels of reliable ISS organizational culture changed immediately prior to the first Test Events, as venuisation demanded that teams collaborate more closely and better appreciate the tasks and responsibilities of each Games-IS function.

The levels of reliable ISS organizational culture did not decrease again until the period of intense venuisation activities, when preparations were made for the first round of Technical Rehearsals. The project drive to implement all Games-ISS technical controls prior to Technical Rehearsals generated, once again, tensions between the Games-ISS experts and the other Games-IS functions. These were particularly evident with regards to interactions with the Technical teams that were responsible of correctly and timely implementing several of the Games-ISS controls.

With regards to controls of **reliable ISS anticipation**, these overall improved throughout the Games-IS(S) project preparation phases. The only project period when ISS anticipation controls appeared to deteriorate were after the completion of the first Test Event, when all Games-IS functions - apart from the Games-ISS experts - suggested that they had previously overestimated these. The first Test Events signalled that more collaborative work had to be conducted in order to implement reliable ISS anticipation controls.

Finally, with regards to controls of **reliable ISS containment**, although these improved over time, they also fluctuated across the project's lifecycle. Therefore, with the transition from 'Analysis and Design' to 'Implementation and Testing' ISS containment controls demonstrated a drop in levels of reliability. This indicated that as the need for containment controls was appreciated, it was also acknowledged that their current level was relatively poor. Immediately prior to the first Test Events, however, as ISS containment efforts increased, they demonstrated their greatest growth rate. Beyond that, the reliability of ISS containment controls fluctuated,

reflecting the organization's overall capacity to effectively contain ISS problems and incidents and learn from past mistakes. Perhaps surprisingly, the organization's capacity to contain ISS problems was slightly reduced prior and during Games-time, when it was observed that several older problems were repeated and ineffectively contained and corrected.

Overall, it is observed that ISS reliability assessments were not only based on the actual maturity of ISS controls, but also on the contextual noise of the project. At periods of intense negotiations between groups, ISS reliability levels appeared to deteriorate. Fluctuations in the levels of ISS reliability were also observed around major project milestones. Thus, as the Games-IS(S) projects moved from 'Analysis and Design' to 'Implementation and Testing', working patterns and priorities changed, and so did assessments of Games-ISS reliability. Similarly, prior to the Technical Rehearsals, negotiations increased and tensions were reflected in reliable ISS organizational culture assessments. Finally, prior and during Games-time, the criticality of the project stage and the 'no space for errors' mentality meant that the reliability of various ISS controls was reassessed.

One last comment with regards to the findings of the reliable ISS questionnaires should be made with regards to discrepancies and similarities between the Games-ISS experts and the rest of the Games-IS functions. Throughout the project lifecycle it is evident that the Games-ISS experts overall shared similar views, while the greatest and most consistent difference in ISS reliability assessments was between the Games-ISS team and the Operations and IT Helpdesk teams. The greatest similarities were observed between the Games-ISS team and the Technical team, despite the various intense debates that occasionally took place among them. This perhaps indicates that the teams that had a similar professional/technical background often shared similar views.

4.5 Conclusion

The above chapter has presented the empirical findings of this study which have been interpreted by utilising the contextualist research method presented earlier in section 3.3.3. The research findings have been analysed in detail across the A2004 Games-ISS project phases, while emergent issues have been also identified. These are related to the ways that the project and organization scope, structure, contextual surrounding and nature of ISS risks have determined the change processes of ISS risk communication and amplification, and the eventual levels of A2004 Games-ISS operational and organizational reliability (i.e. section 3.3.1).

The next chapter of this study will consider the ways in which the major-event organization under review 'encountered' ISS risks, and will overall assess the organization's capacity to reliably manage ISS risks. Any insights that can be potentially applied to other similar organizations or the processes of ISS risk amplification and reliability management will be also considered.

5. Discussion - Encountering Risk

5.1 Introduction: organizational encounters with risk

As suggested in Chapters 1 and 2 of this study, information systems security (ISS) is a topic that has entered the strategic agendas of organizations, yet can be very costly. Hence, there has been an increased appreciation and utilization of risk management practices with regards to ISS[187].

Risk management is a *process* of attention, sense-making and re-organization, where behaviours and formal management controls change. This process of organizational and behavioural change is labelled by Hutter and Power (2005b) as 'organizational encounters with risk'. As argued earlier in this study, the process of risk management or the 'organizational encounters with risk' is a process that is inherently subjective and interpretive, which will be determined by - and will also determine - the context within which it is applied.

Meanwhile, extensive literature has indicated that certain organizational structures - and their corresponding IS - do not only face heightened operational reliability requirements, but are also more prone to errors, accidents and disasters[188].

As presented in Chapters 2, 3 and 4 of this study, the organizational environment and IS of a major event organization is often one of high reliability requirements. In addition, the scale and complexity of such mega organizations and their IT infrastructure endeavours, as well as the great levels of interdependency among project deliverables implies that mega project/event organizations are also prone to error and disaster.

Therefore, as also defined in Chapters 1 and 3, the aim of this research was to investigate closely the ISS risk management efforts of a major event organization and interpret the organization's capacity to reliably manage ISS risk. Adopting a contextualist and longitudinal case-study analysis approach, the researcher presented in Chapter 4 the activities, risks/risk events and context of a major event ISS project, namely that of the Athens 2004 (A2004) Summer Olympic Games. The ISS risks detected and managed during the mega-project's lifecycle were identified (i.e.

[187] I.e. Dhillon, 2007.

[188] I.e. Perrow, 1984, 1992; Sagan, 1993.

Table 4.18) along with the perceptions of key project participants in relation to ISS control reliability. As discussed above (i.e. section 4.4), these findings indicate that both perceptions of ISS risk and reliability levels are subjectively determined by a number of factors such as: (a) the evolving organizational structure and work coordination and communication patterns; (b) the organizational context and culture, including the political negotiations, motivations and expectations between and within groups and opinion leaders; (c) the nature of the identified ISS risks and controls; and (d) the operational phase of the organization which determines whether ISS management controls and risks/risk events are perceived as 'routine' or 'emergency' ones.

As argued by Walsham (1993) and supported in Chapter 3 of this study, a process of change - such as the organizational encounters with (ISS) risk - can be conceptualised with a number of metaphors. The conceptual framework utilised for the purposes of this research is the SARF which links context and process via the metaphor of amplification/attenuation. This is a metaphor that according to its proponents appreciates the dynamic organizational interactions/communications both at a social and individual level, and across the various contextual levels of risk perception (i.e. Fig.3.4)[189].

The process of amplification is a dynamic one of feedback and iteration (i.e. Fig.3.5), and its proponents suggest that its investigation and understanding can lead to the improvement of appraisal, evaluation, management and communication of risk. Extending this argument, the researcher aims to also consider the ways in which understanding of the amplification process and organizational encounters with risk can improve ISS reliability levels of inherently risky mega-event/project organizations.

Therefore, Chapter 5 considers the processes of A2004 Games-ISS risk attention, sense-making and re-organization, and compares perceptions of ISS reliability levels to actual events and research observations. The aim is to understand the parameters and mechanisms of A2004 Games-ISS risk amplification and consider if any problems could have been predicted to further increase levels of operational and organizational reliability. Lessons to be learned for other similar organizations, the organizational encounters with risk and the mechanisms of organizational high reliability will be also considered.

[189] According to Renn and Rohrmann (2000) the various contextual levels of risk perception include the cultural, political, cognitive-affective, and heuristic levels.

5.2 ISS risk attention in a major event context

According to Hutter and Power (2005b:11) 'risk attention' involves the process and mechanisms of risk identification, recognition and definition. It is not a merely cognitive issue at the level of the individual, but is also "socially organized by a wide variety of institutions which support prediction and related forms of intervention around the possibility of future events".

The mechanisms and institutions of risk attention will not only determine what is communicated and the sustainability of one's attention; they will also determine the accuracy, completeness and accessibility of the communicated information.

Hutter and Power (2005b) agree with Freudenburg (2003:115) who suggests that "certain things always need to be forgotten for any cognitive system to work: there is no way of paying full attention to everything". They thus suggest, similar to the SARF proponents, that risk events/incidents tend to have substantial institutional consequences and are effective mechanisms of risk attention. Whether the identified risks/risk events will be normalised[190] or amplified depends on a number of factors relating to the process of sense-making (i.e. section 5.3).

The conceptualisation of 'organizational encounters with risk' suggests that organizational structures, communication channels and technologies determine the process of risk attention. From a reliability management point of view they also determine the extent to which attention is given to the unexpected and appropriately escalated and communicated.

The above conceptualisation of risk attention overlaps with that of the SARF and the first stage of amplification, namely that of information communication which covers factors such as the sources of risk information and the channels of information (i.e. Fig.3.5).

5.2.1. A2004 Games-ISS sources of risk information

Following the researcher's analysis of the ISS risks that were identified during the A2004 Games-IS(S) project (i.e. section 4.4 and Table 4.18), a number of observations can be made with regards to the sources of risk information.

[190] The '*normalization of deviance*' (i.e. Vaughan, 2005) is considered in section 2.3.4 of this study.

Firstly, the sources of risk information varied across different project phases. Therefore, during the 'Analysis and Design' stage of the project ISS risks were identified by the Games-ISS experts utilizing their knowledge of ISS *best practices* and *previous Olympic ISS experience* (i.e. SL2002). The majority of risks identified during this stage were usually of a strategic nature and were greatly related to the ISS interaction, roles and responsibilities of ATHOC and the IT TOP Sponsor. This reflects the contextual noise during the particular project phase, when ISS project negotiations were primarily of a strategic focus and with senior/corporate management across ATHOC and SchlumbergerSema.

As the project progressed into 'Implementation and Testing' the preparation activities of venuisation required the Games-ISS experts to collaborate more with other Games-IS functions, particularly the Technical teams. Once again, the majority of ISS risks were identified by the Games-ISS experts and the utilization of the Games-ISS Baseline. Risk communications were directed to a less extent towards senior management, but primarily towards Games-IS function management. Risk communications were primarily conducted via *informal social/work networks*.

With venuisation and the initiation of Test Events the sources of risk information changed once again. The Games-ISS experts remained the main source of risk information, yet they now utilised *ISS management and monitoring technologies* to detect Games-ISS risks. Therefore, the project phase determined the tools/methods used to detect ISS risks and collect related information.

In addition, the fact that ISS management and monitoring technologies were used to detect ISS risks implied that during the early stages of 'Operational Rehearsals'[191] the majority of identified risks were primarily of a technical nature. In parallel, the utilization of a semi-automated IS(S) *incident management system* also determined how ISS risks were identified, classified and communicated. In fact, the presence of such an incident management system assisted with sustaining attention to ISS risks, and ensuring thorough cross-functional investigation of these.

With the growing scale of the organization and its operations, the Games-ISS experts increasingly utilised *indirect methods* to communicate ISS risks. Informal social networks of communication were utilised only with those groups that Games-ISS experts directly interacted with. For the rest, ISS risk messages were communicated to function managers, who were responsible of informing their team members accordingly. However, as considered in Chapter 4, this was not always an efficient

[191] Or the 'Testing' phase of 'Implementation & Testing' (i.e. August 2003 - January 2004).

mechanism of risk communication. This was demonstrated via persisting ISS problems - especially procedural ones, and the findings of ISS audits.

In fact, with increasing levels of organizational maturity and stability, a further source of ISS risk information was that of *ISS assurance controls*[192]. Such controls did not only detect purely technical ISS risks, but also procedural and cultural/communication ones. In addition, ISS audits and training operated as mechanisms of ISS layperson awareness, encouraging them to improve the detection and reporting of ISS problems to the Games-ISS experts. Hence, the *personal ISS experience* of laypersons was *directly communicated* to the Games-ISS, improving the reliability levels of ISS anticipation and containment controls.

Thus, as 'Operational Rehearsals' progressed, an ongoing ISS risk learning process was facilitated, which was primarily supported by the *personal experience* of Games-ISS experts, and later laypersons. Operational complexity was increasingly experienced and appreciated, leading to conscious efforts to coordinate ISS risk identification and definition activities. Hence, during the later stages of 'Operational Rehearsals' Games-ISS laypersons were also involved in the detection of ISS risks. As ISS roles and responsibilities were increasingly understood across the A2004 Games-IS organization, it was observed that Technical experts, Operations team staff and Venue-IS staff played a significant role in detecting (and managing) ISS risks. In particular, Venue-IS staff had a key role in identifying procedural ISS risks across the increasingly decentralised organizational structure.

A further observation made with regards to the mechanisms of ISS risk attention is that during project phases that represented major milestones[193], the sources of risk information became more varied and accordingly the identified risks were greater in number. This potentially indicates that 'emergency' operations raised levels of ISS vigilance, coordination and communication.

Finally, it is worth noting that of all Games-ISS risks identified throughout the project's lifecycle (i.e. Table 4.18) the vast majority of these were identified during the 'Testing' and 'Operational Rehearsals' phases. It is, thus, demonstrated that the trial-and-error process of Test-Events and Technical-Rehearsals was the most

[192] Games-ISS policy compliance audits, venue-ISS audits, the regular collection of ISS metrics, and the completion of ISS vulnerability tests, all operated as additional sources of risk information.

[193] I.e. prior to the first Test Events (TE-1: August 2003); with the completion of TE-2 and the 'Implementation and Testing' phase (January 2004); prior to the Technical Rehearsals (TR-1: April 2004 and TR-2: June 2004); and finally prior to the Games (July-August 2004).

effective mechanism of identifying ISS risks, facilitating ISS risk attention through personal experience.

5.2.2. A2004 Games-ISS risk information communication channels

Similar to the sources of risk information, the related communication channels also varied across different project phases. During the initial stages of project 'Initiation' and 'Analysis and Design' the communication channels were primarily *formal and documented*, with a central role played by the SchlumbergerSema ISS expert[194]. The involvement of a *professional information broker* was key in raising senior management ISS awareness and defining the strategic objectives of the A2004 Games-ISS project.

As the project progressed, the interaction of the Games-ISS expert/professional information broker and the various Games-IS functional managers increased via the utilization of *informal communication channels*. Mutual adjustment mechanisms were used to share ISS risk information and establish ISS roles and responsibilities. However, as the organization grew in size and operational complexity, formal communication channels were increasingly utilised in order to establish standardised ISS practices and structures of accountability. Therefore, ISS risks were increasingly communicated via documented and formally approved ISS policies and procedures, while decision-making meetings were increasingly formalised. The Games-ISS experts continued to play a critical role in the process of ISS risk communications, with the Games-ISS Risk Manager[195] clearly adopting the role of an *opinion leader*.

With the initiation of Test Events individual senses were increasingly used to detect and classify ISS risks. As organizational levels of ISS awareness and culture matured, increasing members of the Games-IS organization used their personal experience to detect, and make sense of ISS risks. During operational project phases, the semi-automated *IS incident management system* represented the most significant method

[194] The SchlumbergerSema ISS expert later adopted the role of the Games-ISS Risk Manager.

[195] The first manager of the Games-ISS team (he resigned in December 2003, following the Atos Origin acquisition of the Major Events division of SchlumbergerSema) was highly respected and trusted for his ISS expertise and management skills. Trust in his competence was demonstrated by Schlumberger senior/corporate management, his team members and colleagues. Similarly, members of other interacting organizations (e.g. ATHOC, SWATCH, 3rd Parties) also demonstrated to trust the Games-ISS expert. He was, thus, an *opinion leader* that played a key role in the ISS risk amplification processes.

of ISS risk communication, while the degree of physical proximity to the Games-ISS experts also determined the means of ISS risk communication. Therefore, if ISS laypersons were located in the Technology Operating Centre (TOC) alongside the TOC-SEC team, communication was often implemented via *informal social networks*. On the other hand, ISS issues detected across the decentralised venues were *formally communicated* via the IS incident management system.

In addition, social affiliation between members of the Games-ISS team and the various Games-IS functions and Venue-IS teams also determined the channels of ISS risk communication. Thus, Technical teams that collaborated closely with the Games-ISS experts often utilised *informal social networks* of communication. Similarly, informal communication networks were utilised more frequently by staff that were longer with the organization.

It is also interesting to note that different communication channels were used for different risk information audiences. Therefore, inter-organizational ISS risk communications were more formal to those internal to the Games-IS organization. This was clearly demonstrated with Third Parties and ATHOC, where any detected ISS risks were communicated to them via formal meetings, memos, documents and policies. The same risks were communicated via more informal social networks internally to the Games-IS organization.

Another factor that determined the ISS risk communication channel was that of the contextual noise. It was observed that at periods of tension - either due to risk ambiguity or time-pressure - opinion leaders and senior management had to engage in the risk debates in order to resolve any problems and conclude any negotiations. Thus, the greater the intra- or inter-organizational tensions and risk ambiguity, the greater the need for escalation and the use of formal ISS risk communication channels.

Furthermore, the type of ISS risk also determined the utilised communication channel. Hence, technical ISS risks were primarily reported via the IS incident management system, as well as informal social networks. On the other hand, procedural risks were often identified via individual senses and ISS assurance checks, and required formal communication channels in order to effectively communicate these. It was proven that indirect communication[196] was an ineffective mechanism.

[196] 'Indirect communication' refers to cases where the communication of an ISS risk (and associated controls) was delegated to another party/communication channel. E.g. ISS risks that were communicated to Games-IS staff by their function managers and not directly by the Games-ISS experts.

Instead, direct communication via ISS training and audits proved to be particularly effective and had a considerably positive impact with regards to raising reliability levels of ISS operational management and organizational culture controls. In addition, in cases where the risk was 'uncertain'[197] formal communication channels were utilised first, while where an ISS risk was 'ambiguous' informal communication was used first, seeking the views of peers.

Finally, risk communication channels were determined by the extent of 'routine' or 'emergency' operations. During routine project phases communications were often made via *informal social networks*, thus supporting a continuous process of mutual adjustment. Similarly, *indirect communications* were utilised during routine project phases. During 'emergency' phases, however, the same risks were often allocated a higher severity and were communicated via multiple communication channels - both formal and informal. The utilization of multiple risk communication channels increased levels of ISS reliability.

5.2.3. Reflections on the SARF mechanisms of 'risk communication'

In the current study, the SARF has been utilised to link the context and process of organizational change with regards to ISS risk management[198]. However, this study has also highlighted a number of issues with regards to the very mechanisms of risk communication suggested by this conceptual framework.

Firstly, as has been repeatedly suggested in this study, the research findings verify that organizational structures, communication channels and technologies determine the process of risk attention (Hutter and Power, 2005b). Yet, although the SARF highlights that communication channels are key with regards to the filtering and communication of risk information and signals, it does not explicitly consider how *organizational structures* and available *technologies* affect the process of risk communication.

In the current study, Mintzberg's (1979, 1981) scheme of organizational context[199] had to be incorporated into the SARF analysis in order to define these factors and how these affect the 'contextual noise' of the SARF risk communication process.

[197] I.e. Appendix-A2, IRGC (2005) and Klinke and Renn (2006).

[198] I.e. section 3.3.2.1.

[199] I.e. section 3.2.2 and Table 3.1.

Thus, the researcher suggests that future utilization of the SARF could benefit from the incorporation of conceptual frameworks that highlight the structure, situational factors and technologies of organizations.

Also, the findings of the current research indicate that in addition to the 'signal value' of a risk[200], classifying the *type of a risk* can provide clarity with regards to its nature, and subsequently guidance with regards to its communication. Therefore, as suggested by Renn (2008) and the IRGC (2005) risk governance framework[201], simple, complex, uncertain and ambiguous risks may not differ in terms of their risk information source, yet will often require different methods of communication. This underlines further the importance of the risk communication channel - both medium and method. As argued by Hutter and Power (2005b), the sense-making of risks initiates with the processes of risk attention and communication.

Thus, the researcher also suggests that further studies are conducted into the ways in which the characteristics/type of a risk will interact with the channel of risk communication, and how this will subsequently affect the process of risk interpretation and potential amplification.

With regards to the above observations and elements of interest relating to the utilization of the SARF, the findings of this study indicate the following:

Firstly, it has been demonstrated that the more *complex* and *uncertain* a risk is, the more a repetitive process of (ISS) risk learning is required in order to gradually improve levels of risk information completeness and accuracy.

To that direction, repetitive processes of trial-and-error[202] can - over time - improve the effectiveness of risk attention and communication. Although research findings indicate that trial-and-error practices will in the short-run increase levels of risk *ambiguity*[203], they also have the ability to reduce levels of complexity and uncertainty. The mechanism to achieve this appears to involve an inevitable element of risk amplification or attenuation. In addition, it appears that a few of the factors necessary to improve processes of risk attention are related to (a) the organization's

[200] I.e. As this is defined by Slovic et al (1980), section 3.3.2.1 and Fig.3.6.

[201] I.e. Appendix-A2.

[202] Such as the operational rehearsals in the A2004 Olympic Games.

[203] Risk ambiguity is not only related to the nature and impact of the (ISS) risk. It is also related to the cost/resource and power restructuring implications that its management may have. This explains why 'simple' risks can also be 'ambiguous' risks (i.e. Renn, 2008).

'ability' and 'motivation'[204] to pay attention to new or reoccurring signals of failure and risk; and (b) the involvement of opinion leaders and accountable authority figures in the negotiations that will direct risk decisions.

Therefore, this research has indicated that certain *types* of (ISS) risk will require an iterative and monitored process of risk information filtering and communication prior to resolving problems of risk complexity and uncertainty, and adequately justifying ambiguous risk interpretations and organizational responses. The iterative and reflexive character of any trial-and-error learning process is a key success factor to the process of risk attention and communication as certain risk signals - especially near-misses - will have the tendency to be normalized or attenuated.

In addition, this study had indicated that personal experience - potentially via controlled processes of trial-and-error - and direct risk communication are more effective means to raise risk attention than indirect communications[205]. This is particularly relevant for complex and ambiguous risks.

The current research has also highlighted the importance of technologies in raising attention to risks. Particularly in organizations of great scale and operational complexity, technologies that can centrally monitor risks and risk signals[206] can greatly contribute towards addressing risk complexity and uncertainty, thus avoiding phenomena of risk amplification or attenuation. However, this study has also underlined that organizational risk expectations are frequently built into technologies[207]. In agreement with a number of scholars[208], the researcher suggests that the configuration of risk management and monitoring technologies needs to be frequently reviewed and questioned if an organization is to remain sensitive to

---

[204] I.e. Chaiken and Stangor (1987) and section 3.3.2.1.

[205] I.e. section 4.4.3: Examples include ISS risks of poor physical security, poor implementation of ACL controls, and poor compliance with ISS policies at competition venues. All these ISS risks were greatly mitigated after direct communications between the ISS-experts and laypersons took place.

[206] E.g. the A2004 Games-IS(S) SIM solution, centrally managed and/or monitored change management, configuration management and incident management solutions.

[207] A number of related cases are presented in sections 4.3 and 4.4. E.g. in the A2004 Games the centrally monitored change-management system did not initially incorporate the ISS function as this was not viewed as necessary by the Games-IS Operations team. Also, the Games-ISS SIM solution did not raise alerts for incidents of legitimate traffic beyond the acceptable traffic-load threshold, and did not raise alerts for devices that were illegitimately unplugged.

[208] I.e. Weick and Sutcliffe (2007) and Vaughan (2005).

operations and avoid risk-signal simplification and normalisation. Therefore, similar to human cognitive mechanisms of risk attention and classification, organizational technologies require an iterative, reflexive process of customization and fine-tuning.

A further point relating to the SARF process of risk communication relates to the number of available risk communication sources and channels within a particular organizational context. The findings of the current research indicate that an increase in risk information sources does not necessarily lead to the avoidance of risk amplification phenomena; quite the opposite. As risk information sources and communication channels increase in number and type, they initially lead to greater ambiguity; partly because different actors interpret and frame the risk information in different ways according to their interests, motivations and occupational/skills background. Therefore, the legitimacy and trustworthiness of a risk information source and communication channel are issues of concern in the process of risk communication and amplification.

In addition, it was observed that under conditions of routine operations the more complex the nature of an (ISS) risk, the greater the ambiguity that was generated by the increasing numbers of risk information sources and communication channels. Under emergency conditions, however, more risk communication channels were considered necessary and utilised - in line with high reliability management practices.

Finally, this research has indicated that different communication channels were used for different risk information audiences. Where physical proximity, social and occupational affiliation was great, informal communication channels were utilised. Formal communication channels appeared to be more appropriate for inter-organizational risk communications and communications related to escalated and ambiguous ISS risks. Also procedural and cultural ISS risks appeared to be more ambiguous - and in fact attenuated - and required formal risk communication channels that allowed for elaboration and feedback[209].

[209] E.g. interactive ISS training and ISS audits; formal and informal meetings.

5.2.4. Reflections for other organizations and reliable mechanisms of ISS risk attention

Consideration of the A2004 Games-ISS risk attention mechanisms points to a number of insights, not only for the specific organization, but also for other organizations of similar characteristics. In addition, some conclusions can be drawn with regards to the reliable mechanisms of ISS risk attention.

Firstly, the analysis of the research findings indicates that an organization's structure and ways of working[210], its culture and political negotiations, the nature and type of ISS risks[211], and finally the circumstances under which risk are identified[212], are all factors that affect the mechanisms and efficiency of risk attention.

Secondly, the research findings demonstrate that the rate and scale of organizational change also affects the reliability levels of risk attention processes (i.e. section 4.4). The exponential growth in organizational scale and operational complexity of a major event organization poses considerable challenges to the mechanisms of risk attention. Therefore, the data analysis of this study indicates that ISS risk information sources and communication channels must remain flexible and prepared to adjust to organizational changes. Direct ISS risk communications should be utilised wherever possible, while where indirect communications are used, these should be regularly monitored for effectiveness. In addition, regular audience-specific ISS training and audit activities can greatly increase effectiveness and reliability of ISS risk identification sources and communication channels. Moreover, ISS assurance checks can be particularly valuable for the identification of ISS risks, especially procedural ones that are otherwise often ignored. Lastly, the researcher suggests that centralised processes of ISS monitoring, incident management, configuration management, and change management can operate as effective ways to detect ISS risks and non-compliance, while also creating structures of accountability. Hence organizations that share the characteristics of major-event structures can benefit from investing in such solutions.

Furthermore, the findings of this research have demonstrated that within an organization of great interactive complexity, the practical experience and tacit knowledge gained through trial-and-error and operational simulation activities can

[210] As defined by Mintzberg (1979, 1981) and summarised in Table 3.1.

[211] As defined by Klinke and Renn (2006), IRGC (2005) and summarised Appendix-A2.

[212] The circumstance under which a risk is identified and made sense of refer to conditions of time pressure, or not; and great visibility/exposure, or not (i.e. Finucane et al, 2000).

considerably improve the reliability of risk identification and classification processes. Therefore, in the case of the A2004 Games the repetitive Test Events and Technical Rehearsals were the most effective mechanisms of identifying (ISS) risks, appreciating complexities, uncertainties and resolving ambiguities. Through this process of continuous learning and attention to operations organizational and operational reliability improved considerably.

An additional factor that greatly supported the mechanisms of ISS risk detection, reporting and classification was that of the various IS(S) incident management and monitoring technologies. However, such controls appear unable to reach their full potential until these are adequately customized[213]. In a complex and uncertain environment such customization can be only achieved through experience and practice. This stresses further the need for operational testing. The optimization of IT solutions that support the detection and communication of ISS risks is a learning process that requires considerable time and resources. Mechanisms to capture and transfer such experience[214] can greatly assist towards achieving greater returns on investment and increasing levels of operational reliability.

A further observation made with regards to mechanisms of risk attention is related to the increasingly decentralised operations of a (major event) organization. It was demonstrated that as decentralisation levels increase, so must the number of alternative sources and communication channels of risk information. Therefore, in agreement with high reliability theorists[215] it is suggested that there must be risk information source and communication channel redundancy. ISS assurance checks can support such redundancy levels, since they not only detect new risks, but also ensure that sensitivity to operations is maintained. ISS assurance checks and the effective communication of their findings can retain reliable risk attention levels.

Closely related to this observation is the recommendation by High Reliability theorists Weick and Sutcliffe (2001, 2007) to use high reliability audits and questionnaires - such as the one used by the researcher for the purposes of this study (i.e. Appendix-A10) - in order to improve sensitivity to (a) high reliability failures, (b) deviances from related organizational objectives, and (c) differences in perceptions across different individuals and functions. The current study has shown that High

[213] E.g. Games-ISS SIM solution.

[214] E.g. AAR reports and focus group meetings; trial-and-error/simulated operations exercises; setting performance objectives and regularly monitoring and evaluating these.

[215] I.e. Sagan, 1993; Weick and Sutcliffe, 2001.

Reliability audits/questionnaires can indeed assist processes of 'risk attention', yet responses often appear to contradict actual behaviours. For example, in the A2004 Games-IS(S) project the adequate duplication of critical personnel and skills was identified as an operational risk, yet little was done to address this. Such cases, underline the role of the organization's contextual noise[216].

A further research observation with regards to reliable mechanisms of organizational risk attention is related to the impact of routinization and tiredness. The research findings (i.e. section 4.3.5) indicate that these factors can greatly affect organizational sensitivity to operations[217] and should not be downplayed by organizations that remain in an 'emergency' or 'operational/live' state for prolonged periods. The duplication of human resources and skills is of great importance - especially so where operations are critical.

Finally, it is observed that 'ambiguous' risks[218] often lead to inter- and intra-organizational tensions that can lead to blame-allocation structures, hindering processes of continuous learning and the reporting of suspicious activities. Therefore, tensions can impact negatively mechanisms of (ISS) risk attention and levels of operational management and organizational culture reliability. Decision-making with regards to ambiguous risks needs to be deferred to experts or authority figures - especially so where there is no luxury of time and risk management resources. ISS commitment of senior management and opinion leaders can considerably assist with the quick resolution of ISS risk debates and the allocation of attention to new or evolving ISS risks.

[216] Although High Reliability questionnaires can capture and communicate the status of related controls, their effectiveness is restricted by a number of factors: (a) the responses will be subjective, affected by the organization's contextual noise (i.e. section 4.4.4); (b) a significant and diverse sample of respondents is required; (c) questionnaire responses will have to be elaborated during interviews; (d) responses need to be monitored over time.

[217] I.e. Weick and Sutcliffe, 2001.

[218] I.e. Klinke and Renn (2006), IRGC (2005) and Appendix-A2.

5.3 ISS risk sense-making in a major event context

According to Hutter and Power (2005b:18)

> "risk encounters will be mediated by sources of 'knowledge' and by practices which may amplify or attenuate organizational sensitivity and 'inventive' responsiveness to disturbing events. Accidents and crises provide the most extreme challenge to existing frames of interpretation; near misses [...] may be suppressed by routines which are hard-wired into organizational memory. [...] Each risk encounter will be mediated by the legacy of organizational culture and its associated habits and always poses the problem of an alignment between human perception, conceptualization, assessment and management capabilities, and the risk 'event' itself".

Therefore, they suggest that 'sense-making' is the process where organizational actors transform new encounters with risk into acceptable managerial practices.

However, according to Jasanoff (2005) organizational encounters with risk can result in the suspension of sense or in multiple competing sense or epistemologies.

> "Facts and explanations may not be readily produced if the answer to the question 'what happened?' is difficult and contested. [...] The need to allocate responsibility will drive institutionally acceptable explanations and solution sets" (Hutter &Power, 2005b:21).

Short (1992:7) agrees and suggests that "individuals and organizations sometimes act not because they understand risks, but because they feel they must act".

In addition, explanations may encode blaming or learning, may persist or may be short-lived. Jasanoff (2005) suggests that some explanatory tropes recur while others are ignored. She also highlights the significance of preferences for forms of explanation which fit existing policy response possibilities[219].

Hutter and Power (2005b:24-25) further suggest that

> "who does the sense-making is critical. [...] Sense-making will vary across different groups. Styles of explanation may vary across different issues and

[219] According to Jasanoff (2005) risk event explanations can vary between short-run political explanations or a more systemic problem; preferences for technical/mechanical-type explanations rather than organizational and procedural failures; explanatory emphases on systems or on individuals; and finally, there are different explanations provided according to different cost implications.

> patterns of blame may not be consistent across even similar risk events. [...] Different groups have differential capacities to make sense of what has happened. Inequalities and dispersion in provision, access and experiential understandings are significant aspects of sense-making in organizational encounters with risk". They conclude that "sense-making activity is the organization's encounter with itself".

Utilizing the SARF (i.e. section 3.3.2.1) key points are considered with regards to the social and individual stations of Games-ISS risk amplification/attenuation, and the mechanisms of sense-making. Reflections for other organizations and reliable mechanisms of sense-making are also considered.

5.3.1. A2004 Games-ISS social stations of risk amplification

Given that prior to the 'Initiation' of the A2004 Games-ISS project none of the Games-IS project functions, IT partners and customers had strategically considered the issue of ISS, it came as no surprise that the Games-ISS team was initially the main source of ISS risk information. Accordingly, the Games-ISS experts were the ones that controlled the communication of ISS risk information and determined which ISS issues should receive greater attention, amplified or attenuated.

Therefore, in agreement with Hutter and Power (2005b) who suggest that different groups have different capacities to make sense of a risk depending on their access to risk information and experiential understanding[220], the Games-ISS team was the main social station of risk amplification.

Hence, the Games-ISS experts often amplified ISS risks for which they considered that urgent response was required. For example, they amplified the need to security harden Games-IS devices after the completion of TE-1, effectively *framing* this risk through a risk assessment and hacking scenario demonstration. This raised awareness across all Games-IS functions that had to implement the necessary controls, as well as the project's senior management that had to authorise the increased project costs.

Similarly, the Games-ISS experts often amplified ISS risks that they considered to be outside their jurisdiction/control, yet had an impact on their activities. Thus, poor physical security of Olympic venues and TSAs was repeatedly communicated to

[220] I.e. section 3.2.1 and *HERO* by Rosa (2003).

ATHOC and the Admin-ISS team. Indecision from the latter organization implied that the risk was persistently amplified throughout the project's lifecycle. Involving the Admin-ISS team in the Venue-ISS audits was an effective means to communicate the related risk concerns to the responsible organization. On the other hand, with the completion of the Games, the same risk was completely ignored during After-Action-Review (AAR) meetings since this was an issue beyond the responsibility boundaries of the Games-IS(S) organization.

In fact, it was regularly observed that an ISS risk was not persistently amplified or attenuated. Across different project phases the same risk was amplified, then attenuated; or vice versa. The Test Events played a key role in raising awareness of ISS risks and often amplifying these. For example, the first Test-Events (TE-1) demonstrated to Games-ISS experts, Technical and Venue-IS teams that the secure connectivity of Third Parties onto the Games-network had been completely overlooked. The great workload of venuisation preparations prior to TE-1 had hidden this ISS risk. Yet, this quickly changed when problems were made evident during TE-1. However, the same problem was once again attenuated between TE-1 and TE-2, when the implementation of other ISS controls[221] was stressed. Therefore, the great workload, complexity and number of ISS issues that had to be simultaneously addressed and coordinated, often led to the attenuation of several ISS risks[222]. The pressures of major project milestones often led to either the amplification or attenuation of risks.

However, patterns of amplification/attenuation did not only vary across project phases, but also across groups. Therefore, the risks associated with the insecure connectivity of laptops onto the Games-network was amplified in relation to Third Parties, yet remained completely hidden in relation to IT Partners, such as SWATCH. The *trust* shown towards Games-IS IT Partners operated as a risk attenuating mechanism, resulting in the lack of ISS assurance checks for SWATCH devices and the non-compliance of these.

Trust operated as a mechanism of amplification for a number of other Games-ISS risks. Thus, during the initial stages of the project, the trust shown towards the Games-ISS expert by senior/corporate management implied that he often operated

[221] I.e. the implementation of port security and ACL controls.

[222] Another instance where that happened was in relation to the provision of frequent and audience-specific ISS training.

as an *opinion leader* on matters of ISS risk management, determining the respective ISS decision-making processes.

However, as sources and mechanisms of ISS risk communication changed with venuisation and Test-Events, so did the processes of sense-making. Experiential knowledge increased awareness with regards to a number of IS(S) risks not only for the Games-ISS experts, but also ISS laypersons. The need to implement stronger access and authorization controls, security harden Games-IS devices, and implement a number of network segregation and connectivity controls were but a few of the ISS risks that were identified after the first Test-Events. What was also made evident was that collaboration with other Games-IS functions, partners and customers had to improve, while laypersons had to incorporate ISS controls into their technologies and procedures. Although this risk message was amplified by the Games-ISS team, it was attenuated by the majority of lay-groups. The extent to which ISS was common responsibility was an ambiguous issue. Ongoing operational rehearsals operated as a learning mechanism, gradually demonstrating to ISS experts and laypersons alike the extent to which Games-IS solutions and processes were interlinked and complex.

Therefore, although certain ISS risks were 'simple' in nature, the implementation of related ISS management controls was often ambiguous and, thus, greatly negotiated. For example, the security hardening of Games-IS devices was unanimously accepted as a necessary ISS control, yet its implementation was greatly problematic and contested among Games-ISS experts, system owners and the Operations team. Similarly, it was widely agreed that port security had to be implemented on the Games-network, yet its implementation was patchy, often leading to tensions between the Games-ISS experts and the Network specialists. The frequency with which such controls had to be updated and the extent of resulting errors and omissions further aggravated tensions between teams and often led to the allocation of blame. Yet, the lack of a centralised configuration management system and the inadequate ISS assurance controls were never acknowledged as risk contributing factors; only after the project was completed.

Overall, it appeared that whenever an ISS risk implied that further resources[223] had to be utilised, related problem factors were attenuated. Similarly, the lack of procedural controls was also attenuated. Despite the fact that during the early stages of the Games-ISS project the ISS expert stressed the need to adopt a holistic approach to Games-ISS, it appeared that even among ISS experts greater attention

[223] I.e. people, technologies etc.

was given to technical ISS risks and controls. The predominantly technical background of most ISS experts, and the continuous need to update and customise the Games-ISS technologies, implied that procedural ISS risks were attenuated within the experts' team. Hence, several ISS risk events were justified by providing solely technical failure explanations, rather than procedural and communication ones. In addition, risk events were also blamed on the lack of technical and management skills within other teams, and rarely did any Games-IS(S) team admit to its own inadequacies with regards to effective risk communications and coordination practices.

However, blame structures did not remain stable across the project's lifecycle. While during the early project stages no blame culture was observed, the operational rehearsals and the increasing demands to optimize the Games-IS(S) operations changed this. 'Testing' implied that teams had to interact more and coordinate their activities. This was particularly the case for the Games-ISS team that could not understand 'ordinary' and acceptable Games activity without the collaboration of other project functional teams. However, as the workload for all increased, prioritization of activities differed among groups. Thus, the Games-ISS team frequently amplified ISS risks, while Technical and Operations teams attenuated these. This ambiguity led to tensions and blame allocation. Problems had to be frequently escalated to senior project management for resolution. Senior management, which was overall committed to ISS, operated as a further station of social amplification, thus often putting an end to persisting and blame-allocating negotiations.

Blame-allocation structures changed once again immediately prior and during the Games. A shift from functional organizing to venue/operational organizing meant that social groupings changed; and so did respective loyalties. Tensions increased within operational teams; especially across different shifts. On the other hand, the time and visibility pressure of Games-time operations meant that such tensions were often short-lived and focus was given on the efficient resolution and containment of IS(S) incidents. Therefore, risk amplification/attenuation stations did not persist during Games-time.

Another observation made after the Technical Rehearsals and during the Games was that functional teams increasingly co-aligned their ISS risk perceptions and behaviours. The reduced levels of ambiguity and uncertainty, and the increased levels of environment stability meant that ISS experts and laypersons were better prepared to commonly address ISS risk events. Risk explanations and decisions were

increasingly decentralised and deferred to expertise, whether that was the TOC-SEC team or the various Technical and Venue-IS teams.

In fact, improved collaboration between ISS experts and laypersons also stressed - although at a late stage of the project - the significance of ISS procedural and communication/training controls. Such controls were not only an effective mechanism to ensure compliance to ISS policies and procedures, but were also a useful means to make sense of the benefits and costs of ISS controls, as well as the nature of the managed ISS risks[224].

Overall, it is observed that the Games-ISS team mostly operated as a social station of amplification. Meanwhile as 'Operational Rehearsals' revealed the complexity, uncertainty and ambiguity of various ISS risks, negotiations across Games-ISS experts and lay-groups also intensified. These led to even more frequent phenomena of risk amplification and attenuation, often resulting in the allocation of blame and the escalation of ISS decisions to senior project management. As, however, the environment became increasingly stable phenomena of risk amplification and attenuation reduced.

Nevertheless, some ISS risks remained *hidden* to both ISS experts and lay-groups. The insecure design of Games-IS applications, the insecure build of SWATCH laptops, the inadequate ISS access and authorisation controls, routinization, and the persisting configuration errors of Games-IS(S) devices, were all ISS risks that were normalised by the entire Games-IS(S) organization. This attenuation was either due to great levels of trust in technologies, procedures or groups, or because certain risk events were considered unavoidable and often materialised as near-misses that did not receive adequate risk attention.

5.3.2. A2004 Games-ISS individual stations of risk amplification

In addition to the social stations of amplification, the sense-making process of Games-IS(S) individuals was affected by a number of factors. As indicated for other parameters of the risk amplification process, the situational factors of the organization played a significant role.

[224] E.g. Venue-ISS audits not only indicated the levels of Third Party ISS policy compliance, but also demonstrated that the reason for their persisting non-compliance was the lack of Venue-IS staff ISS training.

Firstly, the smaller the size of the organization, the greater the extent of mentoring offered by Olympic-experienced personnel and managers. This direct communication provided guidance with regards to individual roles and responsibilities, and the prioritization of activities. Thus, during the 'Analysis and Design' project phase there were several opportunities for Games-IS(S) individuals to learn from past Olympic knowledge and informally discuss this with colleagues. Individuals were affected by *prior attitudes and experience*. Similarly, with the arrival of the SchlumbergerSema Games-ISS expert - who had prior Olympic experience - considerable *trust* was demonstrated towards him, which increased levels of ISS risk attention by other teams.

As initial ISS communications took place in an informal, team-working environment, ISS risk perceptions were debated with no tensions. The Olympic-experienced Games-ISS Manager was often sought to provide guidance and ISS risk communications appeared to have the desired effect and response.

However, with venuisation and growing levels of organizational size and operational complexity, ISS risk sources and communication channels changed. This affected individual processes of sense-making. As workload increased, the '*ability*' of ISS laypersons to follow ISS risk messages without distraction and their '*motivation*' to process these[225] decreased. In parallel, opportunities of ISS mentoring decreased as the Games-ISS experts had to turn their attention from planning and design to implementation.

The complexity of operational rehearsals and the associated performance pressure and visibility implied that laypersons' ISS risk attention deteriorated further. The Games-ISS Manager had to increasingly stress certain *qualitative aspects of the risks*, and *frame* ISS risk information as he considered fit in order to generate the desired ISS risk management responses. Therefore, the Games-ISS Manager consciously operated as an individual station of risk amplification[226]. Of the amplified ISS risks

[225] As considered in section 3.3.2.1, according to Chaiken and Stangor (1987) '*ability*' refers to the physical possibility of the receiver to follow the message without distraction. '*Motivation*' refers to the readiness and interest of the receiver to process messages.

[226] Risks that were amplified included among others the unmonitored use of IT-Volunteers, the insecure build of Games-IS devices, and the insecure connection of Third Parties on the Games-network.

the majority were effectively communicated and led to the recommended ISS controls[227].

However, the effectiveness of amplified risk communications did not persist. With the increasing demands for ISS practices across Games-IS functions, tensions started surfacing between teams. Despite indications that there was significant unauthorised activity in the Games-network, Games-IS individuals reacted to ISS messages which communicated that network perimeter controls were not adequate and additional internal-network restrictions would have to be implemented (i.e. *selection bias*). The performance problems of Games-IS operations caused by the mis-configured ISS technical controls further aggravated tensions. As a result, Games-ISS laypersons frequently *stigmatised* Games-ISS technologies and eventually the Games-ISS team. Any operational problems that were directly or indirectly caused by the implementation of an ISS control were considered representative of ISS-expert activities (i.e. *representativeness bias*). Such *blame* and *stigmatization* messages were particularly amplified by the managers of the Technical and Operations teams that had engaged in a power-struggle with the Games-ISS experts and manager. The intervention of senior project managers often contributed towards alleviating such tensions, thus acting as effective individual stations of ISS risk amplification/ attenuation.

In addition, it was observed that the greater the size of a functional team was[228], the less effectively ISS risk messages were communicated to its members. This was due to the fact that ISS risk messages were indirectly communicated to them via their respective function managers. Yet, most function managers operated as individual stations of risk attenuation, giving a low priority to ISS risk communications and coordination activities. It appeared that direct communication with ISS laypersons was a more effective way to sustain their 'ability' and 'motivation' to follow and process an ISS risk message without distraction. Therefore, the extent to which individuals - and social groups - attenuated/amplified Games-ISS risk messages also depended on the risk information communication channel. The greater the direct contact with the ISS-experts, the more each individual used their own criteria to make sense of ISS risk messages. Otherwise, in an increasingly decentralised organization, individuals had to depend primarily on their immediate colleagues and

[227] Nonetheless, some risk events were attenuated. E.g. the ISS risk posed by IT-Volunteers was greatly attenuated by ATHOC's IT Department Manager (i.e. *selection bias*).

[228] E.g. Network team, or Venue-IS team.

to a lesser extent on their personal experience in order to interpret ISS risk messages.

The effect of direct communication between Games-ISS experts and laypersons was demonstrated by the positive impact that audience-specific ISS training sessions had prior to TR-2 and the Games. Such interactive communications addressed ambiguous risks and strengthened individual interactions between ISS experts and laypersons, improving considerably the effectiveness of procedural ISS controls across the decentralised organization.

However, it is worth noting that Games-ISS experts also demonstrated biased judgements. On a number of occasions they attenuated ISS risks, particularly procedural ones. Given the predominantly technical background of most ISS experts, attention was primarily given to technical ISS risks. Only in hindsight (i.e. *hindsight bias*) did they acknowledge the value of ISS assurance controls, change and configuration management processes, and direct communications with other teams.

In addition, during Games-time it was particularly evident that the Games-ISS Manager often acted as an individual station of risk attenuation with regards to errors and omissions of his team. In fact, the great visibility of IS(S) activities during Games-time implied that a failure to admit personal/team-internal errors was an attitude observed across teams. Thus, several near-misses were never adequately recorded and communicated.

5.3.3. Reflections on the SARF mechanisms of 'risk interpretation'

In the current study, the SARF has operated as an effective heuristic tool in order to investigate the process of organizational risk sense-making. In parallel, this study has brought to the fore a number of issues relating to the SARF mechanisms of risk interpretation and amplification.

Firstly, this research has shown that risk sense-making starts with the process of risk attention; in SARF terms, risk interpretation starts with risk communication. The number and type of risk signals, information sources and communication channels, are all factors that influence how an individual and/or group classifies and communicates risks. As suggested by Jasanoff (2005) a great number of risk signals can lead to risk ambiguity and multiple risk explanations, or the suspension of sense. Similarly, who owns/controls a risk communication channel, and the language and classification categories built in risk-detecting technologies, are also factors that

affect the initial stages of risk interpretation. Therefore, the findings of this research have indicated that direct communication can increase social affiliation and improve the alignment of risk perceptions. In addition, identifying who owns a risk detection technology and communication channel can also point to potential risk amplification stations. 'Framing' of a risk starts with the choice of a risk communication channel.

Secondly and as also argued in section 5.2.3, the type of (ISS) risk will also affect the process of risk interpretation. For example, ambiguous risks will lead to competing interpretations and epistemologies. Also the more complex and uncertain a risk is, the more risk narratives and stories will emerge[229]. These will be affected by the interests, motivations and social affiliations of the various risk interpretation/ amplification stations, their occupational background and risk experience, and their organizational roles, priorities and activities at specific points in time. Even 'simple' risks can be ambiguous since their reorganization can imply a change in existing organizational structures of resource, workload and power allocation.

Risk ambiguity can also lead to the allocation of blame, and the stigmatization of technologies, people and functions. In fact, the effect of stigma and blame appear to ripple and lead to further rounds of amplification. In the A2004 Games case-study, such self-generating cycles of risk amplification would not terminate until organizational opinion leaders and authority figures concluded the risk negotiations with a finite - in the medium run - decision.

A further parameter that appears to influence the process of risk interpretation is that of the organizational structure and situational factors. For example, under periods of heightened time pressure and operational exposure there was an increased incentive among organizational actors/groups to collaborate, yet they also relied more heavily on heuristic mechanisms of sense-making - especially so where there was a lack of necessary expertise. Therefore as Short (1992) suggests, individuals and organizations sometimes act because the feel they must; not because they understand risks. This type of risk sense-making behaviour appeared to reduce in the A2004 Games-IS(S) environment as more experience was obtained through trial-and-error exercises. Thus, as long as lessons learned from operational rehearsals were recorded, communicated and monitored via further rounds of tests, the organization's levels of operational reliability appeared to improve over time. ISS risks became less complex and uncertain, and as an effect levels of risk ambiguity were also reduced. Repetitive rounds of risk amplification were eliminated and the

[229] I.e. Wiedemann et al (2003).

organization gradually achieved the desired level of operational maturity and stability.

At this point it is worth noting two more issues that this research has underlined. Firstly, a need has been identified to further investigate the ways in which processes of effective learning can affect organizational encounters with risk. Directions can be drawn from High Reliability theory[230], as well as the research in the field of risk communication and ISS awareness and training[231].

In addition, this study has shown that although organizational stability and operational maturity - which imply efficient risk anticipation and containment practices - can help reduce phenomena of risk amplification and attenuation, they can also lead to the reduced sensitivity to operations and the normalization of new or reoccurring risks. Expectations of organizational and operational stability can hide hazards[232].

Relating to the topic of hidden risks, the researcher argues that most SARF studies have historically focused on cases of risk amplification. Yet, in environments of high reliability requirements, risk attenuation is equally - if not more - important. Thus, some of the factors that this research has identified as risk attenuating ones include the following: (a) a plethora of - especially conflicting - risk signals; (b) a heavy workload that does not allow for 'able' and 'motivated' risk attention[233]; (c) the increased cost and power-threatening implications of a related risk reorganization; (d) the amplification of other risks that attract all attention; (e) the inevitability of a risk; (f) the complexity and political fragmentation of a risk problem; (g) the lack of effective risk monitoring mechanisms; and (h) the threatening of existing worldviews.

A further risk amplification or attenuation mechanism identified by the SARF is that of 'trust'. This study has shown that trust can operate as both a risk amplifying and attenuating factor, while 'distrust' operates solely as a risk amplifying factor. In fact, distrust can lead to stigmatization ripples, creating structures of blame.

Related to the topics of stigma and blame, it is interesting to note that in the A2004 Games-IS(S) environment, such phenomena were relatively short-lived. The

[230] I.e. Cooke and Rohleder (2006); Weick and Sutcliffe (2001, 2007); Sagan (1993).

[231] I.e. sections 2.3.3 and 2.2.2 respectively.

[232] I.e. Kasperson and Kasperson (1991).

[233] I.e. footnote-112, and Chaiken and Stangor (1987) on the 'ability' and 'motivation' criteria for risk information selection.

organizational culture of continuous improvement and learning, and the pressing need to timely resolve problems implied that blame structures and stigma effects did not persist. Learning prevailed over blame[234] in the medium/long run. This stresses further the above research argument with regards to the significance of effective organizational learning processes.

One final observation with regards to the SARF mechanisms of risk interpretation relates to the fact that most SARF studies tend to focus on one risk at a time. Yet, as this study has shown, in reality different risks occur simultaneously, competing for risk attention and sense-making cognitive and organizational resources. This condition adds to the ambiguity, complexity and uncertainty of risks leading to processes of risk amplification that extend beyond the 'here' and 'now'. Thus, the researcher suggests that it is necessary to consider the ways in which risks interact with one another.

5.3.4. Reflections for other organizations and reliable mechanisms of ISS risk sense-making

Reviewing the processes of risk sense-making in the A2004 Games-IS(S) project organization points to a number of observations with regards to the processes of ISS risk amplification and an organization's efforts to reliably assess, interpret and communicate ISS risk.

Similar to the mechanisms of (ISS) risk attention it is evident that the organizational structure, ways of working and situational factors, all affect the process of sense-making for both individuals and social groups. The degree of operational complexity and decentralisation has implications on the nature of ISS risks[235], the channels of communication, and the process of risk interpretation.

In addition, the project phase and associated contextual noise affect how risks are interpreted and whether sense is suspended or multiple competing senses are generated. Therefore, during phases of great workload and interactive complexity, priorities differed across groups and individuals and resources were often over-utilised. This led to political debates across different Games-IS groups. Within such

[234] I.e. Jasanoff (2005).

[235] According to Klinke and Renn (2006) and IRGC (2005) risks are classified into *simple*, *complex*, *uncertain* and *ambiguous*. Each type of risk determines the ISS risk management and communication approach (i.e. Appendix-A2).

an organizational context, encounters with ISS risk led to their amplification or attenuation, supporting the various pre-existing negotiations. Simple ISS risks were transformed into ambiguous ones since risk debates were frequently not related to the nature of the risk and its potential impact, but to the capacity of various individuals and groups to manage it. Risk explanations encoded blaming rather than learning.

The subjectivity of the ISS risk and control reliability assessments was also demonstrated by the ISS reliability questionnaires (i.e. Appendix-A10). The responses to these questionnaires indicated that ISS reliability assessments are not only dependent on the availability of information, political context and project phase[236], but on a number of additional factors. Teams and individuals that work closely together share similar ISS risk views, while the 'motivation' and 'ability' to process ISS risk information also depends on the clear specification and prioritization of roles and responsibilities, the types of skills and occupational experience of each person.

Furthermore, while it appears that the Test-Events initially fuelled ISS risk debates, they gradually facilitated the reduction of ISS risk complexity and uncertainty levels, thus also resulting in lower levels of ISS risk ambiguity. As indicated by the findings of the ISS reliability questionnaires, ISS experts and laypersons increasingly aligned their risk assessments.

The case-study data analysed above also indicate that different groups and individuals opted for different forms of risk explanation. These also varied across different project phases. Therefore, short-run political explanations were preferred to systemic ones throughout the project's lifecycle. It was only at the end of the project that systemic ISS risks were acknowledged. Similarly, Games-ISS experts and laypersons opted for technical explanations of failure, rather than procedural and organizational ones. Finally, the cost implications of varying risk event explanations also determined the process of amplification/attenuation[237].

---

[236] Major project milestones affected attention and sense-making processes, either amplifying or attenuating risks. In addition, routine Vs emergency ISS risk and reliability assessment circumstances also affected the process of sense-making.

[237] For example, risk signals related to the inadequate use of ISS assurance controls, a lack of centralised and automated configuration and account management systems and processes, and the lack of adequately duplicated ISS personnel were all attenuated. This was partly because of the cost implications of effective risk management solutions. Instead, it was often preferred to explain the above ISS risks by blaming teams and individuals for incompetency.

The diverse risk explanations witnessed by the researcher are also attributed to the varying ability of different case-study groups and individuals to make sense of what happened. In fact, by the end of the A2004 Games-ISS project the ISS experts acknowledged that cross-functional tests and communications significantly supported the attention and sense-making ISS risk processes. Thus, the researcher suggests that identifying the organization's social and individual stations of amplification/ attenuation can be helpful in directing ISS communication efforts and supporting the reliable management of ISS risks. In addition, monitoring the effectiveness of communications can be critical in the timely application of corrective action.

Finally, the above analysis indicates that centralised ISS management and monitoring processes and technologies can help ISS risk transparency and decision-making in an increasingly decentralised environment. Although such solutions may initially appear as unnecessary[238], scalability challenges will soon require that such processes and technologies are in place. Poor coordination and ISS assurance activities lead to increased complexity, uncertainty and ambiguity. In addition, the utilization of a formal process and tool to gather past information and knowledge can facilitate more effective and efficient learning - both within the lifespan of a single project, as well as across similar projects.

[238] Due to the efficient informal mechanisms of mutual adjustment.

5.4 ISS reorganizing in a major event context

The process of reorganization involves the creation of new formal and informal risk management controls and structures. According to Hutter and Power (2005:30) reorganizing activity embraces "the reform of concepts and language as well as the mechanics of practices". It is not just a single response to an encounter with risk but an unfolding and continual process which "embodies one or more implicit explanations of the failure". They suggest that "the process is continuous because reorganizing is always a source of risk, as well as its solution".

Reorganizing actions can be counterproductive if done in haste, and can be simply ignored if they are perceived as too expensive. Hutter and Power (2005b:30) suggest that

> "a chronic difficulty for reorganizing activity is that of being able to demonstrate clearly the benefits of risk management. [...] Reform processes where benefits are difficult to demonstrate must attach themselves to widely held beliefs and values in the institutional environment".

According to Kasperson et al. (2003) the fundamental and perhaps irresolvable difficulty for organizations is to be 'optimally' responsive to risk alerts by utilizing some form of 'screening' to avoid both over- and under-investment in protective measures.

Generally, it is agreed that organizational responses will tend to be conservative, reflecting the fact that "instituted community blocks personal curiosity, organized public memory, and heroically imposes certainty on uncertainty" (Douglas, 1987:102).

Hutter and Power (2005b:27) further suggest that formal/procedural compliance failures will "typically fail to stimulate any re-organizing activity and become dominated by other concerns. Only in retrospect do they come to have overriding significance".

They also argue that near misses are less powerful engines of change than actual accidents and disasters. Reorganization processes are usually reactions to adverse events, yet precautionary attitudes can drive 'anticipatory' responses.

Finally, Heimer et al. (2005) suggest that reorganizing involves contests over the direction of change, the legitimacy and expertise of the various participants, and negotiation over the rules. The nature of a risk and risk event and the process and

context of attention and sense-making will determine the institutional and social behaviour responses, the risk ripple effects across space and time, and the overall impact on the organizational levels of reliability.

5.4.1. A2004 Games-ISS risk institutional and social behaviour responses

According to the SARF, the process of risk amplification leads to a number of institutional and social behaviour responses, such as a change of attitudes, political and social action, organizational response, and social protest. In the A2004 Games-IS(S) project a series of factors affected responses to the ISS risk amplification process.

The ongoing Test Events facilitated a gradual understanding of 'ordinary' Games-IS(S) activity, which led to new technological controls as well as repeated updates of several ISS policies and procedures. However, revisions in procedural ISS controls were ineffectively communicated to both Games-ISS experts and laypersons. As such, attitudes were frequently slow to adapt to new ISS risk understandings, policies and procedures. Related improvements came mainly via practical experience. Overall, the increasing size and decentralisation of the organizational structure often restricted the communication of ISS risk interpretations, and thus limited reorganization activities[239]. The fact that procedural changes could not be always centrally monitored implied that they were less effective to technological changes.

The research findings also indicate that with regards to ambiguous ISS risks senior project management had to engage in the related negotiations, define acceptable and necessary ISS risk solutions, and thus motivate reorganization. Their involvement was particularly effective in cases where the ISS sense-making process implied an increase of project costs, and where the ambiguity of certain risks or the ambiguous rules of change[240] created social protest and tensions between teams.

Furthermore, it was observed that near major project milestones there were greater pressures to proceed with reorganizing IS(S) controls. Given that most project milestones were aligned to technological deliverables, reorganizing pressure increased with regards to technical ISS controls. However, procedural ISS risks and

[239] The A2004 Games-ISS metrics and venue ISS audits demonstrated that new ISS policies and procedures were inconsistently implemented across different business units (i.e. venues).

[240] I.e. Heimer et al. (2005).

controls were often ignored[241]. Attention to procedural risks remained inadequate to generate a significant change of attitudes until relative technical stability was first achieved. Such delayed attention and communication resulted in many of the detected problems remaining unresolved.

In fact, many of the IS(S) problems detected just before or during the Games remained purposefully hidden as individuals and groups did not wish to be blamed for any errors and oversights. It was only when risks materialised that risk-related information was communicated in order to facilitate effective containment controls[242].

Apart from the ways in which the evolving organizational structure and activities affected ISS reorganization, the cultural and political context of the project also influenced the organization's ability to reliably reorganize its operations. When the organization was in the 'Analysis and Design' project phase, reorganization was easier - due to the smaller size of the organization, yet less frequent. Each team operated in relative isolation, making a number of assumptions in their planning activities. As operational complexity and interdependence increased - exponentially, reorganization activities were hard to coordinate. Opinion leaders often clashed and the lack of automated, centrally-managed tools to implement changes meant that errors and omissions were observed across the decentralised organization. These generated further frictions, and blame structures emerged.

In fact, costly reorganization recommendations were frequently ignored and existing project resources had to be stretched out to cope with the increasingly challenging organizational environment. Thus, although changes did take place throughout the project's lifecycle, these were inconsistent and led to a relative stagnation of ISS reliability levels. Therefore, the availability of adequate project resources - people and IT - determined the effectiveness of ISS risk reorganization activities.

With regards to how risk characteristics affected the process of ISS risk reorganization, the more ambiguous a risk or its rules of change, the more reorganization delayed. This distracted attention and resources from other simultaneous reorganization activities.

---

[241] E.g. Third-Party and IT Partner ISS compliance, ISS training etc.

[242] I.e. section 4.3.5 and ISS incidents related to the delayed detection of: (a) of non-compliant IT Partners SWATCH; (b) mis-configured Antivirus solution impacting the performance of the OVR systems; and (c) insecure Games applications.

Complexity and uncertainty of ISS risks was addressed more gradually through the ongoing process of testing and simulation. Understanding of 'ordinary' Games-IS(S) activity was incremental and therefore readjustment of controls was also ongoing and repetitive. However, the lack of an effective means to monitor and manage configuration changes impacted the ability to effectively reorganize for complex and uncertain ISS risks. As such, many of these problems persisted, resulting in increased risk ambiguity levels.

Reorganization activities were also incremental during routine project phases. It was observed that although project phases of increased time pressure and exposure aggravated organizational tensions, they also motivated the greatest and most coordinated efforts to reorganize.

Also, as noted earlier, the degree to which attitudes changed depended on the skill-set, Olympic experience and occupational background of different persons. Olympic experienced staff collaborated more readily with the ISS experts to address ISS risks and implement new controls. In addition, Technical team staff was more appreciative of the need to implement certain technical ISS controls[243] than operations-focused teams. Similarly, the Games-ISS experts - with a mostly technical background - were keener to implement technical changes than procedural/ communication ones. It was only the ISS experts with a more strategic appreciation of ISS that were also keen to change their informal and formal processes of working. Finally, it was observed that individuals' and teams' ISS risk expectations also affected the type and degree of risk institutional and behavioural changes[244].

Overall, it is observed that ISS risk reorganization was a continuous process of learning and readjustment. Perceived and actual levels of ISS reliability improved only gradually and mostly around major project milestones.

---

[243] E.g. Access Control Lists (ACLs) and Games-IS device security hardening controls.

[244] E.g. Games applications had been previously used - successfully - in the Salt Lake (SL2002) Olympic Games. As such most Games-IS(S) groups and individuals expected Games applications to be problem-free. Most errors were normalised and a consideration of the ISS aspects were delayed (i.e. during the latter phase of 'Operational Rehearsals'). It was only after the Games - in hindsight - that the ISS problems of Games applications were acknowledged.

5.4.2. A2004 Games-ISS risk ripple effects and impact on levels of ISS reliability

The Games-ISS risk attention and sense-making processes not only impacted the reorganization of these risks and their controls, but often had spatial and temporal ripple effects that implicated the organizational and operational levels of ISS reliability. The various types of ripple effects observed included the following:

Firstly, the amplification/attenuation of one ISS risk could lead to the parallel reduced or increased attention towards other ISS risks.

Similarly, amplification of a certain aspect of an ISS risk could lead to the attenuation of other aspects. For example, with regards to the secure connection of laptops onto the Games-network, the non-compliance of Third Parties was amplified. This increased attention towards the particular group led to the attenuation of the same risk with regards to IT-Partners such as SWATCH.

Furthermore, the amplification/attenuation of ISS risks impacted the workload of particular teams or individuals, while it also had an impact on the degree of collaboration and communication among different teams. Such ripple effects directly impacted the levels of organizational ISS reliability.

The amplification process of ISS risks also had an impact on project costs and resource utilization. This, in turn, impacted the extent to which senior project management was involved in the project's decision-making and had to demonstrate their ISS commitment.

As seen in cases such as the one related to the need to implement Games-network segregation controls (e.g. ACLs), risk amplification processes also led to the stigmatization of technologies and teams. Where stigmatization led to the loss of trust, further rounds of amplification/attenuation were generated. These expanded over time and across different risk areas. In addition, increased/decreased confidence in ISS controls often led to the decreased/increased attention to other aspects of the same risk[245], or other ISS risks altogether.

A further ripple and impact of the amplification process was related to complex and uncertain ISS risks. Where such risks were amplified/attenuated, the level of risk

[245] E.g. increased confidence in the reliability of technical ISS controls lead to the increased attention to procedural ISS controls.

ambiguity was also impacted. This in turn affected the levels of organizational tensions with regards to the risk's nature and management.

The amplification/attenuation of ISS risks also affected the extent to which the overall role and responsibilities of Games-ISS experts were made visible to other functions and individuals. It also affected the extent to which laypersons appreciated their own ISS responsibilities.

Finally, a risk's amplification was observed to result into the increase/decrease of the physical dimension of the particular risk, or another related one. For example, the amplification of the poor physical security at venues led to the security hardening of Games-IS devices.

5.4.3. Reflection on the SARF mechanisms of 'risk response'

Further to insights relating to the SARF mechanisms of risk communication and interpretation, the current study has also highlighted a number of issues with regards to the SARF's mechanisms of risk response.

Firstly, the findings of this study show that - as proposed by the SARF - the process of risk amplification is indeed repetitive, with various rounds of feedback. This appears to be especially the case in organizational contexts of great operational complexity and high reliability requirements, where ISS risk reorganization is supported by a continuous process of learning and readjustment.

The above observation is directly related to the type of risks (i.e. Appendix-A2) that are encountered by an organization, as well as the organization's structure and situational factors. Therefore, as also highlighted for the SARF processes of risk communication and interpretation, *ambiguous* risks appear to require management methods that support the integration of stakeholder involvement and communication. Such negotiations also benefit from the presence of opinion leaders and accountable authority figures that are willing to decide on the direction of reorganization in case of inconclusive risk debates. This is particularly the case within an organizational context where there is inefficient time and resources to deliberate for long periods.

Complex and *uncertain* (ISS) risks, on the other hand, appear to require several rounds of risk communication, interpretation and response prior to the organization reaching a reliable and mature level of risk handling. Both these types of risk can

significantly benefit from (a) defining clear organizational risk objectives, (b) an effective process of organizational learning that continuously feeds new results and risk understandings into the organization's routine operations, and (c) a variety of risk information sources and communication channels. The role of technology and (ISS) risk assurance controls can be particularly important in facilitating this process of continuous learning and organizational reflexivity.

In fact, this study has shown that the effectiveness of risk response/management efforts depends on retaining organizational attention on the identified risk beyond the stage of risk sense-making. By endorsing a risk management decision through appropriate communications, and the monitoring and evaluation of risk control effectiveness, organizational behaviours and practices can indeed change.

However, the current case-study indicates that even organizations that aim for highly reliable operations require several rounds of 'risk encounters' in order to effectively respond to identified risks. As suggested earlier in this research, the organizational structure, context and situational factors (i.e. Table 3.1 and section 4.4) will greatly affect the organization's capacity to effectively and reliable anticipate and/or contain (ISS) risks. For example, in an organization whose situational factors[246] change too frequently - such as in a major-event/project organization - reorganizing will be hindered by the time consuming process of adapting human behaviour, language and the mechanics of practices.[247] As several scholars have noted[248], organizational responses will be conservative and instituted community will block change. Also, reorganizing actions that appear to be done in haste will not allow organizational members/groups to become familiar and appreciative of these, leading to a loss of trust and/or 'motivation' to incorporate new controls into existing practices.

Furthermore, the findings of this research verify existing arguments[249] that formal and procedural compliance failures will typically stimulate reorganizing only in retrospect of a major accident, since such failures tend to fundamentally question existing institutionalised ways of working and organizing.

---

[246] I.e. age and size, technical system, environment, and power factors of the organization (Mintzberg, 1979, 1981).

[247] I.e. Hutter and Power (2005b).

[248] E.g. Douglas (1987), Sagan (1993), Vaughan (2005).

[249] I.e. Hutter and Power (2005); Vaughan (2005); Sagan (1993).

Hence, the findings of this research also indicate that risk reorganizing and response are closely related to establishing effective structures of organizational learning and change management. Such centrally managed and monitored systems can greatly improve the organizational encounters with risk[250], providing risk response coordination and transparency. In addition, this research has verified that learning from (ISS) incidents can indeed be an effective means to stimulate risk reorganizing, since it supports an organizational sense-making process of defining what is 'ordinary' and acceptable activity[251].

Reliable structures and technologies of organizational learning and change management are also closely linked to an organization's ability to demonstrate clearly the benefits of risk management controls and response[252]. Therefore, the researcher supports that effective and reliable organizational responses to risk require practices and structures that will be able to assure, measure and monitor the effectiveness of risk controls. As suggested in sections 2.3.2 and 2.3.3 of this study, in order to handle 'systemic' risks interdisciplinary and integrative mechanisms of risk governance are required[253], where the role of context, risk communication and coordination processes are brought to the fore.

A final reflection with regards to the SARF process of risk amplification and risk response relates to the methodology used for the purposes of this research. The researcher suggests that a longitudinal, case-study research methodology provides a 'bounded system' [254] in order to study the process of risk amplification. Kasperson et al (2003) have identified that SARF research often suffers from limitations with regards to risk response ripples and impacts being unbounded, in the sense that their magnitude or persistence over time is not well known. However, the case-study investigated in this research is one of specific time and space boundaries, while the organizational encounters with ISS risk are investigated from the project 'Initiation' to its 'Closure'. The implications of this 'bounded system' include that risk ripples and impacts are considered over the two year period of the A2004 Games-ISS project, supporting an in-depth analysis of the research elements of interest (i.e. section 3.3.1) across vertical and horizontal dimensions of analysis. This research has shown

[250] I.e. Sagan (1993); Weick and Sutcliffe (2007); Cooke and Rohleder (2006); Vaughan (2005).

[251] I.e. Cooke and Rohleder (2006); Spagnoletti (2006).

[252] I.e. Hutter and Power (2005b); Power (2008); Renn (2008).

[253] I.e. Klinke and Renn, 2006; Renn, 2008; IRGC, 2007.

[254] I.e. Creswell (1998).

that the processes of risk amplification and response are indeed iterative, while risk ripples and impacts extend to other risks and controls, as well as over time. Hence, reflecting on the SARF processes of risk amplification and response, the researcher suggests that studies that utilise the SARF can benefit from its application within a 'bounded' research environment.

5.4.4. Reflections for other organizations and reliable mechanisms of ISS risk reorganizing

Having reviewed the process of ISS risk reorganization within the A2004 Games-IS(S) environment it is verified that the nature of a risk/risk event and the process and context of risk amplification will determine institutional and social behaviour responses as well as the organization's capacity to reliably manage ISS risks.

With the completion of the A2004 Olympic Games event - despite a number of issues that were identified to require future improvement - the Games-ISS project was labelled as a 'success'; by both Games-ISS experts and laypersons[255].

Keeping in mind that ISS reliability assessments are partly subjective[256], while the related research questionnaire[257] was not necessarily exhaustive, it is interesting to note that by Games-time organizational and operational ISS reliability levels were indeed at their most mature; in striking contrast with findings 17 months earlier in the project lifespan. This indicates that achieving mature levels of reliability was an ongoing learning process of reorganization.

Similarly, the organization's capacity to reliably anticipate and contain ISS risks during Games-time was an outcome of the ongoing processes of risk amplification which - as examined above - were affected by a number of factors such as: (a) the organizational structure and situational factors; (b) the contextual noise; (c) the expectations, motivations and obligations of various stakeholders in the ISS management process; (d) the characteristics and type of ISS risks; and (e) the routine or emergency circumstances of the risk amplification process.

---

[255] In fact, a number of laypersons suggested that by the end of the project, one of the greatest lessons learned was related to the significance and role of ISS practices in a major IS integration project, such as the A2004 Olympics.

[256] As discussed in section 4.4.4.

[257] I.e. Appendix-A10.

The above factors also determined the lessons learned by the Games-IS(S) organization after the event's completion. As examined in section 4.3.6, not all ISS problems were acknowledged with the completion of the Games. Indeed, formal/procedural compliance failures were acknowledged in retrospect[258], yet organizational forces 'normalising' ISS incidents and near misses persisted. Lessons learned still embodied specific explanations of failure which reflected each individual's and team's expectations, future motivations and obligations.

It is, therefore, suggested that formal knowledge-transfer and After-Action-Review (AAR) practices can be particularly useful across such projects. Yet, one should remain mindful of the tendency to 'normalise' risks and risk events - even in retrospect. Lessons learned in a past project should not restrict one's future attention only to the risks identified previously. It is only via the critical investigation of organizational encounters with risk that an organization's capacity to reliably manage ISS risk can be understood; and perhaps, to an extent, predicted.

[258] I.e. Hutter and Power, 2005b:27.

5.5 Conclusion

The above chapter has considered the parameters and mechanisms of risk amplification in the A2004 Games-ISS project environment. The aim was to improve understanding of an organization's capacity to reliably manage - and predict - ISS risks, while critically reviewing the key SARF concepts. Observations and insights have been extended to other organizations of similar practices and/or operational objectives.

It has, therefore, been shown that similar to several contemporary organizations, major event/project organizations are environments that encounter the unexpected, yet need to demonstrate reliable organizational structures and operations. Thus, they must remain 'mindful'[259] of organizational and individual tendencies to 'normalise' risk events. They need to regularly monitor and evaluate their controls of ISS reliability, seeking to understand their internal- and external-facing processes of risk amplification.

Hence, the researcher has argued that within an organizational context of high reliability requirements, the process of *risk attenuation* is equally important to that of amplification. This point is underlined by the research findings which indicate that despite reliable processes of risk organizing, failures appear inevitable in the longer run.

After a detailed consideration of the A2004 Games-IS organizational efforts to reliably manage ISS risks, the researcher leans towards Sagan's (1993) suggestions with regards to the limitations of high reliability criteria and practices.

Specifically, Sagan suggests that although highly reliable ways of working and organizing can significantly improve organizational risk and safety management efforts, the *structure of an organization* - including its high interactive complexity and tight-coupling - will present limitations to such efforts. Sagan argues that the organizational learning from risk signals and events will be restricted for several reasons, including the ambiguity of incident causation; the politicised environments in which incident investigation and sense-making takes place; the human tendency to cover up mistakes; and the secrecy both within and between competing organizations.

---

[259] '*Mindful management*' is a term proposed and investigated by Weick and Sutcliffe, 2001.

Therefore, the findings of this study stress a number of issues, along with future research directions:

Firstly, there is a need to conduct further research with regards to effective learning and knowledge transfer mechanisms within and between organizations and projects. Such investigations can also address the 'performance paradox' identified in the fields of mega project/event management[260], thus improving highly reliable practices.

In addition, this research has shown that SARF predictions are restricted by a number of factors, such as the dynamic, continuous and not-always-visible interactions of different risk amplification process mechanisms, and the great number and context-specific parameters involved into the process of risk amplification. Although organizational context and risk decision-making history add great insight into the process of risk amplification, such an understanding is difficult to achieve because of physical - time and space - restrictions.

Furthermore, it is the researcher's view that the SARF needs to consider more explicitly the organizational structure and technologies of an organization, since these play a critical role in the organizational encounters with risk[261]. In addition, risks cannot be considered in isolation since they interact not only in terms of their physical impact, but also in terms of how they affect risk perceptions and responses.

Nonetheless, investigating and understanding the amplification process and organizational encounters with risk can improve efforts to reliably manage (ISS) risks. By understanding the mechanisms of risk identification and communication, the processes and stations of amplification[262], and the limitations to risk reorganizing, attention can be drawn to the obstacles of a highly reliable organization and operations. Meanwhile, such a deep understanding can also provide justification for organizational choices with regards to the appropriateness (and cost) of (ISS) risk management controls.

Hence, what is overall underlined by the above research insights is that organizations can no longer solely rely on deterministic and technical, risk-calculating practices. (ISS) risks have been shown to be multi-dimensional and greatly context-specific. In addition, errors are part of organizational life and it is unrealistic to aim for their

[260] I.e. section 2.4.1.

[261] I.e. Vaughan (2005).

[262] I.e. including their interests, motives and behaviours.

complete elimination. The risk management objective of contemporary organizations has shifted from dry risk-calculating statistics to structures and processes of (ISS) risk assurance and governance[263]. Inclusive risk governance frameworks - such as that suggested by the IRGC (2005, 2007) - aim to establish organizational structures and processes of assurance that are able to demonstrate that reliable and due diligence risk management controls are in place.

Beyond that shift towards practices of (ISS) risk governance, the balance of how much to spend on risk management will be a persisting debate [264]. Understanding the process of risk amplification can direct such decisions. However, the researcher suggests that the extent to which an (ISS) risk is amplified or attenuated is not as important as the extent to which an organization can demonstrate that it reliably anticipates and contains risk. Further research in the particular field is considered necessary.

[263] I.e. sections 2.2.2, 2.3.2 and 2.3.3.

[264] I.e. Kasperson et al (2003).

6. Conclusion

6.1 Recapitulating key ideas

6.1.1. Research objectives and findings

Commencing this research with an investigation in the fields of ISS and organization theory two issues were particularly evident. Firstly, ISS risk management practices are essential to any contemporary organization that aims to securely handle its information, while being able to demonstrate its reliable and trustworthy operations to its partners and service/product customers. Secondly, corporate and governmental IS infrastructures are becoming increasingly complex and interconnected, with a near-zero tolerance for failure. As such, contemporary organizations are increasingly required to deliver highly reliable and secure information management practices. An operational ISS failure can have a disastrous impact on their legitimacy and survival, as well as detrimental implications for their stakeholders and the wider public.

In addition to the above observations, investigation into contemporary challenges of organizing indicated that corporations and governments increasingly organize their activities in mega-infrastructure projects and events which, however, have historically performed poorly. Thus, mega-project/event organizational structures and IS infrastructures not only appear to be prone to accident and failure, but also have a low risk tolerance level. Yet, the implementation of IS(S) infrastructures in mega-event/project organizations has been inadequately - if at all - investigated, while related tools and methodologies are not available for practitioners who have great demand for these. Hence, researchers[265] have increasingly suggested that there is a need to consider factors that challenge the successful performance and delivery of mega-project/event organizations and IS infrastructures. They have pointed out an urgent need to identify the methodologies, approaches and processes that will ensure highly reliable operations of mega-project organizations.

Therefore, the objective of this research was to investigate and understand ISS risk management practices and challenges in a mega-project/event context, which is prone to accident, yet has a low risk tolerance level. More specifically, by adopting a sociological and interpretivist approach with regards to the investigation of 'risk', the researcher aimed to understand how ISS management practices, risk perceptions and behaviours can affect a mega-event's capacity to deliver highly reliable IS

[265] I.e. Silvers, 2008; Flyvbjerg et al, 2003.

operations. The focus was not one of testing hypothesis, but an ideographic one that sought to understand the causes and related patterns of behaviour leading to the reliable, or not, ISS operations. Such an approach is particularly relevant in the case of subject matters such as the one under investigation, that still have a lot of maturing to do.

In order to answer the research question a cross-disciplinary approach was adopted, bridging concepts and approaches from across three different research fields, namely information systems security (ISS), technology hazard/risk management and major-events management. It was suggested that in order to understand the organizational capacity to manage ISS reliably, closer attention should be paid to the structural, political and cultural context of the organization. The perceptions of risk and ISS behaviours that the organization aims to manage need to be considered across various levels of analysis - both vertical and horizontal[266]. Such in-depth understanding could lead to an improvement of organizational ISS risk communications and controls.

Thus, the methodological approach adopted was that of a longitudinal case-study, while the data collection and analysis efforts were focused around the following elements of interest: the structural, cultural and political context of the major-event organization under study; the expectations, obligations and motivations of the different mega-event stakeholders; and the nature and type of ISS risks. The objective was to consider how the above factors impacted ISS risk perceptions, behaviours and management efforts across 'routine' and 'emergency' circumstances, as well as with regards to delivering highly reliable ISS operations.

The above elements of research interest were considered both vertically and horizontally, thus assessing the organizational capacity to learn and improve ISS behaviours and practices over time. In line with proponents of the socio-organizational approaches to ISS and technology hazard/risk management, it was proposed that the investigation and understanding of the organizational encounters with (ISS) risk can inform and thus improve ISS reliability management efforts of inherently risky major-event/project organizations.

[266] The vertical elements of research interest are presented in section 3.3.1. The horizontal dimension of research analysis refers to 'time'. Also see section 3.2.2.

The findings of this research were numerous and applied beyond the strict boundaries of the organizational context under study, namely the Athens 2004 (A2004) Olympic Games-ISS project.

With regards to the management of ISS it was identified that the evolving organizational structure, culture and politics often determined the outcome of ISS management efforts, and vice versa.

It was also made evident that the delayed strategic involvement of ISS experts in the IS megaproject led to increased project costs and/or the compromised ISS reliability, as well as increased levels of ISS risk ambiguity. It was found that ISS is not a merely technical issue, but a strategic one that has to interact with various other organizational functions and groups. These observations stress the need for leadership and effective coordination mechanisms with regards to the reliable implementation of an ISS infrastructure and project. The presence of persisting ISS risk uncertainty in a 'no-tolerance-for-failure' organization will lead to increased ISS costs in the long run.

With regards to the process of ISS risk amplification and the implications on 'mindful' (i.e. highly reliable) ISS management, the research findings indicated that both perceptions of ISS and reliability levels are indeed affected by a number of factors: the evolving organizational structure, work coordination and communication patterns; the political negotiations, motivations and expectations between and within groups and opinion leaders; the nature of the identified ISS risks and controls; and the operational phase of the organization which influences whether ISS management controls and risks/risk events are perceived as 'routine' or 'emergency' ones.

Furthermore, it was made evident that involvement of all stakeholders in ISS risk management decisions is not always productive and necessary; this greatly depends on the type of risk. Challenges with regards to stakeholder involvement are intensified in a major-project/event environment as the organizational structure, activities, and context change with great speed. As such, it is not always possible to detect and involve all ISS risk stakeholders in a timely and effective manner; decisions often have to be made without everyone's involvement and agreement.

The research findings also highlighted that ISS assurance controls are a significant means to ensure not only ISS compliance, but also improve coordination efforts across different organizational functions and ISS stakeholders. ISS assurance controls can raise overall ISS awareness and foster a reliable ISS organizational culture. In

addition, centrally managed and monitored organizational processes[267] can greatly improve ISS risk transparency and coordination efforts across teams, while supporting the enforcement and monitoring of ISS controls. However, the research also demonstrated that procedural and communication aspects of ISS risks are often overlooked, and only in hindsight do they receive adequate attention.

Instead, it was identified that within an interactively complex, tightly coupled organizational environment, considerable resources need to be spent on mapping 'ordinary' IS(S) activities. Continuous testing, an effective after-action-review learning process, training and other centrally managed procedures (as discussed above) can help to that direction. Yet, exceptions to 'ordinary' activities do occur, and project and ISS staff need to mindfully address these, making sure that any newly identified ISS risk is reliably anticipated and contained. Attention should be given to ISS risk expectations that may lead to the normalization of ISS risk signals. However, in agreement with Turner (1978), it was demonstrated that most ISS risks and risk events were persistent ones that had an 'incubation period' of early warnings and near misses.

In fact, it was demonstrated that the reliability levels of the risk attention and sense-making processes were greatly affected by the rate and scale of organizational change in the case-study environment. Hence, ISS risk information sources and communication channels require to remain flexible and prepared to adjust to organizational changes. The research findings highlighted the benefits of direct ISS risk communications, while where indirect communications are used, their effectiveness requires to be regularly monitored. In addition, it was shown that regular audience-specific ISS training and audit activities can greatly increase effectiveness and reliability of ISS risk identification sources and communication channels.

Moreover, this study has highlighted the significance of the various IS(S) incident management and monitoring technologies in detecting, reporting and classifying ISS risks. However, such controls appear unable to reach their full potential until they are adequately customized. In a complex and uncertain environment such customization can be only achieved through testing and practice. The optimization of IT solutions that support the detection and communication of ISS risks is a learning process that requires considerable time and resources. Therefore, the researcher has argued that mechanisms to capture and transfer such experience can greatly assist

[267] Such as change, configuration and incident management processes.

towards achieving greater returns on investment and increasing levels of operational reliability.

Finally, the current study has demonstrated that ambiguous ISS risk often lead to inter- and intra-organizational tensions, blame-allocation structures, while hindering processes of continuous learning and the reporting of suspicious activities. Decision-making with regards to ambiguous risks requires to be timely deferred to experts or authority figures. In addition, centralised ISS management and monitoring controls and technologies can further support ISS risk transparency and decision-making which can facilitate the effective management of ambiguous ISS risks[268].

Apart from the above observations, the current research highlighted a number of additional findings related to major-events/projects and other organizations of similar structural characteristics.

Overall, it was demonstrated that a project's scope and context directly influence ISS activities and processes of risk attention, sense-making and reorganization. In addition, it was made evident that ISS management activities greatly depended on the practices, skills and risk perceptions of other functions and stakeholders. Within an environment of great complexity and interdependence the delay or problematic implementation of one project deliverable can impact other ISS risk profiles and associated controls.

It was also demonstrated that within a major-event organization, practical experience and the tacit knowledge gained through trial-and-error and operations simulation activities can considerably improve the reliability of risk anticipation and containment practices. In fact, the reliable operations of a major-event/project organization imply that skills and resources - including those related to IS(S) - need to be duplicated[269]. However, such a control is costly, which explains the heavy reliance of several major events on inexperienced volunteers that join the organization at the last-minute. Such a choice greatly impacts the risk profile of a

---

[268] Although centralised ISS management and monitoring solutions may initially appear as unnecessary, scalability challenges - especially within an organization that quickly expands its size and operations - will soon require that such processes and technologies are in place.

[269] In line with high reliability arguments in favour of redundancy, the findings of this research indicate that within organizations of an increasingly decentralised structure, the alternative sources and communication channels of risk information need to also increase. Similarly, human resources and skills need to be appropriately duplicated where operations are critical, as routinization and tiredness can severely impact the reliability of risk attention mechanisms.

major-event organization, and should therefore be timely taken into consideration. IS volunteers need to be (ISS) trained and gradually incorporated into the organization's operations, while their access and authorisation privileges need to be closely monitored. As indicated above, direct ISS communication and training are effective ISS communication channels and should formally and gradually target the growing numbers of major-event staff/volunteers. It is interesting to note, however, that due to the great reliance of major-events on volunteers the ISS risks posed by them are greatly attenuated, representing an *ideological hidden risk*[270].

It was also noted that in a major-event context clear direction and strong leadership from senior management or experts are critical success factors. The scale and complexity of major-events blurs the greater picture for most teams and individuals, leading to tensions and inappropriate prioritization of project activities. Leadership and the effective communication and monitoring of ISS risks among different functions are key in avoiding ISS errors and tensions.

Effective communication and collaboration with the decentralised (venue-based) IS teams can also greatly improve the enforcement of ISS controls, the anticipation and containment of ISS risks. As for collaborating with other not-contractually-bound partners, consistent efforts are required in order to communicate to them the ISS risks and necessary controls. Effectiveness of communications and compliance to ISS controls must be regularly evaluated and monitored.

Finally, after-action-review (AAR) and transfer-of-knowledge processes are vital and should be implemented soon after a risk event[271], while lessons learned need to be monitored over time. Cross-functional AAR meetings are also helpful in raising attention to ISS risks. However, there will always be a tendency to amplify/attenuate risk events in retrospect. As such, where possible, an impartial third party should monitor these processes.

[270] I.e. Kasperson and Kasperson (1991).

[271] I.e. prior to the normalization of failure explanations.

6.1.2. Research contributions

Similar to the findings of this research it is suggested that this study has made a number of contributions across the fields of ISS, technology hazard/risk management, and major-event/project management.

With regards to the field of ISS, this study has considered the concept of 'reliable ISS management', suggesting that organizational theories of 'high reliability' and 'mindful organizing' can be applied to the field of ISS. This linkage of inter-disciplinary concepts can be utilised to assess the effectiveness of ISS management controls in organizations of near-zero tolerance for failure. Furthermore, this study has integrated concepts from across disciplines, such as sociology and psychology, while putting forward the case of ISS risk assurance and governance practices.

In addition, this research has investigated the still maturing behavioural aspects of ISS within a specific context, focusing on means of effective ISS risk communications and decision making that can lead to greater ISS compliance levels. In line with suggestions from a number of ISS researchers[272], this study has also considered ways to create an effective ISS culture that is integrated with the organization's work culture and structure.

Finally, this study has utilised the SARF in order to investigate ISS incidents and risk events with a theoretically founded methodology.

In relation to research contributions to the field of ISS hazard/risk management, the use of the SARF supports the need for holistic risk management and communication methodologies that are founded on solid theoretical underpinnings, which can facilitate the improvement of ISS practices. Using SARF as the conceptual framework to link the organizational context with the process of change resulting from ISS management practices, it supports the analysis of ISS risk perceptions and behaviours across a number of contextual levels (i.e. Fig.3.4). As identified in Chapter 2 of this study this is an area that has been inadequately explored, yet can greatly benefit the effectiveness of ISS management controls and communications.

[272] I.e. Jones and Ashenden, 2005; Jain, 2006; Mishra and Harris, 2006; D'Arcy and Hovav, 2006.

Hence, SARF points to potential mechanisms of ISS risk amplification/attenuation. The research analysis indicates that risk information sources and communication channels[273] affect organizational processes of risk attention and sense-making. Similarly, the research data analysis indicates that the organizational structure, activities and contextual noise interact to determine how ISS risks/risk events are perceived, interpreted and eventually result in behavioural and formal, organizational changes with regards to the reliable management of ISS risk. Thus, stigmatization, trust, and the characteristics of ISS risks[274] are indeed detected to amplify/attenuate risk perceptions, and determine the organizational explanations of failure[275].

Furthermore, this research demonstrates that consideration of the high reliability criteria in determining an ISS management strategy and tactical activities can significantly improve processes of organizational reflexivity; despite the process's subjectivity. This can support an ongoing process of learning and improvement.

In fact, the current study shows that similar to any other organizational practices of risk management, the management of ISS is a continuous learning process of, ideally, gradual optimization. This learning process is complex and ambiguous, conditioned by culture and the organizational context. Similarly, learning from ISS errors is a continuous process which cannot be easily forced into univocal, totalizing causal narratives. Instead, learning from errors is a process that needs to be 'mindfully' sustained. This research has demonstrated that an organization's capacity to reliably anticipate and contain ISS risks is an outcome of the ongoing process of risk

[273] As indicated in Chapters 4 and 5, risk information sources and information communication channels differ across different project phases, organizational structures and situational factors

[274] I.e. procedural, technical, organizational/communicational and simple, complex, uncertain and ambiguous.

[275] E.g. In an organization of strongly technical expertise, there is indeed a tendency to stress the technical aspect of ISS risks and ignore more communicational and procedural aspects of the same risk.

amplification which - as examined above - was affected by a number of factors[276]. These factors also affect the organization's capacity to learn from errors[277].

A further contribution of this study relates to the observation that ISS experts and laypersons alike are prone to biased judgements of ISS risk. However, this finding does not negate that there is a hierarchical epistemology of risk[278]. A number of factors determine the degree of bias, such as occupational background and organizational/contextual experience, cost and political implications, and proximity to risk. Nonetheless, in order to identify the interplay and overall impact of these factors one must closely investigate the organizational structure and context.

In addition, this research has indicated that ISS risk management practices within an organization are influenced by a number of other administrative functions of the organization[279], which are not necessarily applicable only to major-event/project organizations. Therefore, some degree of generalization is possible with regards to ISS risk management findings of this research.

Research contributions specific to the field of major-event/projects include the investigation of ISS and ISS risk management practices within the particular context; an area that has previously not been considered in-depth, yet has been identified to be of critical importance to the success of a major-event/project.

Thus, this research has investigated the ways in which the organizational demands and challenges of a major-project/event can impact ISS management practices. It

---

[276] This study has identified that the following factors influence an organization's capacity to reliably manage ISS risks: a) the organizational structure and situational factors; (b) the contextual noise; (c) the expectations, motivations and obligations of various stakeholders in the ISS management process; (d) the characteristics and type of ISS risks; and (e) the routine or emergency circumstances of the risk amplification process.

[277] As examined in section 4.3.6 of this study, not all ISS problems were acknowledged with the completion of the A2004 Games. Although, formal/procedural compliance failures were acknowledged in retrospect, organizational forces 'normalising' ISS incidents and near misses persisted. Lessons learned still embodied specific explanations of failure which reflected each individual's and team's expectations, future motivations and obligations.

[278] I.e. section 3.2.1 of this study.

[279] For example: human resources, procurement, and financial management, as well as marketing and promotional activities. Within a context of projects and events, the management of time and work activities will also greatly influence ISS risk management practices - from the capacity to pay 'mindful' attention to ISS risks/risk events, to the way these are 'mindfully' interpreted and change organizational behaviours, and finally to the degree that the organization provides 'mindful' explanations of failure which result to an improvement of high reliability ISS management practices.

has demonstrated the subjectivity of ISS management processes, the ways in which a project's scope and context interact with efforts to manage ISS risks reliably, and stressed that communication and procedural ISS controls are often neglected, yet can be cost-effective and critical to the success of reliable ISS practices. Furthermore, this study had highlighted the challenges that organizational and operational scalability present for ISS management practices. Meanwhile, it has also stressed the significance of decentralising the enforcement of ISS management controls, yet maintaining centralized monitoring and management of some ISS risk controls and processes[280].

With regards to scalability challenges, this study has also underlined that ISS risk communications need to adapt flexibly to the organization's requirements. ISS risk communications with the various project functions and stakeholders need to become increasingly formal, yet as direct as possible. Yet, this study has demonstrated that practical real-life experience cannot be easily communicated to other members of the organization. Therefore, ISS training and practice are necessary. ISS training should focus on real life examples, while trial-and-error/simulation learning processes must be available. The effectiveness of ISS communications needs to be frequently evaluated and accordingly adapted.

Finally, with regards to research contributions to the field of major-events/projects, this research has stressed the great levels of interactive complexity and interconnectedness within such environments, and suggests that the utilization of project/event management models such as EMBOK can facilitate the detection of interdependencies among different project administrative functions and domains of knowledge. This can assist planning activities.

[280] E.g. change management, configuration management and ISS assurance management controls.

6.2 Research considerations and future directions

6.2.1. Reflections on the research conceptual framework

As examined in section 2.2.1 of this study, research in behavioural ISS is often accused of a descriptive nature, not supporting the generation of predictive rule-sets. In addition, it is suggested that such type of ISS research is often inconclusive, partly due to the individual and situational differences which moderate the impact of various countermeasures. Thus, a need to contextualise any behavioural findings and associated solutions has been suggested[281].

Parallel to the above assertions, researchers[282] have highlighted a need to expand the immature body of IS(S) literature that adopts a sociological/organizational and behavioural approach to ISS, with the utilization of an integrative risk conceptual framework.

Guided by these observations the researcher has sought to utilize an integrative risk framework that appreciates the dynamic nature of organizational encounters with risk, and supports an in-depth contextual analysis across various levels. In addition, the researcher supports the need to increase the use of interpretive approaches for the analysis of organizational risk experiences. Therefore, the SARF was chosen to focus primarily on the in-depth contextual description and understanding of the chosen case-study environment. Generating predictions and recommendations was a secondary objective of this study.

The particular conceptual framework remains largely unknown and under-utilised within the IS(S) field, potentially because of its non-explicit recognition of IT and its role in the organizational encounters with risk.

Yet, the particular framework has managed to provide a structured means to connect the process of ISS management to the organizational context. The SARF has supported an analysis across both vertical and horizontal levels, while bridging risk approaches and concepts from across different disciplines.

In addition, the utilization of the IRGC's risk classification framework[283] has further complemented the SARF's classification of risks according to their signal value.

---

[281] I.e. D'Archy and Hovav, 2006; Long Li, 2006.

[282] E.g. Pattinson and Anderson, 2006; Jain, 2006; Smith et al., 2006; D'Arcy and Hovav, 2006.

[283] I.e. IRGC (2005) and Appendix-A2.

Moreover, the utilization of concepts from the discipline of organizational theory and specifically the High Reliability and Normal Accident theories has provided further focus to this research. Requirements for high reliability and mindful management have been utilised to assess the content of organizational change.

Overall, the conceptual framework utilised and proposed in the current study has facilitated the research's objective, namely to understand in-depth an organization's capacity to reliably manage ISS risks. However, a number of limitations have also been identified. Thus, the researcher suggests that the structures and situational factors of an organization and the way these interact with mechanisms of risk amplification are inadequately considered by SARF. In the current study these shortcoming were overcome by integrating into the analysis Mintzberg's (1979, 1981) scheme of organizational context levels.

Furthermore, SARF studies do not appear to investigate extensively the dynamic interactions of risks that take place simultaneously within an organization. This research has demonstrated that this is possible and in fact necessary as the amplification of one risk can affect the amplification/attenuation patterns of another.

Finally, this research has stressed the significance of risk attenuation - especially within organizations of high reliability requirements.

6.2.2. Reflections on the research methodology

In agreement with views of Walsham (1993) and Pettigrew (1990), the current study has demonstrated that a longitudinal in-depth case-study approach is indeed an appropriate methodology to observe the patterns of risk behaviours and events that dynamically unfold over a period of time. This research method has allowed the researcher to explore the context, content and process of change, along with their interconnections through time. Multiple sources and loops of causation and connectivity have been revealed with regards to the process of ISS risk management within a major-event organization.

In agreement with Pettigrew (1990:280), the utilization of the particular methodology in this research has indicated that longitudinal case-studies assist "the iterative process of inductive pattern generation and theory building". Emerging issues and lessons learned have been highlighted at the final interpretive phase of the case study (i.e. Lincoln and Guba, 1985), while "emerging conceptual and

theoretical ideas [have been] inductively derived from the case" Pettigrew (1990:280).

Case-study criticisms with regards to poor representativeness have been partly addressed by identifying lessons learned for other organizations of similar characteristics and reliable ISS requirements. Reflections were also highlighted with regards to the process and mechanisms of ISS risk amplification and reliable management. As Walsham (1993:15) suggests

> "from an interpretive position, the validity of an extrapolation from an individual case or cases depends [...] on the plausibility and cogency of the logical reasoning used in describing the results from the cases, and in drawing conclusions from them".

6.3 Epilogue

Contemporary organizations increasingly structure and deliver their strategic objectives in the form of major-events and projects. With regards to the IS infrastructures that support such organizational structures, or are the end deliverable of such efforts, the secure handling of information is of critical importance to the success of such mega-projects.

Yet, this is a field that has been inadequately investigated, despite the potential organizational, economic and socio-political benefits and the simultaneous poor performance of such structures.

The in-depth, longitudinal investigation of an ISS project within a major-event context has demonstrated that high levels of interactive complexity and operational and functional interdependence, directly or indirectly affect ISS management efforts, decisions and communications. Principles of high reliability can indeed improve overall ISS performance and management of risk, yet the structural and cultural aspects of a major event project will amplify or attenuate risk perceptions and thus constrain the effectiveness of such controls. Therefore, there is a need to improve understanding of such factors, incorporating this into risk and risk control evaluation, management and communication practices.

By sustaining mindful and reflexive processes and structures of risk communication and interpretation, ISS assurance and governance practices will allow organizations to demonstrate that they can reliably anticipate and contain ISS risks.

Appendices

A1 - Approaches to risk

	Risk Approach	Description & References
1	*Technical Risk Assessment*	Traditionally adopted in the insurance industry and focuses on the 'expected value', which can be extrapolated from the statistical data about accidents in previous years. The resulting risk assessment is reduced to a single dimension representing an average over space, time and context. The focus is on cause-effect relationships.
		Cohen, 1996; Bedford & Cooke, 2001; IAEA, 1995; Aven, 2003; Renn, 2008; Dietz et al, 1996; Zinn & Taylor-Gooby, 2006a; Perrow, 1984; Fischhoff, 1995; Slovic, 1987b; Hattis & Kennedy, 1990.
2	*Economic - Rational Actor Paradigm (RAP)*	Based on the core concept of the rational actor and his/her subjective utility functions. A risk decision is, therefore, a decision with a range of possible outcomes with known probability for the occurrence of each stage. Statistical methods can lead to the rational decision about the reduction of risk.
		Renn, 1992a; Jaeger et al, 2001 ; Renn et al, 2005 ; Renn, 2008 ; Coleman, 1990.
3	*Behavioural Economic*	Shows that people rely on a limited number of heuristic principles, which reduce the complex tasks of assessing probabilities and predicting values to simpler judgemental operations. Although these heuristics can be quite useful, they will sometimes lead to severe and systematic errors/biases, such as: the representativeness, availability and adjustment/anchoring bias. The approach also identifies the significance of 'framing'. The framing effect takes place when there is a change of preferences between options as a function of the variation of frames. This phenomenon violates the assumption that people decide by referring to objective entities. This approach also identifies the significance of *risk communication* methods. The central notion of the approach encompasses the idea that risk problems are fundamentally problems of ensuring that the right information is available and that lay people are able to use the information properly. In this view, risk problems are mainly problems of sufficient information and therefore need to be solved by the improvement of communication strategies. The approach has also identified the importance of trust, emphasizing the limitations on knowledge as the basis of trust.
		Tversky & Kahneman, 1974; Jaeger et al., 2001; Renn et al, 2005; Zinn, 2004a; Putnam, 1993; Frewer et al., 2003; Lewis & Weigert, 1985; Elsher, 1998; Sunstein, 2003.

	Risk Approach	Description & References
4	*Psychological*	Focuses on explaining why individuals do not base their risk judgements on expected values. It identifies strong biases in people's drawing inferences from probabilistic information, and has revealed different meanings of risk, depending upon the context in which the term is used. Therefore, psychological studies of risk have focused on the *perception of risk* and have indicated towards different risk connotations among individuals, groups and cultures. Risk perceptions are influenced by intuitive heuristics and judgement processes, contextual factors, semantic associations, trust and credibility.
		Slovic, 1987b, 2000; Rohrmann & Renn, 2000; Loomes, 2005, 2006; Jones-Lee et al., 1995; Slovic et al., 2000; Weyman & Kelly, 1999; Williamson & Weyman, 2005; Bostrom et al., 1992; Taylor-Gooby, 2004; Tversky & Kahneman, 1974; Pidgeon, 1998; Walker et al., 1998; Taylor-Gooby & Zinn, 2005; Epstein, 1994; Loewenstein et al., 2001, 2003; Forgas 2003; Frewer et al., 2003; Poortinga & Pidgeon, 2004;; Hsee, 200; Kemp & Maxwell, 1993.
5	*Reflexive Modernization & the 'Risk Society'*	A sociological approach to risk. The central theme is to analyse risk perception and response within the overall framework of a cultural discontinuity giving rise to a new form of modernity. Proponents of this approach argue that in the pursuit of 'goods' modern industry and society also produce 'bads', which can cross national boundaries and affect social groups indiscriminately. The outcome is a world risk society beyond the level of the risk management institutions of the nation state. The key cultural shift among the citizens of risk society is towards 'reflexivity' - individuals are conscious of their social context and their own role as actors within in.
		Beck, 1992b; Taylor-Gooby & Zinn, 2005; Boyne, 2003; Tulloch & Lupton, 2003; Bonß, 1995; Zinn, 2004b; Elliott, 2002.
6	*Systems Theory*	A sociological approach to risk which suggests that systems can produce 'objective' knowledge about the world, but each observer is imprisoned in a social system that provides constructed meaning, rationality and identity. Therefore, this approach focuses on the internal order and systemic interactions with other systems in the outside world, which have generated the necessary communication media to serve their needs. A key feature of this construction is the distinction between risk and danger. Hazards perceived as external threats to a system are called 'dangers', while hazards that pose internal, and thus manageable, threats are called 'risks'. The approach suggests that the potential for a specific phenomenon to be constructed as a risk in one system and a danger in another impedes communication between systems.
		Luhmann, 1982, 1993; Renn, 2008.
7	*Critical Theory*	A sociological theory that focuses on the exchange of arguments in a discourse setting, which leads to consensus on the basis of mutual understanding of facts, values, experiences and normative assumptions. Therefore, with regards to risks, critical theorists support that the only viable solution to overcome the inequitable distribution of risks is to create a forum for open discourse. This process of discourse must be fair, transparent and truthful.
		Habermas, 1970, 1989, 1991; Webler, 1995; Renn, 2008.

	Risk Approach	Description & References
8	*Post-Modernism*	A sociological theory that aims to provide evidence and indications for the hidden relationships between power and collective claims. Risk is not at the centre of post-modern thinking. What is seen as risks and what as benefits, and to what degree, depends upon the framing of social forces.
		Jaeger et al, 2001; Rose, 1990; Foucault, 1991.
9	*Cultural Theory of Risk*	A socio-cultural approach to risk that focuses on the context of the group that determines which hazards attention is focused on; the acceptability or risk; and the reactions to risk that are legitimized. The focus on risk does not just serve the self-protection of the individual; it can express wider socio-political interests and agendas. It, therefore, suggests that expert judgements of risk are also subject to cultural considerations.
		Douglas and Wildavsky, 1982; Weyman and Kelly, 1999; Walker et al., 1998; Macgill, 1989; Zinn, 2004b; Williamson and Weyman, 2005; Gaskell and Allum, 2001; Renn et al., 1992.
10	*Social Amplification of Risk Framework (SARF)*	A sociological approach to risk which aims to capture the complex risk experience of both individuals and social entities, while the concept of 'amplification' includes both the intensifying and attenuating processes of risk. The process of risk amplification/attenuation initiates with the risk signal which is interpreted via social interaction in order to form risk messages and hence perceptions. Such perceptions influence risk behaviour which, in turn, generate secondary consequences that extend far beyond direct harm to humans or their environment. These secondary effects can then trigger or impede demands for additional institutional responses and protective actions. The impacts may spread or 'ripple' to other parties, locations or risk arenas.
		Kasperson et al, 1988; Kasperson, 1992; Renn, 2008.

A2 - IRGC risk characteristics and their implications for risk management and communication

Knowledge Characterization	Management Strategy	Appropriate Instruments	Stakeholder Participation
1. 'Simple' risk problems	Routine-based: (tolerability/ acceptability judgement)	→ Applying 'traditional' decision-making • Risk-benefit analysis • Risk-risk trade offs	Instrumental discourse
	(risk reduction)	• Trial and error • Technical standards • Economic incentives • Education, labelling, information • Voluntary agreements	
2. Complexity-induced risk problems	Risk-informed: (risk agent and causal chain)	→ Characterizing the available evidence • Expert consensus seeking tools • Results fed into routine operation • Risk-risk trade offs	Epistemological discourse
	Robustness-focused: (risk absorbing system)	→ Improving buffer capacity of risk target through: • Additional safety factors • Redundancy and diversity in designing safety devices • Improving coping capacity • Establishing high reliability organizations	
3. Uncertainty-induced risk problems	Precaution-based: (risk agent)	→ Using hazard characteristics such as persistence, ubiquity etc. as proxies for risk estimates. Tools include: • Containment • ALARA (as low as reasonably achievable • ALARP (as low as reasonably possible) • BACT (best available control technology)	Reflective discourse
	Resilience-focused: (risk absorbing system)	→ Improving capability to cope with surprises • Diversity of means to accomplish desired benefits • Avoiding high vulnerability • Allowing for flexible responses • Preparedness for adaptation	

Knowledge Characterization	Management Strategy	Appropriate Instruments	Stakeholder Participation
4. Ambiguity-induced risk problems	Discourse-based	➔ Application of conflict resolution methods for reaching consensus or tolerance for risk evaluation results and management option selection • Integration of stakeholder involvement in reaching closure • Emphasis on communication and social discourse	Participative discourse

Source: adapted from IRGC, 2005:16.

A3 - List of research interviews

#	Date	Interviewee (organization: role)	Interview Structure & Method
1	20 May 2002	IOC: Director of Technology	Semi-structured
2	10 October, 2002	ATHOC: Quality & ISS (QIS) Section Manager	Semi-structured
3	11 October, 2002	ATHOC IT Manager	Semi-structured
4	14 October, 2002	SchlumbergerSema: ISS Risk Manager	Semi-structured
5	13 November, 2002	ATHOC: IT Manager	Semi-structured
6	15 November, 2002	ATHOC: Quality & ISS (QIS) Section Manager	Semi-structured
7	22 November, 2002	ATHOC: Office Applications & Intranet Section Manager	Semi-structured
8	22 November, 2002	IOC: Director of Technology	Structured
9	25 November, 2002	SchlumbergerSema: Games-IS Chief Integrator	Structured
10	29 November, 2002	ATHOC: Director of Games Network IS	Structured
11	29 November, 2002	SchlumbergerSema: ISS Risk Manager	Structured
12	11 December, 2002	SchlumbergerSema: ISS Risk Manager	Structured
13	14 January, 2003	IOC: Technology Director and IOC Technology Manager	Semi- structured
14	22 January, 2003	ATHOC: Games Results Manager	Semi-structured
15	22 January, 2003	SchlumbergerSema: Games Results Supervisor	Semi-structured
16	24 January, 2003	ATHOC: ISS Manager	Semi-structured
17	27 January, 2003	ATHOC: ISS Manager	Structured
18	27 January, 2003	ATHOC: Quality & ISS (QIS) Section Manager	Semi-structured
19	31 January, 2003	SchlumbergerSema: ISS Risk Manager	Semi-structured
20	4 February, 2003	ATHOC: Quality & ISS (QIS) Section Manager	Structured
21	4 February, 2003	ATHOC: ISS Manager	Structured
22	6 February, 2003	ATHOC: Quality & ISS (QIS) Section Manager	Semi-structured
23	6 February, 2003	ATHOC: ISS Manager	Semi- structured
24	10 February, 2003	ATHOC: Director of Technology (Energy, Telecoms, IT)	Structured
25	11 February, 2003	IOC: Director of Technology	Semi-structured
26	14 February, 2003	SchlumbergerSema: ISS Risk Manager	Semi-structured
27	21 February, 2003	ATHOC: ISS Manager	Semi-structured
28	21 February, 2003	SchlumbergerSema: ISS Risk Manager	Semi-structured

#	Date	Interviewee (organization: role)	Interview Structure & Method
29	27 February, 2003	SchlumbergerSema: UNIX Systems Team Expert	Structured
30	7 March, 2003	SchlumbergerSema: ISS Risk Manager	Structured
31	12 March, 2003	ATHOC: Quality and ISS (QIS) Section Manager	Structured
32	13 March, 2003	SchlumbergerSema: ISS Risk Manager	Structured
33	18 March, 2003	SchlumbergerSema: ISS Risk Manager	Structured
34	18 March, 2003	ATHOC: Manager of Games network IS	Structured
35	19 March, 2003	IOC: Technology Director	Structured
36	21 March, 2003	SchlumbergerSema: ISS Risk Manager	Structured
37	21 March, 2003	SchlumbergerSema: IS Integration Project Quality Manager	Structured
38	1 April, 2003	SchlumbergerSema: ISS Risk Manager	Structured
39	3 April, 2003	SchlumbergerSema: ISS Risk Manager	Semi-structured
40	4 April, 2003	ATHOC: ISS Manager	Semi-structured
41	8 April, 2003	SchlumbergerSema: ISS Architect/Analyst	Structured
42	9 April, 2003	SchlumbergerSema: ISS Risk Manager	Semi-structured
43	10 April, 2003	SchlumbergerSema: IS Integration Project Quality Manager	Structured
44	11 April, 2003	SchlumbergerSema: ISS Risk Manager	Semi-structured
45	16 April, 2003	SchlumbergerSema: ISS Risk Manager	Semi-structured
46	17 April, 2003	SchlumbergerSema: ISS Architect/Analyst	Semi-structured
47	5 May, 2003	SchlumbergerSema: ISS Architect/Analyst	Semi-structured
48	9 May, 2003	SchlumbergerSema: ISS Risk Manager	Structured
49	15 May, 2003	ATHOC: Quality & ISS (QIS) Section Manager	Semi-structured
50	20 May, 2003	SchlumbergerSema: ISS Risk Manager	Semi-structured
51	9 June, 2003	SchlumbergerSema: IS Operations Manager	Semi-structured
52	23 June, 2003	SchlumbergerSema: ISS Risk Analyst	Structured
53	8 July, 2003	SchlumbergerSema: Major Events Marketing VP	Structured
54	8 July, 2003	SchlumbergerSema: ISS Risk Manager	Structured
55	10 July, 2003	SchlumbergerSema: ISS Risk Analyst	Structured
56	15 July, 2003	SchlumbergerSema: W2K Systems Expert & Team Lead	Structured

#	Date	Interviewee (organization: role)	Interview Structure & Method
57	16 July, 2003	SchlumbergerSema: Unix Systems Expert & Team Lead	Structured
58	24 July,2003	SchlumbergerSema: ISS Risk Manager	Structured
59	29 August, 2003	SchlumbergerSema: ISS Risk Analyst	Semi-structured
60	4 September, 2003	SchlumbergerSema: ISS Risk Manager	Structured
61	9 September, 2003	SchlumbergerSema: Games Systems Architect	Semi-structured
62	12 September, 2003	SchlumbergerSema: ISS Risk Manager	Semi-structured
63	15 September, 2003	SchlumbergerSema: ISS Network Analyst	Semi- structured
64	15 October, 2003	SchlumbergerSema: ISS Risk Analyst	Structured
65	17 October, 2003	SchlumbergerSema: Games-IS Operations Team Manager	Structured
66	13 November, 2003	SchlumbergerSema: ISS Risk Manager	Structured
67	26 November, 2003	SchlumbergerSema: ISS Risk Manager	Structured
68	27 November, 2003	SchlumbergerSema: ISS Risk Analyst	Structured
69	27 November, 2003	SchlumbergerSema: ISS Network Architect	Structured
70	27 November, 2003	SchlumbergerSema: ISS Network Analyst	Structured
71	28 November, 2003	SchlumbergerSema: ISS Systems Analyst	Structured
72	13 January, 2004	Atos Origin: ISS Network Analyst	Structured
73	15 January, 2004	Atos Origin: (new) Games ISS Manager	Structured
74	22 January, 2004	Atos Origin: Games-IS Chief Integrator	Structured
75	2 February, 2004	Atos Origin: (new) Games ISS Manager	Structured
76	27 February, 2004	Atos Origin: ISS Network Architect	Structured
77	10 March, 2004	Atos Origin: Games-IS Chief Integrator	Semi-structured
78	19 March, 2004	Atos Origin/ KOEP: Games-IS Network Administrator	Semi-structured
79	29 March, 2004	Atos Origin: Major Events Marketing VP	Structured
80	4 April, 2004	Atos Origin: IT Helpdesk Manager	Structured
81	16 April, 2004	Atos Origin: Games ISS Risk Analyst	Structured
82	4 May, 2004	Atos Origin: Games-IS Chief Integrator	Structured
83	14 May, 2004	Atos Origin: Games ISS Manager	Structured
84	24 May, 2004	Atos Origin: Games ISS Network Analyst	Semi-structured
85	25 May, 2004	Atos Origin: Games ISS Risk Analyst	Semi-structured
86	2 June, 2004	Atos Origin: Games ISS Manager	Structured

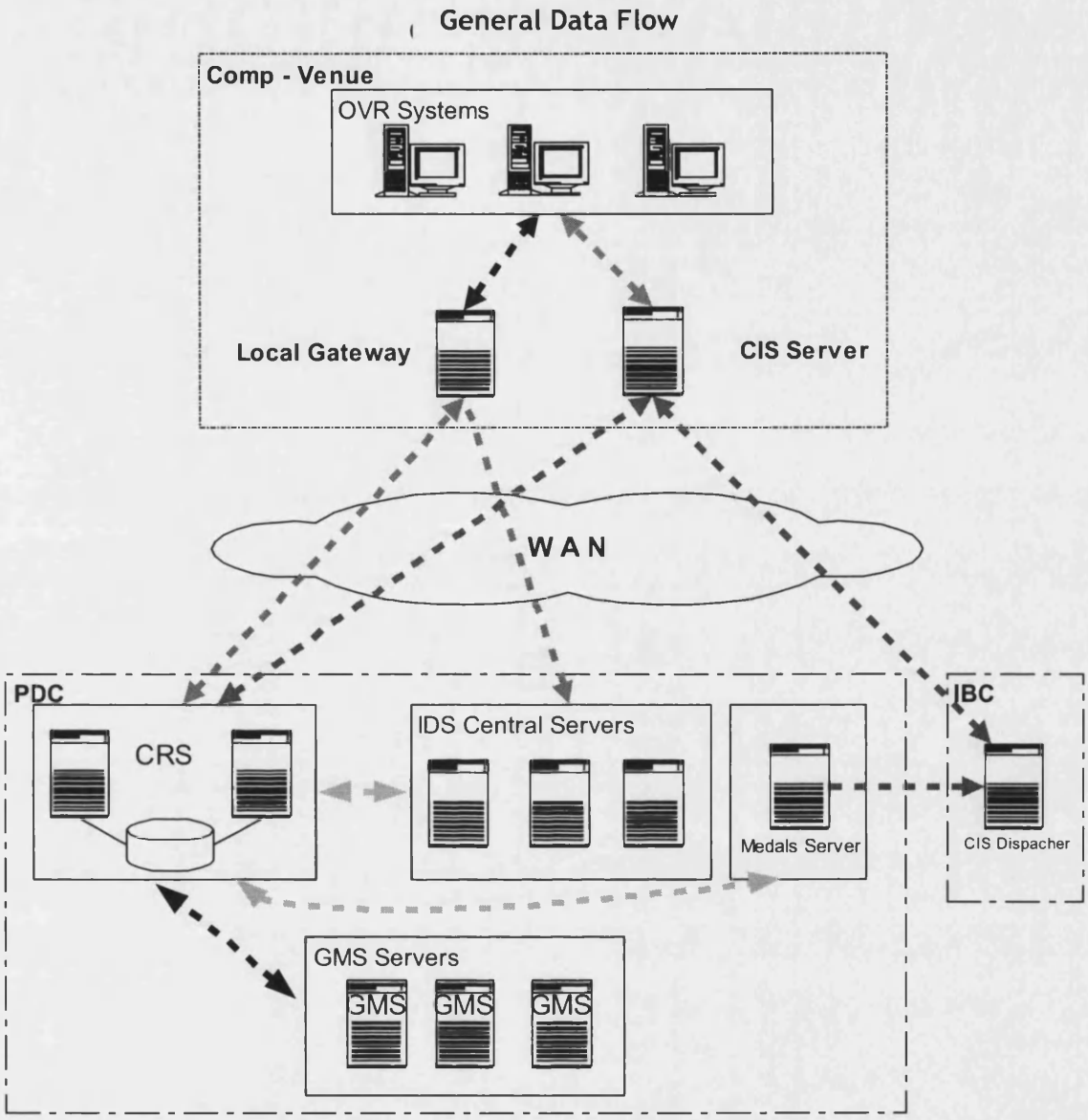
#	Date	Interviewee (organization: role)	Interview Structure & Method
87	12 June, 2004	Atos Origin: Games TRO Manager	Structured
88	24 June, 2004	Atos Origin: Games ISS Manager	Structured
89	24 June, 2004	Atos Origin:Games TRO Manager	Structured
90	22 July, 2004	Atos Origin: Games ISS Manager (TOC-SEC team#1 Duty Manager)	Structured
91	23 July, 2004	Atos Origin: Games ISS Risk Analyst (TOC-SEC team#2 ISS Incident Analyst)	Structured
92	30 July, 2004	Atos Origin: Major Events Marketing VP	Structured
93	4 August, 2004	Atos Origin: Games ISS Risk Analyst (TOC-SEC team#2 ISS Incident Analyst)	Structured
94	18 August, 2004	Atos Origin: Games ISS Risk Analyst (TOC-SEC team#2 ISS Incident Analyst)	Structured
95	9 September, 2004	Atos Origin: Games ISS Manager (TOC-SEC team#1 Duty Manager)	Structured
96	9 September, 2004	Atos Origin: Games-IS Chief Integrator (TOC IT Duty Manager)	Structured

A4 - The five services provided by the IOC's IT (TOP) sponsor for the A2004 Games-IS

	IS-Games Integration Project Service	Service Description, Mission, Challenges & Approach
1	*Partner Management*	• The coordination of IS development, deployment and operations across a number of organizations, including ATHOC, other IT sponsors, suppliers and providers, consultants and volunteers. • In A2004, partners included 10 IT sponsors and providers, the IOC and ATHOC. IT Volunteers supporting the Games-IS functionality were more than 3000 during Games-time. • Partners had to seamlessly coordinate their activities, without compromising the required quality and exceeding the budgeted resources/cost. They also had to deliver an integrated Games-IS on time. • The IT partners had no contractual relationship with one another. There was no hierarchical control. Yet common skills, policies and procedures had to be created. • The operation of the A2004 Games-IS was greatly dependent on volunteers.
2	*Systems Integration*	• The integration of people, processes and technology supporting mission-critical operations of the Games. The integrated systems serviced the IOC, ATHOC, the various suppliers, providers, media, sports and event audiences. • The integrated systems had to seamlessly support the business functions, providing reliable Games services. • The project resources had to be effectively allocated. Delays in system delivery would compromise both the project budget and end deliverable. • The A2004 mission-critical Games-IS infrastructure was great in size, comprising of 32 interfacing applications,900 servers, 10500 workstations, and 4000 printers. Network devices consisted of 200 routers, 1600 switches, 24 firewalls, and 130 intrusion detection systems. The Games IT-supported services had to be facilitated across 60 geographically dispersed venues. Integration of services had to take place across 10 IT partners, the IOC and ATHOC. The operation of the integrated Games-IS involved the role-specific training of 1000 IT personnel and 3000 IT volunteers. • According to the Games-IS Chief Integrator, "the single most important success factor is testing" (i.e. Appendix-A3:9)
3	*Change Control*	• Management of change in the Games-IS project had two aspects: (a) the exponential growth of Games -IS operations, people and technology, and (b) the tracking of defects across applications, hardware and configurations, which needed to be communicated to all appropriate parties, reaching a decision and implementing a solution within service-acceptable timeframes. • There were various organizations and functional groups that had to be involved in the change management process. Roles and responsibilities across these parties had to be defined. Managing and implementing a change implied that a baseline had been set to which all relevant parties had agreed to. • Not all changes had a home. Certain changes had to follow an escalation procedure.

	IS-Games Integration Project Service	Service Description, Mission, Challenges & Approach
4	*Information Security*	• The management of A2004 Games-ISS focused on ISS assurance, ISS architecture, and ISS operations. The evaluation of the overall ISS Posture was enabled via a combination of risk modelling and mitigation strategies. • The A2004 Games were the first ones where ISS was a strategic priority. There was limited transfer of knowledge from previous events. A2004 ISS requirements had to be defined with a number of IS partners. • ISS was a transversal activity which needed to be integrated with the rest of IT operations. However, lack of contractual hierarchy posed ISS compliance problems.
5	*Olympic Operations*	• Operations management involved five activity areas: (a) venue planning; (b) implementation; (c) central operations (e.g. helpdesk, staffing, procedures); (d) training; and (e) Games-times operations (i.e. facilities management; venue IT management, ATHOC and IT partner coordination; centralised management and monitoring from the Technology Operations Centre (TOC)). • According to the Games-IS Chief Integrator, "operational readiness is an outcome of lots and lots of testing; understanding what is normal and what is not in our environment; of training and policy and procedure awareness" (i.e. Appendix-A3:82).

A5 - A2004 Games-IS high level system architecture and data flows



Glossary:

- The *OVR* (On-Venue Results system) includes systems and data located across the different competition venues used to manage local systems such as timing or scoreboards.
- The *CIS Server* (Commentator Information System) is part of the IDS systems and provides real-time event results to producers, commentators and announcers located at the venues or at central locations such as the International Broadcasting Centre (IBC).
- *Comp-venue* refers to the 35 A2004 competition venues.

- The *CRS* (Central Repository System) is part of the IDS systems and consolidates the information regarding the Games. It receives and stores the data, as well as creates new consolidated information for the rest of the IDS applications.
- The *PDC* is the Primary Data Centre facility.
- The *IBC* is the International Broadcasting Centre facility.
- *IDS* refers to the Information Diffusion System, which gathers and distributes information related to the event to multiple clients. Among others, the information consists of the all the results, medals and records for the current and past Games.
- *GMS* refers to the Games Management System, which provides functionality to assist in gathering information about the people attending the event and their needs.

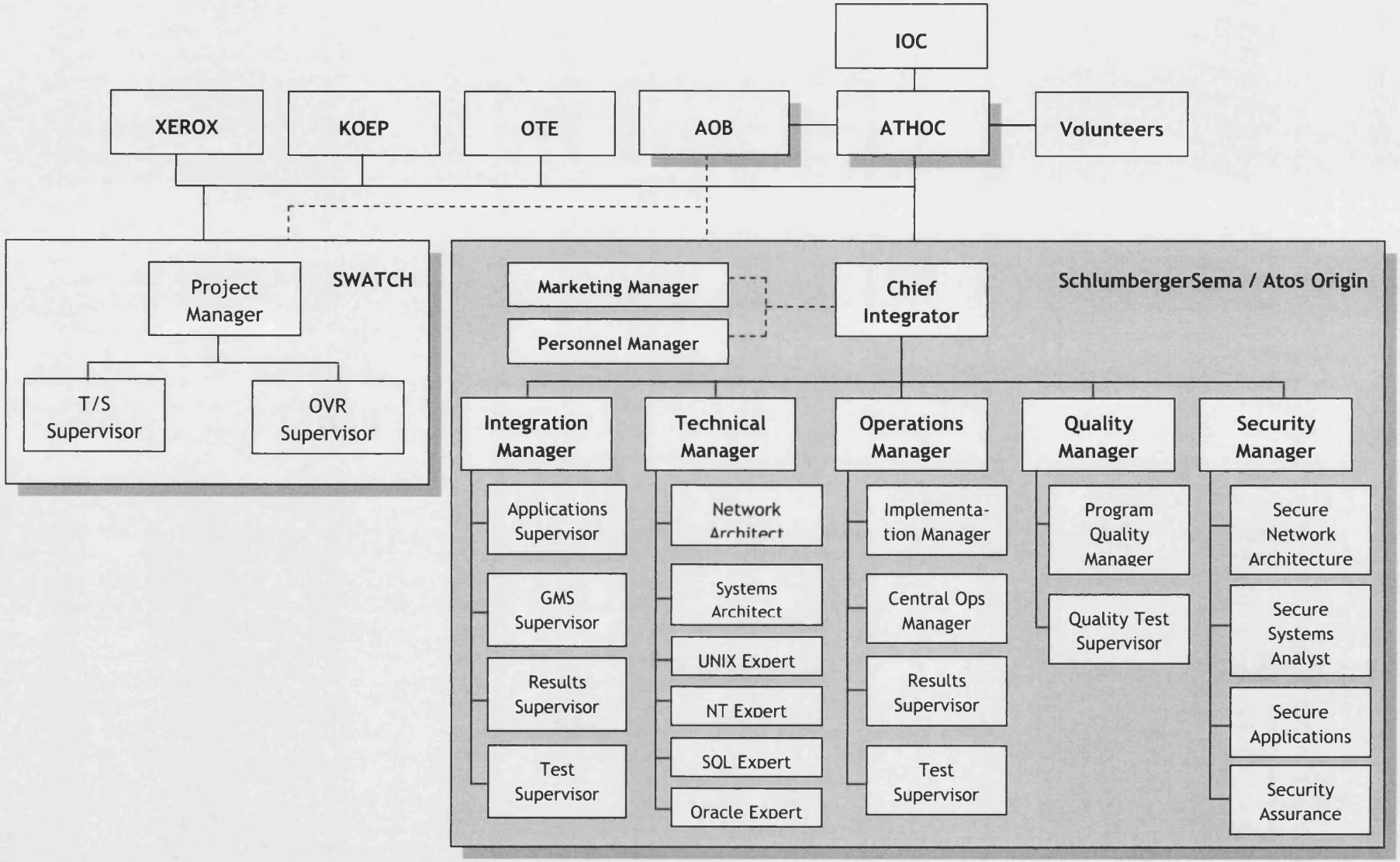
A6 - The parts of the A2004 Games-IS project organization

	Organization	Games-IS Integration Project Role, Responsibilities & Deliverables
1	IOC	The IOC located and contracted all international sponsors and TOP partners that would contribute to the A2004 Games-IS Integration project. In addition, the IOC provided the project management framework - i.e. the *Masterplan* - by which they monitored the project progress, issues and risks. Monthly meetings were organized by ATHOC, where the latter organization along with all other Games-IS project partners would present to the IOC the project development and problems.
2	ATHOC	ATHOC was overall responsible for ensuring that the project was delivered as planned and defined in the *Masterplan*. ATHOC contractually bound all other project partnering organizations, and was responsible of ensuring the smooth collaboration between the Games-IS project organization and the rest of the ATHOC functions, partners and Greek government.
3	International Sport Federations (IFs)	The 35 IFs that participated in the A2004 Games, were responsible of providing their sport event specific requirements with regards to the rules of the field of play, timing and scoring, athlete/team qualification, and broadcasting. These requirements would be incorporated into the Games-IS application build, which would then have to be tested by IF members during various sports test events.
4	Schlumberger-Sema/ Atos Origin[284]	SchlumbergerSema (or Atos Origin after January 2004) was the IOC's TOP IT partner for the A2004 Games. Its responsibilities are summarised in Appendix-A4.
5	SWATCH	SWATCH was the IOC international sponsor for the A2004 Games Timing and Scoring (T&S) system. ATHOC managed the A2004 deliverables of SWATCH. SWATCH was responsible of delivering, testing and operating the Results Systems applications, which were to be integrated with the rest of the Games-IS solutions provided by SchlumbergerSema/Atos Origin.
6	XEROX	XEROX was the IOC's international partner for document publishing, processing and supplies activities. ATHOC managed the A2004 XEROX deliverables. XEROX was responsible of printing and distributing information during Games-time, generated by the Games-IS applications. The production of accreditation badges was one of the key activities in which XEROX was involved in the Games-IS Integration project.
7	KODAK	KODAK was the IOC's international partner with regards to the production of film, photographics and imaging. Such imaging was required by a number of Games-IS applications, including the GMS accreditation application. In A2004, the KODAK contract was managed by ATHOC.

[284] The SchlumbergerSema/Atos Origin TOP contract with the IOC is historically the greatest sports- and event-IT contract of its type, covering in total 6 Olympic events, from the Salt Lake 2002 to the London 2012 Games.

	Organization	Games-IS Integration Project Role, Responsibilities & Deliverables
8	Panasonic	Panasonic, the IOC's international sponsor of audio, TV, and video equipment, provided all necessary equipment across Olympic venues, according to ATHOC's and SchlumbergerSema's venue resource requirements. During A2004, the Panasonic contract was managed by ATHOC.
9	Samsung	Samsung, the IOC's international sponsor of wireless communication equipment, provided all mobile/wireless equipment necessary the communication and coordination of Games-IS activities during the Event. The Samsung contract was managed by ATHOC in the A2004 Games.
10	OTE	OTE, the Hellenic Telecommunications Organization, was a grand national sponsor, providing the telecommunications infrastructure upon which the Games-IS operated. The OTE contract was managed and monitored by ATHOC.
11	KOEP	KOEP consisted an A2004 consortium of five Greek IT companies, which provided ATHOC with workstations, computer servers, and digital storage equipment. KOEP also sourced IT-skilled personnel for the Games-IS Integration project. KOEP contractual arrangements were made and managed by ATHOC.
12	IT Vendors	A number of IT vendors procured the Games-IS equipment and technologies. These included Dell, NetIQ, Cisco, Oracle, Sun Microsystems, CA, and others. Contracts were managed by SchlumbergerSema, and approved by ATHOC.
13	Media / Broadcasters	The Athens Olympic Broadcasting (AOB) was established as the host broadcaster of the A2004 Games, responsible of producing the International Television and Radio signal of the Games, and delivering it to the venues and the International Broadcasting Centre (IBC). AOB also provided the broadcast services and equipment to the Broadcasters. ATHOC fully funded and monitored AOB's operations. AOB members (3700), broadcasters (12000) and Games commentators (1500) had to be accredited. This was a service provided by the Games-IS GMS Accreditation application. The AOB connectivity with the Games-IS network results and information had to be coordinated with SchlumbergerSema and SWATCH.
14	Volunteers	More than 3000 IT volunteers were required during A2004 Games operations. The volunteers were recruited by ATHOC by the end of April 2004. All IT volunteers had to be trained by SchlumbergerSema/Atos Origin with regards to the Games-IS policies and procedures, their roles and responsibilities. Hundreds of IT volunteers also participated in the A2004 Games Test Events and Technical Rehearsals.

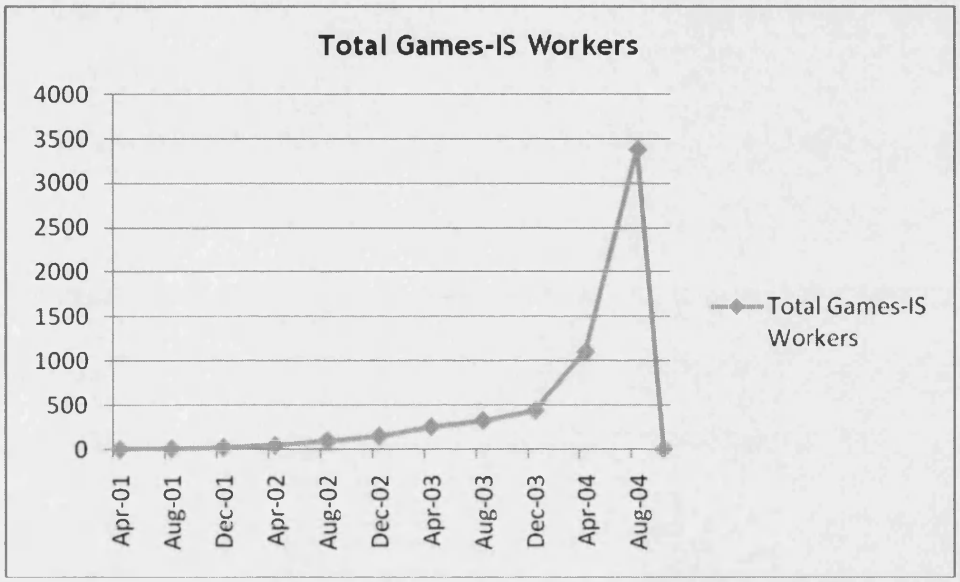
A7 - A2004 Games-IS Integration project organigram



A8 - A2004 Games-IS organization size

The Games-IS project organization consisted of a diverse organizational and cultural workforce, which expanded greatly in size during the later stages of the project. The below graphs summarize this.

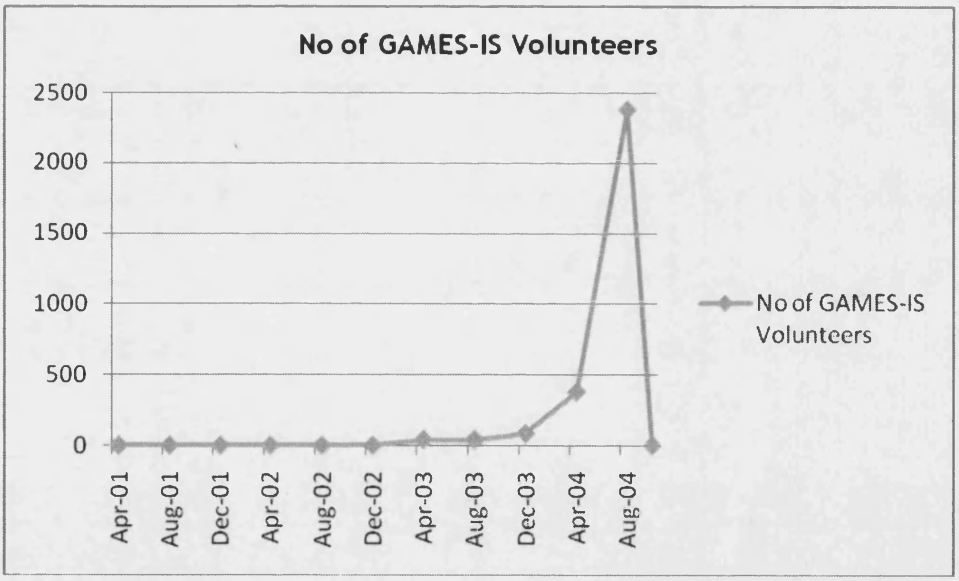
A8.1: *Total Games-IS workers*



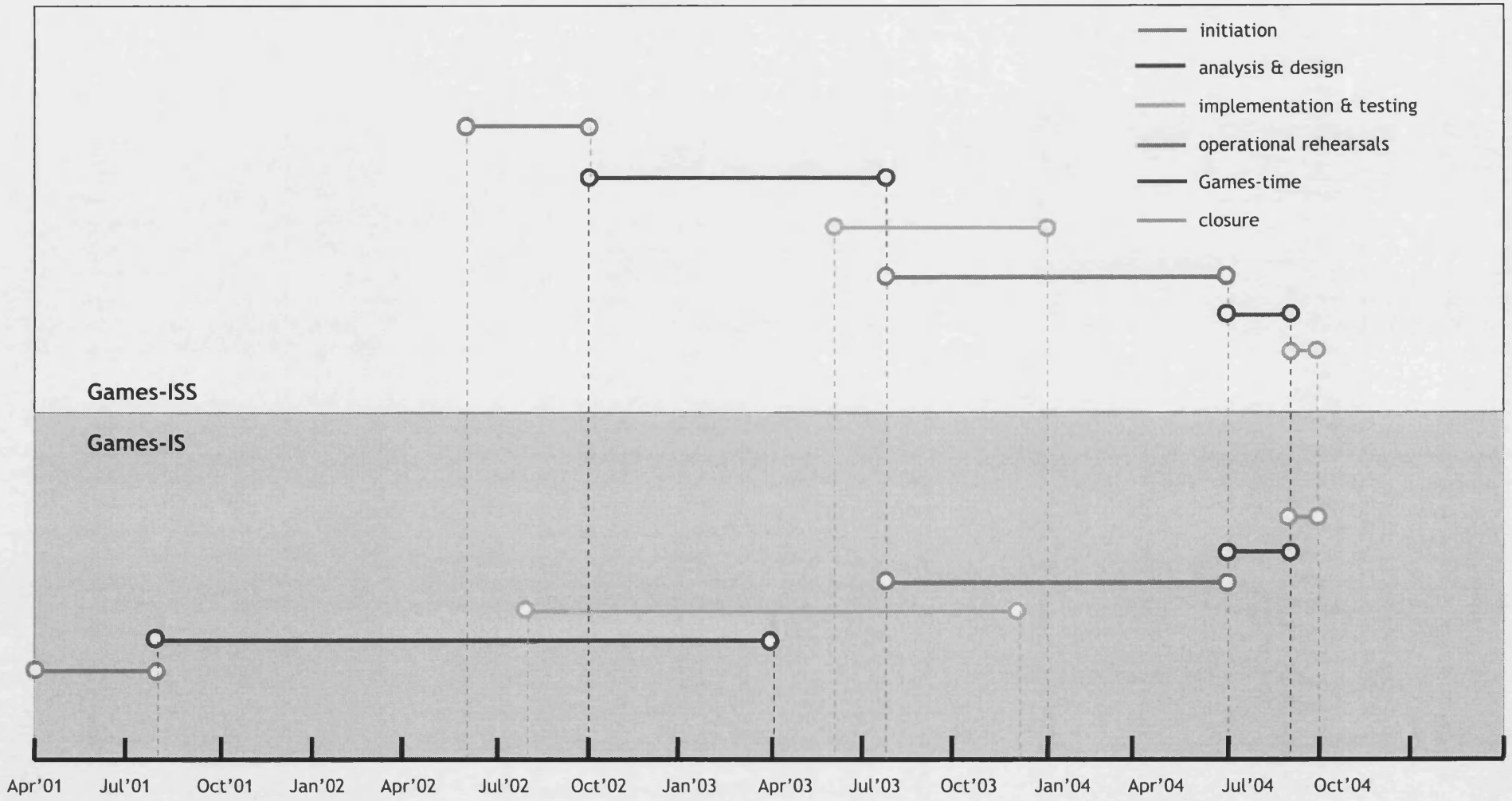
A8.2: *No of Games-IS Integrator Staff*

A8.3: *No of Games-IS Partner Staff*

A8.4: *No of Games-IS Volunteers*



A9 - A2004 Games-IS and Games-ISS project phase synchronization



A10 - Maturity of reliable ISS organizations and operations questionnaire

The following questionnaire incorporates Weick and Sutcliffe's (2001, 2007) idea that an organization's operational reliability can be monitored with the use of audit/compliance checklists or questionnaires, providing useful information with regards to levels and perceptions of high reliability across organizational units and over time.

High reliability controls - and the associated questions - are categorised into anticipation (A) and containment (C) controls, while there are three areas of control, namely organizational design, operational management, and organizational culture. These are summarised in Tables 3.3 and 3.4.

The *'Maturity of Reliable ISS Organization & Operations'* questionnaire was completed by various members of ATHOC and SchlumbergerSema across different project phases.

The questionnaire asked respondents to rate organizational ISS reliability of their work units, organizations and those of other groups/organizations. The questionnaire aimed to capture perceptions of organizational ISS reliability and operational preparedness across functional groups and over time.

The roles of the questionnaire respondents and the timing of questionnaire completion are summarised in Table A10.1 below.

Table A10.2 summarises the growth rates in the reliability of the Games-ISS management controls as assessed by the questionnaire respondents.

Questionnaire: Maturity of Reliable ISS Organization & Operations

Organization/ Organizational role: _____

Date: _____

How well do the following statements describe (the work unit/organization)?
For each item, circle the number that best reflects your conclusion:
1 = not at all (immature), 2 = to a limited extent (relatively immature),
3 = to a great extent (relatively mature), 4 = yes (mature), DK = don't know.

Organizational Design

A	1	There is a clear understanding of the application interactions, interdependencies, ISS needs and implemented controls.	1	2	3	4	DK
A	2	There is a clear understanding of the system interactions, interdependencies, ISS needs and implemented controls.	1	2	3	4	DK
A	3	There is a clear understanding of the network interactions, interdependencies, ISS needs and implemented controls.	1	2	3	4	DK
A	4	There are no unnecessary feedback loops in the network.	1	2	3	4	DK
C	5	Component redundancy is built in the IT infrastructure for all critical assets.	1	2	3	4	DK
C	6	There are no single points of failure.	1	2	3	4	DK
C	7	Resource buffers are built into the IT infrastructure.	1	2	3	4	DK
A	8	Technical IS and ISS controls are duplicated and overlap where operations are critical.	1	2	3	4	DK
C	9	Management of IT infrastructure is/can be decentralised during operational phases.	1	2	3	4	DK

Operational Management								
A	1	Management clearly communicates what the operational and ISS priorities are.	1	2	3	4	DK
A	2	There are multiple and independent channels of communication during operational phases.	1	2	3	4	DK
C	3	Key IS and ISS personnel are duplicated and overlap where operations are critical.	1	2	3	4	DK
C	4	Decision-making authority is decentralized during operational phases.	1	2	3	4	DK
A	5	Decision-making is centrally monitored during operational phases.	1	2	3	4	DK
A	6	ISS operational policies and procedures are regularly revised in order to adjust to new business requirements and operational understanding.	1	2	3	4	DK
A	7	Revised ISS operational policies and procedures are communicated to the necessary parties.	1	2	3	4	DK
C	8	IS and ISS learning is supported through a process of trial and error.	1	2	3	4	DK
C	9	Formal mechanisms are in place to enhance ISS learning from trial and error activities.	1	2	3	4	DK
A	10	There is a variety of ISS error detection and reporting mechanisms.	1	2	3	4	DK
A	11	IS and ISS personnel are encouraged to give undivided attention to operations.	1	2	3	4	DK
C	12	When ISS problems arise during operational phases, decision making migrates where expertise lies.	1	2	3	4	DK

Organizational Culture								
A	1	Management clearly communicates that operational reliability, stability and security is a top priority.	1	2	3	4	DK
A	2	Formal training and/or mentoring is provided with regards to the organizational and operational ISS priorities.	1	2	3	4	DK
A	3	Regular training and/or mentoring is provided with regards to the organizational and operational ISS priorities.	1	2	3	4	DK
A	4	ISS problems can be quickly identified and correctly labelled and assigned to the responsible party.	1	2	3	4	DK
A	5	Operational ISS policies and procedures are well communicated and understood.	1	2	3	4	DK
A	6	Structures of ISS decision-making authority are known during routine operation phases.	1	2	3	4	DK
C	7	Structures of ISS decision-making authority are known during emergency operation phases.	1	2	3	4	DK
A	8	There is no routinization during project preparation phases.	1	2	3	4	DK
A	9	There is no routinization during operational phases.	1	2	3	4	DK
A	10	Personnel are encouraged to pay close attention to signals of ISS failure.	1	2	3	4	DK
A	11	Unauthorised activity and actions that must be avoided are clearly communicated.	1	2	3	4	DK
A	12	Personnel are encouraged to question what normal system, network and people activity is.	1	2	3	4	DK
A	13	Personnel are encouraged to seek the viewpoint and expertise of other organizational groups and individuals.	1	2	3	4	DK
A	14	Inter-disciplinary and inter-departmental formal and/or informal meetings take place in order to discuss and clarify the reasons for any operational ISS deviations.	1	2	3	4	DK
C	15	IS and ISS personnel are encouraged to expand their ISS knowledge and technical facility.	1	2	3	4	DK
C	16	IS and ISS personnel are encouraged to elaborate their ISS incident response capabilities.	1	2	3	4	DK
C	17	Formal and/or informal meetings take place to discuss ways to prevent new and avoid past ISS errors in the future.	1	2	3	4	DK
A	18	There is a good understanding of each person's ISS role and responsibilities.	1	2	3	4	DK
C	19	There is a good understanding of each person's IS and ISS skills and expertise.	1	2	3	4	DK

Table A10.1: *Reliable ISS questionnaire respondents and completion periods.*

	Games-ISS Project Phase	Questionnaire Completion Date	Completed by (Organization/ Role)
1-2	Analysis & Design	4 April 2003	Assessing the Admin-network: • ATHOC: ISS Section Manager • ATHOC: ISS Manager • SLB: ISS Risk Manager Assessing the Games-network: • SLB: ISS Risk Manager • SLB: Games-IS Chief Integrator • SLB: Games-IS Technical Team Manager • SLB: Games-IS Operations Manager • SLB: IT Helpdesk Manager • SLB: Games-IS Integration Manager
		10 June 2003	Assessing the Admin-network: as above Assessing the Games-network: as above, and • SLB: Games-ISS Architect
3-4	Analysis & Design/ Implementation	4 July 2003	Assessing the Admin-network: as above Assessing the Games-network: as above, and • SLB: Games-ISS Risk Analyst
		1 August 2003	As above
5-8	Implementation / Operational Rehearsals	4 September 2003	As above
		3 October 2003	As above
		5 December 2003	As above
		29 January 2004	As above (Note: the Games-ISS Risk Manager was replaced by a new one)
9-12	Operational Rehearsals	4 March 2004	As above
		5 April 2004	As above
		4 May 2004	As above
		4 June 2004	As above
13-14	Operational: pre-Games	5 July 2004	As above
	Operational: Games-time	2 August 2004	As above
15	Closure	1 September 2004	As above

Table A10.2: *Monthly average maturity growth rate of ISS high reliability controls.*

Project period (month)	Type of ISS High Reliability Control									
	Organizational Design		Operational Management		Organizational Culture		Anticipation Controls		Containment Controls	
June'03	+	1.10	+	2.06	-	**0.79**	+	1.07	-	**0.94**
July'03	+	1.13	+	1.18	+	1.32	+	1.25	+	1.26
August'03	+	1.35	+	1.72	+	1.80	+	1.75	+	1.79
September'03	-	**0.98**	+	1.13	-	**0.99**	-	**0.96**	+	1.09
October'03	-	**0.88**	+	1.08	+	1.01	+	1.06	-	**0.95**
December'03	+	1.02	+	1.07	+	1.16	+	1.10	+	1.08
January'04	+	1.24		1.00	+	1.12	+	1.12	+	1.08
March'04		1.00	+	1.06	-	**0.99**		1.00	+	1.02
April '04	+	1.10	+	1.03	-	**0.97**	+	1.01		1.00
May '04	+	1.33		1.00		1.00	+	1.07	+	1.06
June '04	+	1.04		1.00	+	1.08	+	1.05	+	1.04
July '04	+	1.04	+	1.03	+	1.01	+	1.01	+	1.05
August '04	+	1.00	+	1.00	+	1.00	+	1.00	-	**0.99**
September'04	-	**1.00**	-	**1.00**		1.00	-	**1.00**	-	**1.00**

A11 - Games-time wrong anti-virus server configuration ISS incident

Date	Shift	TOC-SEC Team On Shift	Description of ISS Incident Management Process
15 Aug, 2004	7-19.00	TOC-SEC #2	• A competition Venue-IT team reports that: "suddenly the OVR[285] redundancy server (server B) picked up all the services, with server-A rebooting on its own. This incident occurred yesterday as well, at the exact same time, i.e. 2pm. This is the typical automated failover procedure in case of a network connectivity interruption. No ticket was opened yesterday since OVR services were not interrupted and no competition was taking place at the time. Yet, today with the occurrence of the exact same incident during competition time, the technicians at the venue are getting concerned. Can you please check your logs and investigate if during yesterday and today there was a suspicious network connectivity problem that may have caused the initiation of the OVR server failover process?"[286] • The TOC-SEC ISS Incident Analyst communicates with the TOC-NET (i.e. Games-network) team to proceed with investigations, while the issue is also investigated by the TOC-SEC ISS Administrator. No suspicious network activity is reported and the ticket is put on hold for the next TOC-SEC shift (TOC-SEC team-#3) to review in case they have any more information.
	19-7.00	TOC-SEC #3	• The new shift does not find any further information and closes the ticket without finding the cause of the problem.

[285] The OVR (On-Venue-Results) systems were located across the different competition venues and were used to manage all the local timing and scoring venue systems. These systems were jointly managed by SWATCH and Atos Origin technical personnel, and were considered highly critical for the success of the A2004 Games.

[286] This is an excerpt from the ISS ticket log as recorded on the 15th August, 2004.

Date	Shift	TOC-SEC Team On Shift	Description of ISS Incident Management Process
16 Aug, 2004	7-19.00	TOC-SEC #2	• While the Games-ISS Incident Analyst conducted a number of routine checks, she identifies that the Games systems have to be updated with new virus definitions as new viruses have been identified by the anti-virus solution provider. Conducting a check on the three Games anti-virus servers she identifies a number of problems: (a) the anti-virus server that was meant to update its definition on a daily basis has not done so in over 10 days; (b) the anti-virus server that manages all OVR devices does not have real-time definition update deactivated as was agreed at an earlier project stage[287]; and (c) several Games devices are managed by the wrong anti-virus server. • None of the TOC-SEC team-#2 members have administrative rights on the Games anti-virus servers. The required configuration changes can not take place until the TOC-SEC team-#1 is once again on shift. Thus, a severity-3 ticket is opened by the TOC-SEC team and internally assigned to the next shift. The ticket states: "the above corrections on the anti-virus servers need to be implemented ASAP. I also suspect that the still active real-time anti-virus updates on the OVR anti-virus server is what causes OVR systems at venues to fail at the same time everyday. I spoke with the Venue-IT Manager at the competition venue today, and he verified that the problem occurred today as well. During competition time such an incident could lead to the loss of data"[288].
	19-7.00	TOC-SEC #3	• No action is taken by the TOC-SEC team on shift to investigate or fix the problem. The team members do not have the adequate skills and privileges to fix the problem.
17 Aug, 2004	7-19.00	TOC-SEC #1	• The TOC-SEC team (#1) on shift overlooks the ticket and does not fix the problem.
	19-7.00	TOC-SEC #2	• A frustrated TOC-SEC team (#2) on shift identifies that the problem has still not been fixed.

[287] As identified during the 'Operational Rehearsals' phase of the A2004 Games IS(S) project (i.e. Section 4.3.4.3 and Table 4.14:18), the anti-virus definition updates impacted the performance of the OVR systems. Hence, it had been agreed that a separate anti-virus server would be set up to manage only the OVR systems. This OVR anti-virus server would update the OVR device on a daily basis, but during non-operational hours, therefore not impacting the performance of the OVR systems. Thus, the real-time anti-virus definitions update was deactivated on the OVR anti-virus server; updates were done manually off-peak hours.

[288] This is an excerpt from the ISS ticket log as recorded on the 16th August, 2004.

Date	Shift	TOC-SEC Team On Shift	Description of ISS Incident Management Process
18 Aug, 2004	7-19.00	TOC-SEC #1	• The Duty Manager and Games-ISS Incident Analyst of TOC-SEC #2 stay in the TOC after their shift has ended to ensure that proper hand-over is conducted and raise the next shift's (i.e. TOC-SEC #1) attention to the problem and the urgency of its resolution. • There is tension and the Games-ISS Incident Analyst from team-#2 openly blames her Games-ISS Incident Analyst colleague on team-#1 of unreliability and lack of professionalism. The Duty Manager on the TOC-SEC #1 downplays the significance of the ISS incident and suggests to the ISS Incident Analyst from TOC-SEC #2 that: "you are too eager and probably a bit tired too. Go home and get some rest. We will take care of this. There is no need to create trouble for all of us out of this. Nothing happened after all. Nobody needs to know about this. You don't need to tell the IT team at (the venue) what the cause of the problem was". • The TOC-SEC #1 on shift corrects the Games anti-virus configuration problems.
	19-7.00	TOC-SEC #2	• The Games-ISS Incident Analyst communicates with the Venue-IT team and verifies that the OVR system failover problem does not persist. The Venue-IT team verifies that the problem has not re-occurred. An explanation is not offered to the Venue-IT team with regards to the cause of the problem.

Bibliography

1. Alexander D (2002) *Principles of Emergency Planning and Management*, Oxford, UK: Oxford University Press.

2. Alhakami A S and P Slovic (1994) "A Psychological Study of the Inverse Relationship between Perceived Risk and Perceived Benefit", *Risk Analysis*, Vol.14 (6), pg.1085-1096.

3. Allan D (1996) *The Shape of General Hospital Nursing: The Division of Labour at Work*, PhD Thesis, Nottingham, UK: University of Nottingham.

4. Allenby B and J Fink (2005) "Toward Inherently Secure and Resilient Societies", *Science*, Vol. August.

5. Anderson J M (2003) "Why we Need a New Definition of Information Security", *Computers & Security*, Vol.22 (4), pg.308-313.

6. Arvai J L, R Gregory and T L McDaniels (2001) "Testing a Structured Decision Approach: Value-focused Thinking for Deliberative Risk Communication", *Risk Analysis*, Vol.21, pg.1065-1076.

7. Au S Y Z, M C Ryan, M S Carey, and S P Whalley (1993) *Managing Crowd Safety in Public Venues*, Health and Safety Executive, London (UK): HSE Books. Available at: http://www.hse.gov.uk/pubns/indg142.htm (last accessed: 19/03/09).

8. Ausburn L J and FB Ausburn (1978) "Cognitive Styles: Some Information and Implications for Instructional Design", *Educational Communication and Technology Journal*.

9. Aven T (2003) *Foundations of Risk Analysis: A Knowledge and Decision-Oriented Perspective*, Chichester, UK: Wiley.

10. Bagchi K and G Udo (2003) "An Analysis of the Growth of Computer and Internet Security Breaches", *Communications of the AIS*, Vol.12 (46), pg.684-700.

11. Barber B R (1984) *Strong Democracy: Participatory Politics for a New Age*, Berkeley: University of California Press.

12. Baron R M and S J Misovich (1999) "On the Relationship Between Social and Cognitive Modes of Organization", in S Chaiken and Y Trope (eds.) *Dual-Process Theories in Social Psychology*, New York, NY: Guilford Press, pg.586-605.

13. Baskerville R (1992) "The Development Duality of Information Systems Security", *Journal of Management Systems*, Vol.4 (1), pg.1-12.

14. Bauman Z (1998) *Globalization: The Human Consequences*, Cambridge, UK: Polity Press.

15. Beck U (1992a) "From Industrial Society to the Risk Society: Questions of Survival, Social Structure and Ecological Enlightenment", *Theory, Culture and Society*, Vol.9, pg.97-123.

16. Beck U (1992b) *Risk Society: Towards a New Modernity*, London, UK: Sage.

17. Bedford T and R Cooke (2001) *Probabilistic Risk Analysis: Foundations and Methods*, Cambridge, UK: Cambridge University Press.

18. Bener A B (2000) *Risk Perception, Trust and Credibility: A Case in Internet Banking*, PhD Thesis, London, UK: London School of Economics and Political Sciences.

19. Benz A and B Eberlein (1999) "The Europeanization of Regional Policies: Patterns of Multi-level Governance", *Journal of European Public Policy*, Vol.6 (2), pg.329-348.

20. Berlonghi A (1990) *The Special Event Risk Management Manual*, Dana Point, CA: Bookmasters Inc.

21. Berlonghi A (1995) "Understanding and Planning for Different Spectator Crowds", *Safety Science*, Vol.18 (4), pg.239-247.

22. Beyer J and H Trice (1982) "The Utilization Process: A Conceptual Framework and Synthesis of Empirical Findings", *Administration Science Quarterly*, Vol.27, pg.591-622.

23. Blumer H (1969) *Symbolic Interactionism: Perspective and Method*, Englewood Cliffs, NJ: Prentice Hall.

24. Bonß W (1995) *Von Risiko: Unsicherheit und Ungewißheit in der Moderne*, Hamburg, D: Hamburg Edition.

25. Bostrom A, B Fischoff, and M G Morgan (2002) "Characterizing Mental Models of Hazardous Processes: A Methodology and an Application to Radon", *Journal of Social Issues*, Vol.48 (8), pg.85-100.

26. Bowdin G A J, J Allen, W O'Toole, R Harris, and I McDonnell (2006) *Events Management*, 2nd edition, Oxford, UK: Elsevier Butterworth-Heinemann.

27. Boyne R (2003) *Risk*, Milton Keynes, UK: Open University Press.

28. Bradford G (2003) "What's Old is New Again: Training is the Information Technology Constant", *Proceedings of the 31st Annual ACM SIGUCCS Conference on User Services*, San Antonio, Texas: US, 21-24 September 2003.

29. Breakwell G M (1994) "The Echo of Power: A Framework for Social Psychological Research", *The Psychologist*, Vol.17, pg.65-72.

30. Breakwell G M and J Barnett (2003) "Social Amplification of Risk and the Layering Method", in N Pidgeon, R E Kasperson, and P Slovic (eds.) *The Social Amplification of Risk*, Cambridge (UK): Cambridge University Press.

31. Breakwell G M (2007) *The Psychology of Risk*, Cambridge (UK): Cambridge University Press.

32. Broder J F (2000) *Risk Analysis and the Security Survey*, 2nd edition, Oxford: Butterworth-Heinemann.

33. Bunderson J S and K M Sutcliffe (2003) "Comparing Alternative Conceptualizations of Functional Diversity in Management Teams: Process and Performance Effects", *Academy of Management Journal*, Vol.45, pg.875-893.

34. Bunting C, O Renn, M V Florin, and R Cantor (2007) "Introduction to the IRGC Risk Governance Framework", *John Liner Review*, Vol.21 (2), pg.7-26.

35. Burns W J, P Slovic, R E Kasperson, J X Kasperson, O Renn, and S Emani (1993) "Incorporating Structural Models into Research on the Social Amplification of Risk: Implications for Theory Construction and Decision-Making", *Risk Analysis*, Vol.13 (6). Pg.611-624.

36. Burrell G and G Morgan (1979) *Sociological Paradigms and Organizational Analysis*, London: Heinemann.

37. Carroll J S (1995) "Incident Reviews in High-Hazard Industries: Sensemaking and Learning under Ambiguity and Accountability", *Industrial and Environmental Crisis Quarterly*, Vol.9, pg.175-197.

38. Carroll J S and Perin C (1995) *Organizing and Managing for Safe Productions: New Frameworks, New Questions, New Actions*, Cambridge, MA: Sloan School of Management, MIT.

39. Cavusoglu H, B Mishra, and S Raghunathan (2004) "A Model for Evaluating IT Security Investments", *Communications of the ACM*, Vol.47 (7), pg.92-97.

40. Cavusoglu H, B Mishra, and S Raghunathan (2005) "The Value of Intrusion Detection Systems in Information Technology Security Architecture", *Information Systems Research*, Vol.16 (1), pg.28-46.

41. Chaiken S and Stangor C (1987) "Attitudes and Attitude Change", *Annual Review of Psychology*, Vol.38, pg.575-630.

42. Chappelet J L and E Bayle (2005) *Strategic and Performance Management of Olympic Sport Organizations*, Champaign, IL: Human Kinetics.

43. Checkland P (1981) *Systems Thinking, Systems Practice*, New York: Wiley & Sons.

44. Chelladurai P and A Madella (2006) *Human Resource Management in Olympic Sport Organizations*, Human Kinetics Europe Ltd.

45. Chen T M (2003) "Trends in Viruses and Worms", *The Internet Protocol Journal*, Vol.6 (3), pg.23-33.

46. Cheng A (2008) *Splitting the Second: My Wacky Business in Olympic and Sports Timing*, Bloomington, Indiana (US): AuthorHouse.

47. Ciborra C and associates (2000) *From Control to Drift: The Dynamics of Corporate Information Infrastructures*, Oxford, UK: Oxford University Press.

48. Clarke L (1992) "Context Dependency and Risk Decision Making" in L Clarke and J F Short (eds.) *Organizations, Uncertainties, and Risk*, Boulder, CO: Westview Press, pg.27-38.

49. Clarke L (1993) "The Disqualification Heuristic" in W Freudenberg and T Youn (eds.) *Research in Social Problems and Public Policy*, Vol.5, Greenwich, CT: JAI Press.

50. Clausen L (2007) "Corporate Communication Challenges: A 'Negotiated' Culture Perspective", *International Journal of Cross Cultural Management*, Vol.7 (3), pg.317-332.

51. Cohen F (1984) "Computer Viruses: Theory and Experiments", in J H Finch and E G Dougall (eds.) *Computer Security: A Global Challenge*, North-Holland: Elsevier.

52. Cohen A V (1996) "Quantitative Risk Assessment and Decision about Risk", in C Hood and D K C Jones (eds.) *Accident and Design: Contemporary Debates in Risk Management*, London, UK: UCL Press.

53. COHRE (Centre on Housing Rights and Evictions) (2007) *Fair Play for Housing Rights: Mega-Events, Olympic Games and Housing Rights*, Report, Geneva (SW): COHRE.

54. Coleman J S (1990) *Foundations of Social Theory*, Cambridge, MA: Bellknap Press

55. Conway R W, W L Maxwell, and H L Morgan (1972) *On the Implementation of Security Measures in Information Systems*, Communications of the ACM, Vol.15 (4), pg.211-220.

56. Cooke D L (2003) "A System Dynamics Analysis of the Westray Mine Disaster", *System Dynamics Review*, Vol.19, pg.139-166.

57. Cooke D L and T R Rohleder (2006) "Learning from Incidents: From Normal Accidents to High Reliability", *System Dynamics Review*, Vol.22 (3), pg.213-239.

58. Cooper C L (1999) "The Changing Psychological Contract at Work", *European Business Journal*, Vol.11 (3), pg.115-118.

59. Creswell J W (1998) *Qualitative Inquiry and Research Design: Choosing Among Five Traditions*, Thousand Oaks (CA): Sage Publications.

60. Crotty M (2003) *The Foundations of Social Research*, Wiltshire, UK: Sage Publications Ltd.

61. Crown, The (2005) *Emergency Response and Recovery*, HM Government. Available at: http://www.ukresilience.info/ccact/errpdfs/emergresponse.pdf (last accessed: 28/09/08).

62. Currie G (1999) "Resistance Around a Management Development Programme", *Management Learning*, Vol.30 (1), pg.43-61.

63. Cvetkovich G and R Löfstedt (eds.) (1999) *Social Trust and the Management of Risk*, London (UK): Earthscan.

64. D'Arcy J and A Hovav (2006) "IS Security Research: An Analysis and Integrative Framework for Future Work", *Proceedings of the 5th Annual Security Conference*, Las Vegas: US, 19-20 April 2006.

65. D'Arcy J and A Hovav (2005) "Deterring Information Systems Misuse: The Impact of Three Security Countermeasures", *Proceedings of the 4th Security Conference*, Las Vegas: US.

66. Dahl O and K Habert (1986) *Meeting Between Cultures*, Oslo: Oslo University Press.

67. Dean M (1999) *Governmentality: Power and Rule in Modern Society*, London, UK: Thousand Oaks.

68. Deming W E (1999) *Out of the Crisis*, 9th edition, Cambridge, MA: Massachusetts Institute of Technology Center for Advanced Engineering Study.

69. Denzin N K (1978) "The Methodological Implications of Symbolic Interactionism for the Study of Deviance", in A Wells (ed.) *Contemporary Social Theories*, Santa Monica, CA: Goodyear, pg.99-108.

70. Desman M B (2003) "The Ten Commandments of Information Security Awareness Training", *Security Management Practices*, Vol.11 (6), pg.39-44.

71. Dhillon G (2001) "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns", *Computers & Security*, Vol.20 (2), pg.165-172.

72. Dhillon G (2007) *Principles of Information Systems Security: Text and Cases*, Hoboken, NJ: John Wiley & Sons, Inc.

73. Dhillon G and J Backhouse (1994) "Responsibility Analysis: A Basis for Understanding Complex Managerial Situations", *International System Dynamics Conference*, University of Stirling: Scotland, 11-15 July 2004.

74. Dhillon G and J Backhouse (2000) "Information System Security Management in the New Millennium", *Communications of the ACM*, Vol.43 (7), pg.125-128.

75. Dhillon G and J Backhouse (2001) "Current Directions in IS Security Research: Towards Socio-organizational Perspectives", *Information Systems Journal*, Vol.11 (2), pg.127-153.

76. Dietz T, R S Frey, and E A Rosa (1996) "Risk, Technology, and Society", in R E Dunlap and W Michelson (eds.) *Handbook of Environmental Sociology*, Westport, CT: Greenwood Press.

77. Douglas M and Wildavsky A (1982) *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*, Berkeley (CA): University of California Press.

78. Dryzek J S (2000) *Deliberative Democracy and Beyond: Liberals, Critics, Contestations*, Oxford, UK: Oxford University Press.

79. Dutta A and R Roy (2003) "The Dynamics of Organizational Information Security", *Proceedings from the 24th International Conference on Information Systems*, pg.921-927.

80. Earle T C and G T Cvetkovich (1995) *Social Trust: Toward a Cosmopolitan Society*, Westport, CT: Praeger.

81. Edmondson A C (1999) "Psychological Safety and Learning Behaviour in Work Teams", *Administrative Science Quarterly*, Vol.44, pg.350-383.

82. Elliott A (2002) "Beck's Sociology of Risk: A Critical Assessment", *Sociology*, Vol.36 (2), pg.293-315.

83. Elster J (1998) "Emotions and Economic Theory", *Journal of Economic Literature*, Vol.36, pg.47-74.

84. Epstein S (1994) "Integration of the Cognitive and the Psychodynamic Unconscious", *American Psychologist*, Vol.49. pg. 709-724.

85. Ettredge M L and V J Richardson (2003) "Information Transfer among Internet Firms: The Case of Hacker Attacks", *Journal of Information Systems*, Vol.17 (2), pg.71-82.

86. European Commission (2001) *European Governance: A White Paper*, COM (2001): 428 final, Brussels (B): EU.

87. Fagnot I J and Stanton J M (2006) "Using Security Assessment Interviews to Predict Organizational Security Status", *Proceedings of the 5th Annual Security Conference*, Las Vegas: US, 19-20 April 2006.

88. Fang T (2003) "A Critique of Hofstede's Fifth National Culture Dimension", *International Journal of Cross Cultural Management*, Vol. 3(3), pg.347-368.

89. Filley D (1999) "Risk Homeostasis and the Futility of Protecting People from Themselves", Independence Institute, Colorado: US. Available at: http://www.i2i.org/main/article.php?article_id=602 (last accessed: 13/01/2009).

90. Fine G A (1984) "Negotiated Order and Organizational Cultures", *Annual Review of Sociology*, Vol.10, pg.239-262.

91. Finucane M L, A Alhakami, P Slovic, and S M Johnson (2000) "The Affect Heuristic in Judgements of Risks and Benefits", *Journal of Behavioural Decision Making*, Vol.13, pg.1-17.

92. Fischhoff B (1974) "Hindsight: Thinking Backward?", in *Oregon Research Institute Research Monograph*, Vol.14(1).

93. Fischhoff B (1994) "Acceptable Risk: A Conceptual Proposal", *Risk Issues in Health, Safety and Environment*, Vol.5, pg.1-18.

94. Fischhoff B (1995) "Risk Perception and Communication Unplugged", *Risk Analysis*, Vol.15 (2), pg.137-145.

95. Fischhoff B, P Slovic, S Lichtenstein, S Read, and B Combs (2000) "How Safe is Safe enough? A Psychometric Study of Attitudes toward Technological Risks and Benefits", in P Slovic (ed.) *The Perception of Risk*, London (UK): Earthscan, pg.80-103.

96. Flower L (1994) *The Construction of Negotiated Meaning: A Social Cognitive Theory of Writing*, Carbondale: Southern Illinois University Press.

97. Flynn J, R E Kasperson, H Kunreuther, and P Slovic (1997) "Redirecting the US High-Level Nuclear Waste Programme", *Environment*, Vol.39, pg.6-11, 25-30.

98. Flynn J, P Slovic, and H Kunreuther (eds.) (2001) *Risk, Media and Stigma: Understanding Public Challenges to Modern Science and Technology*, London (UK): Earthscan.

99. Flyvbjerg B, N Bruzelius, and W Rothengatter (2003) *Megaprojects and Risk: An Anatomy of Ambition*, Cambridge: Cambridge University Press.

100. Foltz C B (2000) *The Impact of Deterrent Countermeasures Upon Individual Intent to Commit Misuse: A Behavioural Approach*, PhD Thesis, Arkansas, US: University of Arkansas.

101. Forgas J (2003) "Affective Influences on Attitudes and Judgements", in R Davidson, K Scherr, and H Goldsmith (eds.) *Handbook of Affective Studies*, Oxford: Oxford University Press.

102. Foucault M (1991) "Governmentability" in G Burchell, C Gordon, and P Miller (eds.) *The Foucault Effect: Studies in Governmentability*, Chicago (IL): Chicago University Press and Harvester, pg.87-104.

103. Frame J D (2003) *Managing Risks in Organizations*, San Francisco, CA: Jossey-Bass.

104. Freudenburg W R (1988) "Perceived Risk, Real Risk: Social Science and the Art of Probabilistic Risk Assessment", *Science*, Vol.242, pg.44-49.

105. Freudenburg W R (1992) "Nothing Recedes Like Success? Risk Analysis and the Organizational Amplification of Risk", *Risk: Issues in Health and Safety*, Vol.3 (3), pg.1-35.

106. Freudenburg W R (2003) "Institutional Failure and the Organizational Amplification of Risks: The Need for a Closer Look", in N Pidgeon, R E Kasperson, and P Slovic (eds.) *The Amplification of Risk*, Cambridge (UK): Cambridge University Press, pg.102-120.

107. Frewer L, J Scholderer, and L Bredahl (2003)"Communicating about the Risks and Benefits of Genetically Modified Foods: The Mediating Role of Trust", *Risk Analysis*, Vol.23 (6), pg.1117-1133.

108. Fruin J J (1984) "Crowd Dynamics and Auditorium Management", *Auditorium News*, May 1984. Available at: http://www.crowddynamics.com/Main/Fruin%20-%20causes.htm (last accessed: 28/11/08).

109. Furnell S (2005) "Why Users Cannot Use Security", *Computers & Security*, Vol.24 (4), pg.274-279.

110. Garber M (2004) "Security Counsel", *Special Events Magazine*, Vol.23 (3), pg.61-63.

111. Gaskell G and N Allum (2001) "Sound Science, Problematic Publics? Contrasting Representations of Risk and Uncertainty", *Politeia* Vol.XV11 (63), pg.13-25.

112. Gasser M (1988) *Building a Secure Computer System*, New York: Van Nostrand Reinhold Co.

113. Geffert B T (2004) "Incorporating HIPAA Security Requirements into an Enterprise Security Program", *Information Systems Security*, Vol.13 (5), pg.21-28.

114. Gerson E (1976) "On Quality of Life", *American Sociological Review*, Vol.41, pg.793-806.

115. Getz D (1997) *Event Management and Event Tourism*, Cognizant Communication Corporation.

116. Giddens A (1984) *The Constitution of Society*, Cambridge, UK: Polity Press.

117. Gladwell M (2005) *Blink: The Power of Thinking Without Thinking*, London, UK: Penguin Books Ltd.

118. Glaesser D (2006) *Crisis Management in the Tourism Industry*, Oxford, UK: Elsevier Butterworth-Heinemann.

119. Glaser B and A Strauss (1967) *The Discovery of Grounded Theory*, New York, NY: Aldine de Gruyter.

120. Glesne C and Peshkin A (1992) *Becoming Qualitative Researchers: An Introduction*, White Plains (NY): Longman.

121. Goffman E (1963) *Stigma: Notes on the Management of Spoiled Identity*, Englewood Cliffs, NJ: Prentice Hall.

122. Goldschmidt R and O Renn (2006) *Meeting of Minds - European Citizen's Deliberation on Brain Sciences*, Final Report of the External Evaluation, Vol.5, Stuttgart (D): University of Stuttgart, Social Science Department.

123. Gopal R D and G L Sanders (1997) "Preventative and Deterrent Controls for Software Piracy", *Journal of Management Information Systems*, Vol.13 (4), pg.29-47.

124. Gordon L A and M P Loeb (2002) "The Economics of Information Security Investment", *ACM Transactions on Information and System Security*, Vol.5 (4), pg.438-457.

125. Gordon L A, M P Loeb, W Lucyshyn, and R Richardson (2005) *2005 CSI/FBI Computer Crime and Security Survey*, San Francisco, CA: Computer Security Institute.

126. Grabowski M and K H Roberts (1997) "Risk Mitigation in Large-Scale Systems: Lessons from High Reliability Organizations", *California Management Review*, Vol.39 (4), pg.152-162.

127. Gregory R, S Lichtenstein, and D G MacGregor (1993) "The Role of Past States in Determining Reference Points for Policy Decisions", *Organizational Behaviour and Human Decision Processes*, Vol.55, pg.195-206.

128. Gregory R, I Flynn, and P Slovic (1995) "Technological Stigma", *American Scientist*, Vol.83, pg.220-223.

129. Guba E G and Y S Lincoln (1994) "Competing Paradigms in Qualitative Research", in N K Denzin and Y S Lincoln (eds.) *Handbook of Qualitative Research*, Thousand Oaks: Sage Publications Ltd, pg.105-117.

130. Habermas J (1970) "Towards a Theory of Communicative Competence", *Inquiry*, Vol.13, pg.360-375.

131. Habermas J (1989) "The Public Sphere: An Encyclopaedia Article", translated by S Lennox and F Lennox, in S E Bronner and D MacKay Kellner (eds.) *Critical Theory and Society: A Reader*, London (UK): Routledge.

132. Habermas J (1991) *Communication and the Evolution of Society*, translated by T McCarthy, Cambridge (MA): Polity Press.

133. Hall E T (1959) *The Silent Language*, 2nd edition, New York, NY: Anchor Books.

134. Halliday S, K Badenhorst, and R von Solms (1996) "A Business Approach to Effective Information Technology Risk Analysis and Management", *Information Management and Computer Security*, Vol.24, pg.16-30.

135. Handmer J and E C Penning-Rowsell (1990) *Hazards and the Communication of Risk*, Aldershot (UK): Gower.

136. Harrington S J (1996) "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgements and Intentions", *MIS Quarterly*, Vol.20 (3), pg.257-278.

137. Hattis D and D Kennedy (1990) "Assessing Risks from Health Hazards: An Imperfect Science", in T S Glickman and M Gough (eds.) *Reading in Risk*, Washington DC: Resources for the Future.

138. Hatton J (2000) "Background Paper", *Proceedings of the Risk Management Workshop*, NSW Centenary of Federation Committee, Australia, 28 August 2000.

139. Heidegger M (1962) *Being and Time*, Oxford, UK: Basil Blackwell.

140. Heimer C A (1988) "Social Structure, Psychology, and the Estimation of Risk", *Annual Review of Sociology*, Vol.14, pg.491-519.

141. Heimer C A, Coleman Petty J and Culyba R J (2005) "Risk and Rules: the 'Legalization' of Medicine", in B Hutter and M Power (eds.) *Organizational Encounters with Risk*, Cambridge, UK: Cambridge University Press.

142. Heiser J G (2005) "Read at your own Risk", *Information Security*, Layer 8: September. Available at: http://searchsecurity.techtarget.com/loginMembersOnly/1,289498,sid14_gci1256914,00.html (last accessed: 19/01/2009).

143. Henwood K L and N F Pidgeon (1992) "Qualitative Research and Psychological Theorizing", *British Journal of Psychology*, Vol.83, pg.97-111.

144. Henwood K L and N F Pidgeon (2003) "Grounded Theory" in P M Camic, J E Rhodes, and L Yardly (eds.) *Qualitative Research in Psychology*, Washington, DC: American Psychological Association Press, pg.131-155.

145. Hier S P (2002) "Raves, Risks and the Ecstasy Panic", *Canadian Journal of Sociology*, Vol.27 (1), pg.33-57.

146. Hiller H H (2003) "Mega-Events, Urban Boosterism and Growth Strategies: An Analysis of the Objectives and Legitimations of the Cape Town 2004 Olympic Bid", *International Journal of Urban and Regional Research*, Vol.24 (2), pg.449-458.

147. Hirschi T (1969) *Causes of Delinquency*, Berkeley, CA: University of California Press.

148. Hollnagel E and D D Woods (2006) "Epilogue: Resilience Engineering Precepts", in E Hollnagel, D D Woods, and N Leveson (eds.) *Resilience Engineering: Concepts and Precepts*, Burlington, Vt.: Ashgate.

149. Hood C (2002) "The Risk Game and the Blame Game", *Government and Opposition*, Vol.37 (1), pg.15-37.

150. Hood C, Rothstein H, and Baldwin R (2001) *The Government of Risk*, Oxford: Oxford University Press.

151. Horlick-Jones T, J Sime, and N Pidgeon (2003) "The Social Dynamics of Environmental Risk Perception: Implications for Risk Communication Research and Practice", in N Pidgeon, R E Kasperson, and P Slovic (eds.) *The Social Amplification of Risk*, Cambridge (UK): Cambridge University Press, pg.262-285.

152. Horne J and W Manzenreiter (eds.) (2006) *Sports Mega-Events: Social Scientific Analyses of a Global Phenomenon*, London, UK: Blackwell Publishing.

153. Hovav A and D'Arcy (2003) "The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms", *Risk Management and Insurance Review*, Vol.6 (2), pg.97-121.

154. Hsee C (2000) "Attribute Evaluability: Its Implications for Joint-Separate Evaluations and Beyond", in D Kahneman and A Tversky (eds.) *Choices, Values and Frames*, Cambridge: Cambridge University Press.

155. Huszar P (1998) "Overestimated Benefits and Underestimated Costs: The Case of the Paraguay-Parana Navigation Study", *Impact Assessment and Project Appraisal*, Vol.16 (4), pg.295-304.

156. Hutter B M (2005) "'Ways of Seeing': Understandings of Risk in Organizational Settings", in B Hutter and M Power (eds.) *Organizational Encounters with Risk*, Cambridge, UK: Cambridge University Press.

157. Hutter B M & M Power (eds.) (2005) *Organizational Encounters with Risk*, Cambridge: Cambridge University Press.

158. Hutter B M & M Power (2005b) "Organizational Encounters with Risk: An Introduction", in B Hutter and M Power (eds.) *Organizational Encounters with Risk*, Cambridge, UK: Cambridge University Press.

159. IAEA (International Atomic Energy Agency) (1995) *Guidelines for Integrated Risk Assessment and Management in Large Industrial Areas*, Technical Document, IAEA-TECDOC PGVI-CIJV, Vienna, Austria: IAEA.

160. IFEA (International Festivals and Events Association) (2005) *Overview*, IFEA. Available at: http://www.ifea.com/about_ifea_main.htm (last accessed: 19/03/2009).

161. International Olympic Committee (IOC) (2007) *Olympic Charter*, Lausanne: IOC. Available at: http://multimedia.olympic.org/pdf/en_report_122.pdf (last accessed: 19/06/09).

162. Inglehart R (1988) "The Renaissance of Political Culture", *American Political Science Review*, Vol.82 (December), pg.1203-1230.

163. Irakleous I, S M Furnell, P S Dowland, and M Papadaki (2002) "An Experimental Comparison of Secret-Based User Authentication Technologies", *Information Management & Computer Security*, Vol.10 (3), pg.100-108.

164. IRGC (International Risk Governance Council) (2005) *Risk Governance - Towards an Integrative Approach*, White Paper No.1, Geneva (SW): IRGC. Available at: http://www.irgc.org/IMG/pdf/IRGC_WP_No_1_Risk_Governance__reprinted_version_.pdf (last accessed: 09/02/2009).

165. IRGC (International Risk Governance Council) (2007) *An Introduction to the IRGC Risk Governance Framework*, Policy Brief, Geneva (SW): IRGC. Available at: http://www.irgc.org/IMG/pdf/An_introduction_to_the_IRGC_Risk_Governance_Framework.pdf (last accessed: 09/02/2009).

166. ISO/IEC 17799 (2000) Information Technology - Code of Practice for Information Security Management.

167. Jaeger C, O Renn, E A Rosa, and T Webler (2001) *Risk, Uncertainty, and Rational Action*, London, UK: Earthscan Publications Ltd.

168. Jain A (2006) "An Exploratory Assessment of Security Principles & Practices: An Insight from a Financial Services company", *Proceedings of the 5th Annual Security Conference*, Las Vegas: US, 19-20 April 2006.

169. Jandt F E (1998) *Intercultural Communication: An Introduction*, 2nd edition, Thousand Oaks, CA: Sage Publications.

170. Jasanoff S (2004) "Ordering Knowledge, Ordering Society", in S Jasanoff (ed.) *States of Knowledge: The Co-production of Science and Social Order*, London (UK): Routledge, pg.13-45.

171. Jasanoff S (2005) "Restoring Reason: Causal Narratives and Political Culture" in B Hutter and M Power (eds.) *Organizational Encounters with Risk*, Cambridge, UK: Cambridge University Press.

172. Johnson B B and V T Covello (eds.) (1987) *The Social and Cultural Construction of Risk*, Dordrecht: Reidel.

173. Jones A and D Ashenden (2005) *Risk Management for Computer Security*, Oxford: Elsevier Inc.

174. Jones-Lee M, G Loomes, and A Robinson (1995) "Why Did Two Theoretically Equivalent Methods Produce Two Very Different Values?", in N Schwab and M Saguel (eds.) *Contingent Valuation, Transport Safety and the Value of Life*, Boston, US: Kluwer Publications.

175. Joyce P (2001) "Governmentality and Risk: Setting Priorities in the New NHS", *Sociology of Health and Illness*, Vol.23 (5), pg.594-614.

176. Kahneman D and A Tversky (1973) "On the Psychology of Prediction", *Psychological Review*, Vol.80, pg.237-251.

177. Kahneman D and A Tversky (1979) "Prospect Theory: An Analysis of Decision under Risk", *Econometrica*, Vol.47, pg.263-291.

178. Kahneman D, P Slovic, and A Tversky (eds.) (1982) *Judgement under Uncertainty: Heuristics and Biases*, New York, NY: Cambridge University Press.

179. Kankanhalli A, T Hock-Hai, B C Y Tan, and K K Wei (2003) "An Integrative Study of Information Systems Security Effectiveness", *International Journal of Information Management*, Vol.23 (2), pg.139-154.

180. Kasperson J X, R E Kasperson, N Pidgeon, P Slovic (2003) "The Social Amplification of Risk: Assessing Fifteen Years of Research and Theory", in N Pidgeon, R Kasperson and P Slovic (eds.) *The Social Amplification of Risk*, Cambridge: Cambridge University Press.

181. Kasperson J X, R E Kasperson, B J Perkins, O Renn and A L White (2005) "Media Risk Signals and the Proposed Yucca Mountain Nuclear Waste Repository, 1985-1989", in J X Kasperson and R E Kasperson (eds.) *The Social Contours of Risk - Volume 1*, London (UK): Earthscan, pg.133-160.

182. Kasperson R E (1992) "The Social Amplification of Risk: Progress in Developing an Integrative Framework of Risk", in S Krimsky and D Golding (eds.) *Social Theories of Risk*, Westport (CT): Praeger, pg.153-178.

183. Kasperson R E (2000) "Siting Hazardous Facilities: Searching for Effective Institutions and Processes", in S Lesberal, Hayden, and Shaw D (eds.) *Challenges and Issues in Facility Siting: Conference Proceedings*, Columbia University Press.

184. Kasperson R E (2003) "Risk and the Stakeholder Express", in J X Kasperson and R E Kasperson (eds.) *The Social Contours of Risk - Volume 1: Publics, Risk Communication and the Social Amplification of Risk*, London (UK): Earthscan, pg.95-96.

185. Kasperson R E (2005a) "Acceptability of Human Risk" in J X Kasperson and R E Kasperson (eds.) *The Social Contours of Risk: Volume II. Risk Analysis, Corporations and the Globalization of Risk*, London (UK): Earthscan, pg.19-28.

186. Kasperson R E (2005b) "Six Propositions on Public Participation and their Relevance for Risk Communication" in J X Kasperson and R E Kasperson (eds.) *The Social Contours of Risk: Volume I. Risk Communication and the Social Amplification of Risk*, London (UK): Earthscan, pg.19-28.

187. Kasperson R E and J X Kasperson (1991) "Hidden Hazards", in D C Mayo and R Hollander (eds.) *Acceptable Evidence: Science and Values in Hazard Management*, Oxford (UK): Oxford University Press, pg.9-28.

188. Kasperson R E and J X Kasperson (1996) "The Social Amplification and Attenuation of Risk", *The Annals of the American Academy of Political and Social Science*, Vol.545, pg.95-105.

189. Kasperson R E and I Palmund (1989) "Evaluating Risk Communication", in V Covello, D McCallum, and M Pavlova (eds.) *Effective Risk Communication: The Role and Responsibility of Government and Nongovernment Organization*, New York: Kluwer Academic/Plenum Press.

190. Kasperson R E, N Jhaveri, and J X Kasperson (2001) "Stigma and the Social Amplification of Risk: Towards a Framework of Analysis", in J Flynn, P Slovic, and H Kunreuther (eds.) *Risk, Media and Stigma: Understanding Public Challenges to Modern Science and Technology*, London (UK): Earthscan, pg.9-27.

191. Kasperson R E, D Golding, and J X Kasperson (1999) "Risk, Trust and Democratic Theory", in G Cvetkovich and R Löfstedt (eds.) *Social Trust and the Management of Risk*, London (UK): Earthscan, pg.22-44.

192. Kasperson R E, D Golding, and S Tuler (1992) "Social Distrust as a Factor in Siting Hazardous Facilities and Communicating Risks", *Journal of Social Issues*, Vol.48, pg.161-187.

193. Kasperson R E, O Renn, P Slovic, H S Brown, J Emel, R Goble, J X Kasperson, S Ratick (1988) "The Social Amplification of Risk: A Conceptual Framework", *Risk Analysis*, Vol.8, pg.177-187.

194. Kasperson R E, J Emel, R Goble, C Hohenemser, J X Kasperson and O Renn (1987) "Radioactive Wastes and the Social Amplification of Risk, in R G Post (ed.) *Waste Management '87 - Volume 2, High-Level Waste*, Tuscon: Arizona Board of Regents, University of Arizona, pg.85-90.

195. Kelly P (2001) "Youth at Risk", *Discourse*, Vol.22 (1), pg.23-33.

196. Kemp M and C Maxwell (1993) "Exploring a Budget Context for Contingent Evaluation", in J Hauseman (ed.) *Contingent Valuation: a Critical Assessment*, Amsterdam: North-Holland Publishing Co.

197. Kendrick T (2003) *Identifying and Managing Project Risk*, New York, NY (US): AMACOM.

198. Kennedy K (2006) *Data Leakage: A Real Business Continuity Issue*. Available at: http://www.continuitycentral.com/feature0361.htm (last accessed: 21/03/2009).

199. Khan M H and K S Jomo (2000) *Rents, Rent-Seeking and Economic Development: Theory and Evidence in Asia*, Cambridge, UK: Cambridge University Press.

200. Kling R (1987) "Defining the Boundaries of Computing Across Complex Organizations", in R Boland and R Hirschheim (eds.) *Critical Issues in Information Systems Research*, New York: Wiley.

201. Kling R and W Scacchi (1982) "The Web of Computing: Computer Technology as Social Organization", *Advances in Computers*, Vol.21, pg.1-90.

202. Klinke A and O Renn (2006) "Systemic Risks as Challenge for Policy Making in Risk Governance", *Forum: Qualitative Social Research*, Vol.7 (1). Available at: http://www.qualitative-research.net/index.php/fqs/article/view/64/131 (last accessed: 19/01/2009).

203. Kotler P, J Bowen, J Makens (1996) *Marketing for Hospitality and Tourism*, 2nd edition, Englewood Cliffs, NJ: Prentice Hall.

204. Kunreuther H and G Heal (2005) "Interdependencies within an Organization", in B Hutter and M Power (eds.) *Organizational Encounters with Risk*, Cambridge: Cambridge University Press.

205. La Porte T R (1982) "On the Design and Management of Nearly Error-Free Organizational Control Systems", in D L Sills, C P Wolf, and V B Shelanski (eds.) *Accident at Three Mile End: The Human Dimension*, Boulder, CO: Westview Press.

206. La Porte T R (1988) "The United States Air Traffic System: Increasing Reliability in the Midst of Rapid Growth", in R Mayntz and T P Hughes (eds.) *The Development of Large Technical Systems*, Boulder, CO: Westview Press.

207. La Porte T R (1994) "A Strawman Speaks Up", *Journal of Contingency and Crisis Management*, Vol.4, pg.60-72.

208. La Porte T R and P M Consolini (1991) "Working in Practice but not in Theory: Theoretical Challenges of 'High Reliability Organizations'", *Journal of Public Administration Research and Theory*, Vol.1, pg.19-47.

209. Laswell H (1948) *The Structure and Function of Communication and Society: The Communication of Ideas*, New York: Institute for Religious and Social Studies, pg.203-243.

210. Lee S M, S G Lee, and S Yoo (2004) "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories", *Information and Management*, Vol.41 (6), pg.707-718.

211. Leiss W (1996) "Three Phases in Risk Communication Practice" in H Kunreuther and P Slovic (eds.) *Annals of the American Academy of Political and Social Science, Special Issue: Challenges in Risk Assessment and Risk Management*, Thousand Oaks (CA): Sage, pg.85-94.

212. Levitt R E (1975) "The Effect of Top Management on Safety in Construction", PhD thesis, Department of Civil Engineering, Stanford University.

213. Lewis J P (1997) *Fundamentals of Project Management*, New York, NY (US): AMACOM.

214. Lewis D and A Weigert (1985) "Holism and Trust", *Sociological Quarterly*, Vol.26 (4), pg.455-471.

215. Li Long (2006) "An Institutional Analysis on Confidentiality in Health Information Systems", *Proceedings of the 5th Annual Security Conference*, Las Vegas: US, 19-20 April 2006.

216. Lichtenstein S (1996) "Factors in the Selection of a Risk Assessment Method", *Information Management and Computer Security*, Vol.4 (4), pg.20-25.

217. Liebenberg A and R Hoyt (2003) "The Determinants of Enterprise Risk Management: Evidence from the Appointments of Chief Risk Officers", *Risk Management & Insurance Review*, Vol.6 (February), pg.37-52.

218. Lincoln Y S and Guba E G (1985) *Naturalistic Inquiry*, Beverly Hills (CA): Sage Publications.

219. Lippa R A (1994) *Introduction to Social Psychology*, 2nd edition, Belmont, CA: Wadsworth.

220. Loewestein G and J Lerner (2003) "The Role of Affect in Decision-Making", in R Davidson, K Scherr, and H Goldsmith (eds.) *Handbook of Affective Studies*, Oxford: Oxford University Press.

221. Loewestein G, E Weber, C Hsee, and N Welch (2001) "Risks as Feelings", *Psychological Bulletin*, Vol.127 (2), pg.267-286.

222. Löfstedt R E (2003) "Risk Communication: Pitfalls and Promises", *European Review*, Vol.11 (3), pg.417-435.

223. Löfstedt R E (2005) *Risk Management in Post-Trust Societies*, New York (NY): Palgrave MacMillan.

224. Loomes G (2006) "(How) Can We Value Health, Safety and the Environment?", *Journal of Economic Psychology*, Vol.27, pg.713-736.

225. Lou, D and J Liu (2002) "Stenographic Method for Secure Communications", *Computers & Security*, Vol.21 (5), pg.449-460.

226. Luhmann N (1979) *Trust and Power: Two Works by Niklas Luhmann*, Chichester (UK): Wiley.

227. Luhmann N (1982) "The World Society as a Social System", *International Journal of General Systems*, Vol.8, pg.131-138.

228. Luhmann N (1993) *Risk: A Sociological Theory*, translated by R Barrett, New York (NY): Aldine de Gruyter.

229. Lupton D (1999) *Risk*, London, UK: Routledge.

230. Lyall C and J Tait (2004) "Shifting Policy Debates and the Implications for Governance" in C Lyall and J Tait (eds.) *New Modes of Governance: Developing an Integrated Policy Approach to Science, Technology, Risk and the Environment*, Aldershot (UK): Ashgate, pg.3-17.

231. MacGill S (1989) "Risk Perception and the Public: Insights from Research around Sellafield", in J Brown (ed.) *Environmental Threats: Perception, Analysis and Management*, London, UK: Belhaven Press.

232. MacGregor D G (2003) "Public Response to Y2K: Social Amplification and Risk Adaptation: or, "How I Learned to Stop Worrying and Love Y2K"", in N Pidgeon, R E Kasperson, and P Slovic (eds.) *The Social Amplification of Risk*, Cambridge, UK: Cambridge University Press, pg.243-261).

233. Machlis G E and E A Rosa (1990) "Desired Risk: Broadening the Social Amplification of Risk Framework", *Risk Analysis*, Vol.10 (1), pg.161-168.

234. Magklaras G B and S M Furnell (2005) "A Preliminary Model of End User Sophistication for Insider Threat Prediction in IT Systems", *Computer & Security*, Vol.24 (5), pg.371-380.

235. Maines D R (1977) "Social Organization and Social Structure in Symbolic Interactionist Thought", *Annual Review of Sociology*, Vol.3, pg.235-259.

236. Major Projects Association (1994) *Beyond 2000: A Source Book for Major Projects*, Oxford, UK: Major Projects Association.

237. March J G (1981) "Decisions in Organizations and Theories of Choice", in A H Van de Ven and W F Joyce (eds.) *Perspectives on Organization Design and Behaviour*, New York, NY: John Wiley.

238. March J G and J P Olsen (1988) "The Uncertainty of the Past: Organizational Learning under Ambiguity", in J March (ed.) *Decisions and Organizations*, Oxford , UK: Basil Blackwell.

239. Marcus A (1995) "Managing with Danger", *Industrial Environment Crisis Quarterly*, Vol.9, pg.139-151.

240. Mares D R and W W Powell (1990) "Cooperative Security Regimes" in R L Kahn and M N Zald (eds.) *Organizations and Nation States: New Perspectives on Conflict and Cooperation*, San Francisco: Jossey-Bass.

241. Marone J G and E J Woodhouse (1986) *Averting Catastrophe: Strategies for Regulating Risky Technologies*, Berkeley: University of California Press.

242. Masterman G (2004) *Strategic Sports Event Management: An International Approach*, Oxford, UK: Elsevier Butterworth-Heinemann.

243. Masterman G (2009) *Strategic Sports Event Management: Olympic Edition*, 2nd edition, Oxford, UK: Elsevier Butterworth-Heinemann.

244. Mazur A (1981) *The Dynamics of Technical Controversy*, Washington, DC: Communication Press.

245. McNeil B J, S G Pauker, H C Sox Jr, and A Tversky (1982) "On the Elicitation of Preferences for Alternative Therapies", *New England Journal of Medicine*, Vol.306 (21), pg.1259-1262.

246. Mead G H (1934) *Mind, Self and Society*, Chicago: Chicago University Press.

247. Mellor M and D Noyes (2006) "Awareness and Accountability in Information Security Training", *Proceedings of the 5th Annual Security Conference*, Las Vegas: US, 19-20 April 2006.

248. Merkhofer M W (1984) "Comparative Analysis of Formal Decision-Making Approaches" in V T Covello, J Menkes and J Mumpower (eds.) *Risk Evaluation and Management*, New York (NY): Plenum, pg.183-220.

249. Merleau-Ponty (1962) *Phenomenology of Perception*, London, UK: Routledge and Kegan Paul.

250. Merrow E W (1988) *Understanding the Outcomes of Megaprojects: A Quantitative Analysis of Very Large Civilian Projects (RAND Report)* Santa Monica: CA, RAND Corporation.

251. Meyerson D and J Martin (1987) "Cultural Change: An Integration of Three Different Views", *Journal of Management Studies*, Vol.24, pg.623-647.

252. Miller D (1993) "The Architecture of Simplicity", *Academy of Management Review*, Vol.18, pg.116-138.

253. Millstone E P, P van Zwanenberg, C Marris, L Levidow, and H Torgersen (2004) *Science in Trade Disputes Related to Potential Risks: Comparative Case Studies*, Seville (ES): Institute for Prospective Technological Studies.

254. Mintzberg H (1978) "Patterns in Strategy Formulation", *Management Science*, Vol.24 (9), pg.934-948.

255. Mintzberg H (1979) *The Structuring of Organizations*, London, UK: Prentice Hall International.

256. Mintzberg H (1981) "Organizational Design, Fashion or Fit?", *Harvard Business Review*, Vol.59 (1), pg.103.

257. Mintzberg H (1994) *The Rise and Fall of Strategic Planning*, London, UK: Prentice Hall.

258. Mishra S and M A Harris (2006) "Human Behavioural Aspects in Information Systems Security", *Proceedings of the 5th Annual Security Conference*, Las Vegas: US, 19-20 April 2006.

259. Monks JC (1996) *Shaum's Outline of Theory and Problems of Operations Management*, New York, NY (US):McGraw-Hill.

260. Morgan G (1986) *Images of Organization*, Beverly Hills, CA: Sage Publications.

261. Morgan M G, B Fischhoff, A Bostrom, L Lave, and C Atman (1992) "Communicating Risk to the Public", *Environmental Science and Technology*, Vol.26 (11), pg.2049-2056.

262. Morris P and G H Hough (1987) *The Anatomy of Major Projects: A Study of the Reality of Project Management*, New York, NY: John Wiley and Sons.

263. Moscaritolo A (2009) "Despite Downturn, IT Security Spending to Increase", *SC Magazine*, April 2009. Available at: http://www.scmagazineus.com/despite-downturn-it-security-spending-to-increase/article/130550/ (last accessed: 19/05/2009).

264. National Institute for Standards and Technology (NIST) (1998) *Information Technology Security Training Requirements (SP 800-16)*, Washington DC. Available at: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (last accessed: 19/01/2009).

265. National Institute for Standards and Technology (NIST) (2000) *Federal Information Technology Security Assessment Framework*, Washington DC. Available at: http://csrc.nist.gov/drivers/documents/Federal-IT-Security-Assessment-Framework.pdf (last accessed: 19/01/2009).

266. National Institute for Standards and Technology (NIST) (2002) *Risk Management Guide for Information Technology Systems.* Available at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (last accessed: 19/01/2009).

267. OECD (Organization for Economic Co-operation and Development) (2002) *Guidance Document on Risk Communication for Chemical Risk Management*, Series on Risk Management, No.16, Paris (FR): Environment, Health and Safety Publications.

268. OECD (Organization for Economic Co-operation and Development) (2003) *Emerging Systemic Risks in the 21st Century: An Agenda for Action*, Final Report on the OECD Futures Projects, Paris (FR): OECD.

269. Osborn S, S Ravi and M Qamar (2000) "Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies", *ACM Transactions on Information and System Security*, Vol.3(2), pg.85-106.

270. O'Toole W (2006) *Event Project Management System.* Available at: http://www-personal.usyd.edu.au/~wotoole/epmspage1.html (last accessed: 13/03/2009).

271. Otway H J (1980) "Risk Perception: A Psychological Perspective", in M Dierkes, S Edwards and R Coppock (eds.) *Technological Risk: Its Perspective and Handling in Europe*, Gunn and Hain: US.

272. Palmer C G S, L K Carlstrom, and J A Woodward (2001) "Risk Perception and Ethnicity", *Risk Decision and Policy*, Vol.6, pg.187-206.

273. Panko R R (2003) "Slammer: The First Blitz Worm", *Communications of the AIS*, Vol.11 (12), pg.207-218.

274. Paquet G (2001) "The New Governance, Subsidiarity, and the Strategic State" in OECD (ed.) *Governance in the 21st Century*, Paris (FR): OECD, pg.183-215.

275. Parker D (1998) *Fighting Computer Crime: A New Framework for Protecting Information*, New York, NY: John Wiley and Sons.

276. Patriotta G (2003) *Organizational Knowledge in the Making*, New York, NY: Oxford University Press.

277. Pattinson M R and G Anderson (2005) "Risk Communication, Risk Perception, and Information Security", *Proceedings of IFIP WG11.1 & WG11.5 Working Conference*, Fairfax, Virginia: US, 1-2 December 2005.

278. Pattinson M R and G Anderson (2006a) "Information Risk Management: Some Social-psychological Issues", *Proceedings of the 5th Annual Security Conference*, Las Vegas: US, 19-20 April 2006.

279. Pattinson M R and G Anderson (2006b) "Risk Homeostasis as a Factor of Information Security", *Proceedings of the 5th Annual Security Conference*, Las Vegas: US, 19-20 April 2006.

280. Pattinson M R and G Anderson (2007) "How well are information risks being communicated to your computer end-users?", *Information Management and Computer Security*, Vol.15 (5), pg.362-371.

281. Payne C (2002) "On the Security of Open Source Software", *Information Systems Journal*, Vol.12 (1), pg.61-78.

282. Perin C (2006) *Shouldering Risks: The Culture of Control in the Nuclear Power Industry*, Princeton, NJ: Princeton University Press.

283. Perrow C (1983) "The Organizational Context of Human Factors Engineering", *Administrative Science Quarterly*, Vol.28 (4).

284. Perrow C (1984) *Normal Accidents: Living with High Risk Technologies*, New York, NY: Basic Books.

285. Perrow C (1992) "Accidents in High Risk Systems", *Technology Studies*, Vol.1 (1).

286. Peters E and P Slovic (1996) "The Role of Affect and Worldviews as Orienting Dispositions in the Perception and Acceptance of Nuclear Power", *Journal of Applied Social Psychology*, Vol.26 (16), pg.1427-1453.

287. Pettigrew A M (1985) *The Awakening Giant*, Oxford, UK: Blackwell.

288. Pettigrew A M (1987) "Context and Action in the Transformation of the Firm", *Journal of Management Studies*, Vol.24 (6), pg.649-670.

289. Pettigrew A M (1990) "Longitudinal Field Research on Change: Theory and Practice", *Organization Science*, Vol.1 (3), pg.267-292.

290. Pettigrew A M, E Ferlie, and L McKee (1992) *Shaping Strategic Change*, London, UK: Sage Publications Ltd.

291. Pfefer J (2003) "Deep in Benchmarking: Using Industry Standards to Assess a Training Program", *Proceedings of the 31st Annual ACM SIGUCCS Conference on User Services*, San Antonio, Texas: US, 21-24 September 2003.

292. Pidgeon N F (1997) *Risk Communication and the Social Amplification of Risk - Phase 1 Scoping Study*, Report to the UK Health and Safety Executive (Risk Assessment and Policy Unit), RSU Ref 3625/R62.076, London (UK): HSE Books.

293. Pidgeon N F (1998) "Risk Assessment, Risk Values and the Social Science Programme: Why We Do Need Risk Perception Research", *Reliability Engineering and System Safety*, Vol.59, pg.5-15.

294. Pidgeon N F (1999) "Risk Communication and the Social Amplification of Risk: The Evidence, and Policy Implications", *Risk, Decision and Policy*, Vol.4 (1), pg.1-15.

295. Pidgeon N F, C Hood, D Jones, B Turner and R Gibson (1992) "Risk Perception", in Royal Society Study Group (eds.) *Risk: Analysis, Perception and Management*, London (UK): The Royal Society, pg.89-134.

296. Pidgeon N F, K Henwood and B Maguire (1999) "Public Health Communication and the Social Amplification of Risks: Present Knowledge and Future Prospects", in P Bennett and K Calman (eds.) *Risk Communication and Public Health*, Oxford (UK): Oxford University Press, pg.65-77.

297. Pidgeon N F, R E Kasperson, and P Slovic (eds.) (2003) *The Social Amplification of Risk*, Cambridge (UK): Cambridge University Press.

298. Pincus J D (2005) "Computer Science is Really a Social Science", Microsoft Research. Available at: http://dl.lib.brown.edu/intranet/ws/userx/docs/Microsoft--Computer%20Science%20is%20Really%20a%20Social%20Science.pdf (last accessed: 19/01/2009).

299. Plough A and S Krimsky (1987) "The Emergence of Risk Communication Studies: Social and Political Context", *Science, Technology, and Human Values*, Vol.12 (3-4), pg.4-10.

300. PMI (Project Management Institute) (2000), *A Guide to the Project Management Body of Knowledge: PMBOK Guide*, 2000 edition, Project Management Institute.

301. Poortinga W and N Pidgeon (2004) "Trust in Risk Regulation: Cause or Consequence of the Acceptability of GM Food?", *Centre of Environmental Risk*, University of East Anglia.

302. Post G and A Kagan (1998) "The Use and Effectiveness of Anti-Virus Software", *Computers & Security*, Vol.17 (7), pg.589-606.

303. Power M (2008) *Organized Uncertainty: Designing a World of Risk Management*, Oxford, UK: Oxford University Press.

304. Putnam R (1993) *Making Democracy Work: Civic Traditions in Modern Italy*, Princeton, US: Princeton University Press.

305. Putnam R (1995) "Tuning In, Tuning Out: The Strange Disappearance of Social Capital in America", *PS: Political Science and Politics*, Vol.28 (4), pg.664-683.

306. Rayner S (1988) "Muddling Through Metaphors to Maturity: A Commentary on Kasperson et al, 'The Social Amplification of Risk'", *Risk Analysis*, Vol.8 (2), pg.201-204.

307. Rayner S (1992) "Cultural Theory and Risk Analysis", in S Krimsky and D Golding (eds.) *Social Theories of Risk*, Westport, CT: Praeger, pg.83-115.

308. Rayner S and R Cantor (1987) "How Fair is Fair enough? The Cultural Approach to Societal Technology Choice", *Risk Analysis*, Vol.7 (1), pg.3-13.

309. Reason J (1990) *Human Error*, Cambridge, UK: Cambridge University Press.

310. Reason J (1997) *Managing the Risks of Organizational Accidents*, Brookfield, Vt.: Ashgate.

311. Regester M and J Larkin (2008) *Risk Issues and Crisis Management in Public Relations*, 4th edition, London (UK): Kogan Page Ltd.

312. Renn O (1991) "Risk Communication and the Social Amplification of Risk", in R E Kasperson and P-J M Stallen (eds.) *Communicating Risks to the Public: International Perspectives*, Dordrecht: Kluwer, pg.287-324.

313. Renn O (1992a) "Concepts of Risk: A Classification", in S Krimsky and D Golding (eds.) *Social Theories of Risk*, Westport, CT: Praeger.

314. Renn O (1992b) "Risk Communication: Towards a Rational Dialogue with the Public", *Journal of Hazardous Materials*, Vol.29 (3), pg.465-519.

315. Renn O (1998) "The Role of Risk Perception for Risk Management", *Reliability Engineering and System Safety*, Vol.59, pg.49-62.

316. Renn O (2001) "The Changing Character of Regulation: A Comparison of Europe and the United States", *Risk Analysis*, Vol.21 (3), pg.406-410.

317. Renn O (2003) "Social Amplification of Risk in Participation: Two Case Studies", in N Pidgeon, R E Kasperson, and P Slovic (eds.) *The Social Amplification of Risk*, Cambridge (UK): Cambridge University Press, pg.374-401.

318. Renn O (2004a) "Perception of Risks", *Geneva Papers on Risk and Insurance*, Vol.29 (1), pg.102-114.

319. Renn O (2004b) "The Challenge of Integrating Deliberation and Expertise: Participation and Discourse in Risk Management", in T L McDaniels and M J Small (eds.) *Risk Analysis and Society: An Interdisciplinary Characterization of the Field*, Cambridge (UK): Cambridge University Press, pg.289-366.

320. Renn O (2007) "The Risk Handling Chain" in F Bouder, D Slavin, and R Löfstedt (eds.) *The Tolerability of Risk: A New Framework for Risk Management*, London (UK): Earthscan, pg.21-74.

321. Renn O (2008) *Risk Governance: Coping with Uncertainty in a Complex World*, Sterling, VA: Earthscan.

322. Renn O and B Rohrmann (2000) "Cross-cultural Risk Perception Research: State and Challenges", in O Renn and B Rohrmann (eds.) *Cross-Cultural Risk Perception: A Survey of Empirical Studies*, Dordrecht: Kluwer, pg.211-233.

323. Renn O and A Klinke (2004) "Systemic Risks: A New Challenge for Risk Management", *EMBO Reports*, Vol.5 (Special Issue), pg.41-46. Available at: http://www.nature.com/embor/journal/v5/n1s/pdf/7400227.pdf (last accessed: 9/2/2009).

324. Renn O and Levine D (1991) "Credibility and Trust in Risk Communication", in R E Kasperson and P J Stallen (eds.) *Communicating Risk to the Public*, Dordrecht, The Netherlands: Kluwer Academic Publishers, pg.175-218.

325. Renn O, W J Burns, J X Kasperson, R E Kasperson, and P Slovic (1992) "The Social Amplification of Risk: Theoretical Foundations and Empirical Applications", *Journal of Social Issues*, Vol.48 (4), pg.137-160.

326. Renn O, T Webler, H Rakel, P C Dienel, and B Johnson (1993) "Public Participation in Decision Making: A Three-step Procedure", *Policy Sciences*, Vol.26, pg.189-214.

327. Renn O, T Webler, and P Wiedemann (eds.) (1995) *Fairness and Competence in Citizen Participation: Evaluating Models of Environmental Discourse*, Dordrecht: Kluwer.

328. Renn O, C Jaeger, E Rosa, and T Webler (2005) "The Rational Actor Paradigm in Risk Theories: Analysis and Critique", *Proceedings of the Social Contexts & Responses to Risk (SCARR) Launch Conference*, Canterbury, UK: 28-29 January 2005.

329. Repenning N P and J D Sterman (2001) "Nobody Ever Gets Credit for Fixing Problems that Never Happened: Creating and Sustaining Process Improvement", *California Management Review*, Vol.43, pg.64-88.

330. Rijpma J A (1997) "Complexity, Tight-Coupling and Reliability: Connecting Normal Accidents Theory and High Reliability Theory", *Journal of Contingencies and Crisis Management*, Vol.5, pg.15-23.

331. Riley P (1983) "A Structurationist Account of Political Culture", *Administration Science Quarterly*, Vol.28, pg.414-437.

332. Rindfleisch T C (1997) "Privacy, Information Technology, and Health Care", *Communications of the ACM*, Vol.40 (8), pg.93-100.

333. Rip A (1988) "Should Social Amplification of Risk be Counteracted?", *Risk Analysis*, Vol.8 (2), pg.193-197.

334. Roberts K H (1989) "New Challenges in Organization Research: High Reliability Organizations", *Industrial Crisis Quarterly*, Vol.3 (2), pg.111-125.

335. Roberts K H (1990a) "Some Characteristics of One Type of High Reliability Organization", *Organization Science*, Vol.1 (2).

336. Roberts K H (1990b) "Managing High Reliability Organizations", *California Management Review*, Vol.32 (4).

337. Roberts K H and R Bea (2001) "Must Accidents Happen? Lessons from High-Reliability Organizations", *Academy of Management Executive*, Vol.15, pg.70-79.

338. Roberts K H and Libuser C (1993) "From Bhopal to Banking", *Organizational Dynamics*, Vol.21, pg.15-26.

339. Roberts K H and D M Rousseau (1989) "Research in Nearly Failure-Free, High Reliability Organizations: Having the Bubble", *IEEE Transactions on Engineering Management*, Vol.36 (2).

340. Roche M (2000) *Mega-Events and Modernity: Olympics and Expos in the Growth of Global Culture*, London, UK: Routledge.

341. Rochlin G I, T R La Porte, and K H Roberts (1987) "The Self-Designing High Reliability Organization: Aircraft Carrier Flight Operations at Sea", *Naval War College Review*, Vol. August, pg.84-85.

342. Rohrmann B (1992) "The Evaluation of Risk Communication Effectiveness", *Acta Psychologica*, Vol.81, pg.169-192.

343. Rohrmann B and O Renn (2000) "Risk Perception Research: An Introduction", in O Renn and B Rohrmann (eds.) *Cross-Cultural Risk Perceptions: A Survey of Empirical Studies*, Dordrecht: Kluwer, pg.11-54.

344. Rosa E A (1994) "Mirrors and Lenses: Towards Theoretical Method in the Study of the Nature-Culture Dialectic", in D Duclos (ed.) *La Societe au Naturel: Functions de la Nature*, Paris, FR: L'Harmattas.

345. Rosa E A (1998) "Metatheoretical Foundations for Post-Normal Risk", *Journal of Risk Research*, Vol.1, pg.15-44.

346. Rosa E A (2003) "The Logical Structure of the Social Amplification of Risk Framework (SARF): Metatheoretical Foundations and Policy Implications", in N Pidgeon, R E Kasperson, and P Slovic (eds.) *The Social Amplification of Risk*, Cambridge (UK): Cambridge University Press, pg.47-79.

347. Rose N (1990) *Governing the Soul*, London, UK: Routledge.

348. Ryan K E and L Destefano (2000) *Evaluation as a Democratic Process: Promoting Inclusion, Dialogue, and Deliberation*, San Francisco, CA: Jossey-Bass.

349. Sagan S D (1993) *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*, Princeton, NJ: Princeton University Press.

350. Schein E H (1996) "Culture: The Missing Concept in Organization Studies", *Administrative Science Quarterly*, Vol.41, pg.229-240.

351. Schneier B (2000) *Secrets & Lies: Digital Security in a Networked World*, New York: John Wiley and Sons.

352. Schneier B (2004) "The People Paradigm". Available at: http://www.csoonline.com/article/219787/Bruce_Schneier_The_People_Paradigm (last accessed: 13/01/2009).

353. Schulman P R (1993a) "The Analysis of High Reliability Organizations", in K H Roberts (ed.) *New Challenges to Understanding Organizations*, New York, NY: Macmillan.

354. Schulman P R (1993b) "The Negotiated Order of Organizational Reliability", *Administration and Society*, Vol.25, pg.353-372.

355. Schultze U and D E Leidner (2002) "Studying Knowledge Management in Information Systems Research: Discourses and Theoretical Assumptions", *MIS Quarterly*, Vol.26 (3), pg.213-242.

356. Scott W R (1987) *Organizations: Rational, Natural and Open Systems*, Englewood Cliffs, NJ: Prentice-Hall.

357. Senge P M (1990) *The Fifth Discipline: The Art and Practice of the Learning Organization*, New York, NY: Doubleday.

358. Shannon C E and W Weaver (1949) *A Mathematical Model of Communication*, Urbana, IL: University of Illinois Press.

359. Shedden P, T Ruighaver, and A Ahmad (2006) "Risk Management Standards - The Perception of Ease of Use", *Proceedings of the 5th Annual Security Conference*, Las Vegas: US, 19-20 April 2006.

360. Short J F (1989) "On Defining, Describing, and Explaining Elephants (and Reactions to the Them): Hazards, Disasters, and Risk Analysis", *Mass Emergencies and Disasters*, Vol.7 (3). Pg.397-418.

361. Short J F (1992) "Defining, Explaining, and Managing Risks", in J F Short and L Clarke (eds.) *Organizations, Uncertainties, and Risk*, Boulder, CO: Westview, pg.3-23.

362. Short J F and L Clarke (1992) "Social Organization and Risk", in J F Short and L Clarke (eds.) *Organizations, Uncertainties, and Risk*, Boulder, CO: Westview, pg.309-332.

363. Silverman D (1993) *Interpreting Qualitative Data: Methods for Analysing Talk, Text and Interaction*, London (UK): Sage.

364. Silvers J R (2003) *Event Management Body of Knowledge Project (EMBOK)*. Available at: http://www.juliasilvers.com/embok.htm (last accessed: 23/03/2009).

365. Silvers J R (2004) *Professional Event Coordination*, New York, NY: John Wiley and Sons.

366. Silvers J R (2008) *Risk Management for Meetings and Events*, Oxford: Elsevier Ltd.

367. Silvers J R, G A J Bowdin, W J O'Toole, and K B Nelson (2006) "Towards an International Event Management Body of Knowledge (EMBOK)", *Event Management*, Vol.9 (4), pg.185-198.

368. Sjöberg L (1999) "Risk Perception in Western Europe", *Ambio*, Vol.28, pg.555-568.

369. Slovic P (1972) "From Shakespeare to Simon: Speculation - and Some Evidence - about Man's Ability to Process Information", *Oregon Research Institute Research Monograph*, Vol.12 (2).

370. Slovic P (1986) "Informing and Educating the Public about Risk", *Risk Analysis*, Vol.6 (4), pg.403-415.

371. Slovic P (1987a) "Forecasting the Adverse Economic Effects of a Nuclear Waste Repository", in R G Post (ed.) *Waste Management '87*, Tuscon: Arizona Board of Regents, University of Arizona, pg.91-94.

372. Slovic P (1987b) "Perception of Risk", *Science*, Vol.236 (4799), pg.280-285.

373. Slovic P (1992) "Perception of Risk: Reflections on the Psychometric Paradigm", in S Krimsky and D Golding (eds.) *Social Theories of Risk*, Westport, CT: Praeger, pg.117-152.

374. Slovic P (1993) "Perceived Risk, Trust and Democracy", *Risk Analysis*, Vol.13 (6), pg. 675-682.

375. Slovic P (1997) "Trust, Emotion, Sex, Politics and Science: Surveying the Risk-assessment Battlefield", in M Bazerman, D Messick, A Tenbrunsel and K Wade-Benzoni (eds.) *Environment, Ethics and Behaviour*, San Francisco, CA: New Lexington Press, pg.277-313.

376. Slovic P (2000) *The Perception of Risk*, London (UK): Earthscan.

377. Slovic P (2002) "Terrorism as Hazard: A New Species of Trouble", *Risk Analysis*, Vol.22 (3), pg.425-426.

378. Slovic P, B Fischoff, and S Lichtenstein (1976) "Cognitive Processes and Societal Risk Taking", in J S Carroll and J W Payne (eds.) *Cognition and Social Behaviour*, Potomac, MD: Lawrence Erlbaum Associates Inc., pg.165-184.

379. Slovic P, B Fischoff, and S Lichtenstein (2000) "Response Mode, Framing, and Information-Processing Effects in Risk Assessment", in P Slovic (ed.) *The Perception of Risk*, London (UK): Earthscan.

380. Slovic P, B Fischoff, and S Lichtenstein (1980) "Facts and Fears: Understanding Perceived Risk", in R C Schwing and W A Alberts (eds.) *Societal Risk Assessment: How Safe is Safe Enough?*, New York: Plenum Press.

381. Smith P G and G M Merritt (2002) *Proactive Risk Management: Controlling Uncertainty in Product Development*, New York, NY (US): Productivity Press.

382. Smith B, R Montagno and S K Sharma (2006) "Translating Security Framework info an Organization Culture", *Proceedings of the 5th Annual Security Conference*, Las Vegas: US, 19-20 April 2006.

383. Snyder M and A A Stukas Jr (1999) "Interpersonal Processes: The Interplay of Cognitive, Motivational, and Behavioural Activities in Social Interaction", *Annual Review of Psychology*, Vol.50 (1999), pg.273-303.

384. Spafford E H (1989) "Crisis and Aftermath", *Communications of the ACM*, Vol.32 (6), pg.678-687.

385. Spagnoletti P (2006) "Learning from Computer Incidents", *Proceedings of the 5th Annual Security Conference*, Las Vegas: US, 19-20 April 2006.

386. Spears J L (2006a) "Defining Information Security", *Proceedings of the 5th Annual Security Conference*, Las Vegas: US, 19-20 April 2006.

387. Spears J L (2006b) "The Effects of User Participation in Identifying Information Security Risk in Business Processes", *Proceedings of the 2006 ACM SIGMIS CPR Conference on Computer Personnel Research*, Claremont, CA: US, 13-15 April 2006.

388. Spears J L and R J Cole (2006) "A Preliminary Investigation of the Impact of the Sarbanes-Oxley Act on Information Security", *Proceedings of the 39th Hawaii International Conference on Systems Sciences (HICSS)*, Koloa, Kauai, HI: IEEE Computer Security.

389. Spencer J (2006) "Disaster Recovery and Business Continuity Planning: A Case Study of an Incident at ABC Corporation", *Proceedings of the 5th Annual Security Conference*, Las Vegas: US, 19-20 April 2006.

390. Stake R (1995) *The Art of Case Study Research*, Thousand Oaks (CA): Sage Publications.

391. Stanton J M, K R Stam, P R Mastrangelo, and J Jolton (2004) "Behavioural Information Security: Two End-User Survey Studies of Motivation and Security Practices", *Proceedings from the 10th Americas Conference on Information Systems*, New York, US.

392. Stanton J M, K R Stam, P R Mastrangelo, and J Jolton (2005) "Analysis of End User Security Behaviours", *Computers & Security*, Vol.24 (2), pg.124-133.

393. Star S L and E Gerson (1987) "The Management and Dynamics of Anomalies in Scientific Work", *Sociological Quarterly*, Vol.28, pg.147-169.

394. Starbuck W H and F J Milliken (1988) "Challenger: Fine-Tuning the Odds Until Something Breaks", *Journal of Management Studies*, Vol.25, pg.329-330.

395. Stavroulakis P (2003) *Reliability, Survivability and Quality of Large Scale Telecommunication Systems: Case Study - Olympic Games*, Chichester, UK: John Wiley and Sons.

396. Stedman G, J J Godlblatt, and L D Neirotti (2001) *The Ultimate Guide to Sports Marketing*, 2nd edition, New York, NY (US): McGraw-Hill Professional.

397. Steinbruner J D (1974) *The Cybernetic Theory of Decision*, Princeton, NJ: Princeton University Press.

398. Sterman J D (2000) *Business Dynamics: Systems Thinking and Modelling for a Complex World*, Boston, MA: Irwin/McGraw-Hill.

399. Stern P C and H V Fineberg (eds.) (1996) *Understanding Risk: Informing Decisions in a Democratic Society*, Report for National Research Council, Committee on Risk Characterization, Washington, DC: National Academy Press.

400. Straub D (1990) "Effective IS Security: An Empirical Study", *Information Systems Research*, Vol.1 (3), pg.255-276.

401. Straub D and Welker R (1998) "Coping with Systems Risk: Security Planning Models for Management Decision Making", *MIS Quarterly*, Vol.22 (8), pg.441-465.

402. Strauss A (1978) *Negotiations*, San Franciscon, CA: Jossey-Bass.

403. Strauss A (1982) "Inter-organizational Negotiation", *Urban Life*, Vol.11, pg.350-367.

404. Suh B and I Han (2003) "The IS risk analysis based on a business model", *Information & Management*, Vol.41 (2), pg.149-158.

405. Sunstein C (2003) "Terrorism and Probability Neglect", *The Journal of Risk and Uncertainty*, Vol.26 (2/3), pg.121-136.

406. Sutcliffe K M and Vogus T J (2003) "Organizing for Resilience", in K S Cameron, J E Dutton, and R E Quinn (eds.) *Positive Organizational Scholarship*, San Francisco, CA: Berrett-Koehler, pg.94-110.

407. Svenson O (1988a) "Managing Product Hazards at Volvo Car Corporation", in R E Kasperson, J X Kasperson, C Hohenemser, and R W Kates (eds.) *Corporate Management of Health and Safety Hazards: A Comparison of Current Practice*, Boulder, CO: Westview, pg.57-78.

408. Svenson O (1988b) "Mental Models of Risk Communication and Action: Reflections on Social Amplification of Risk", *Risk Analysis*, Vol.8 (2), pg.199-200.

409. Tamuz M (1987) "The Impact of Computer Surveillance on Air Safety Reporting", *Columbia Journal of World Business*, Vol.22, pg.69-77.

410. Tarlow P E (2002) *Event Risk Management and Safety*, New York, US: John Wiley and Sons, Inc.

411. Taylor P (1998) "The Internet Changes Everything", FT Information Technology. Available at: http://specials.ft.com/ln/ftsurveys/q4f9a.htm (last accessed: 12/01/2009).

412. Taylor-Gooby P (2004) "Psychology, Social Psychology and Risk", *SCARR Working Paper (2004/3)*, Canterbury, UK: University of Kent.

413. Taylor-Gooby P and J Zinn (2005) "Current Directions in Risk Research: Reinvigorating the Social?", *SCARR Working Paper (2005/8)*, Canterbury, UK: University of Kent.

414. Theodoraki E (2007) *Olympic Event Organization*, Oxford, UK: Elsevier Butterworth-Heinemann.

415. Theoharidou M, S Kokolakis, M Karyda, E Kiountouzis (2005) "The Insider Threat to Information Systems and the Effectiveness of ISO17799", *Computers and Security*, Vol.24, pg.472-484.

416. Thomson M E and R von Solms (1998) "Information Security Awareness: Educating Your Users Effectively", *Information Management & Computer Security*, Vol.6 (4), pg.167-173.

417. Thompson P B and W R Dean (1996) "Competing Conceptions of Risk", *Risk: Health, Safety and Environment*, Vol.7, pg.361-384.

418. Trumbo C W (1996) "Examining Psychometrics and Polarization in a Single-risk Case Study", *Risk Analysis*, Vol.16, pg.429-438.

419. Tulloch J and D Lupton (2003) *Risk and Everyday Life*, London, UK: Sage.

420. Turner B A (1978) *Man-made Disasters*, London, UK: Wykeham.

421. Turner B A and N F Pidgeon (1997) *Man-made Disasters*, 2nd edition, Oxford, UK: Butterworth-Heinemann.

422. Tversky A and Kahneman D (1974) "Judgement under Uncertainty: Heuristics and Biases", *Science*, Vol.185, pg.1124-31.

423. Tversky A and Kahneman D (1981) "The Framing of Decisions and the Psychology of Choice", *Science*, Vol.211, pg.453-458.

424. UK Audit Commission (1994) *Opportunity Makes a Thief: An Analysis of Computer Abuse*, London: UK Audit Commission.

425. Vaughan D (1992) "Regulating Risk: Implications of the Challenger Accident", in J F Short Jr. and L Clarke (eds.) *Organizations, Uncertainties, and Risk*, Boulder, CO: Westview, pg.235-254.

426. Vaughan D (1995) "The Significance of Socioeconomic and Ethnic Diversity for the Risk Communication Process", *Risk Analysis*, Vol.15 (2), pg.169-180.

427. Vaughan D (1996) *The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA*, Chicago: University of Chicago Press.

428. Vaughan D (1999) "The Dark Side of Organizations: Mistake, Misconduct, and Disaster", *Annual Review of Sociology*, Vol.25, pg.271-305.

429. Vaughan D (2002) "Signals and Interpretive Work: The Role of Culture in a Theory of Practical Action", in K A Cerulo (ed.) *Culture in Mind: Toward a Sociology of Culture and Cognition*, New York, NY: Routledge, pg.28-54.

430. Vaughan D (2005) "Organizational rituals of risk and error", in B Hutter and M Power (2005) *Organizational Encounters with Risk*, Cambridge, UK: Cambridge University Press.

431. Venter H S and J H P Eloff (2003) "A Taxonomy for Information Security Technologies", *Computer and Security*, Vol.12 (6), pg.527-535.

432. Wahlberg A (2001) "The Theoretical Features of Some Current Approaches to Risk Perception", *Journal of Risk Research*, Vol.4, pg.237-250.

433. Walker G, P Simmons, B Wynne, and A Irwin (1998) *Public Perception of Risks Associated with Major Accident Hazards*, Health and Safety Laboratory, CRR 194/1998.

434. Walsham G (1993) *Interpreting Information Systems in Organizations*, Chichester: Wiley.

435. Wang J and C Wang (2003) "Taxonomy of Security Considerations and Software Quality", *Communications of the ACM*, Vol.46 (8), pg.91-95.

436. Watts B D (1989) "Unreported History and Unit Effectiveness", *Journal of Strategic Strategies*, Vol.12 (1), pg.88-98.

437. WBGU (German Advisory Council on Global Change) (2000) *World in Transition: Strategies for Managing Global Environmental Risks*, Annual report, Heidelberg and New York: Springer.

438. Weber M (1949) *The Methodology of the Social Sciences*, Glencoe: Free Press.

439. Weber M (1962) *Basic Concepts in Sociology*, London, UK: Peter Owen.

440. Weber M (1968) *On Charisma and Institution Building: Selected Papers*, (ed.) S N Eisenstadt, Chicago: University of Chicago Press.

441. Webler T (1995) "'Right' Discourse in Citizen Participation: an Evaluative Yardstick" in O Renn, T Webler and P Wiedemann (eds.) *Fairness and Competence in Citizen Participation: Evaluating New Models for Environmental Discourse*, Dordrecht: Kluwer, pg.35-86.

442. Webler T (1999) "The Craft and Theory of Public Participation", *Risk Research*, Vol.2, pg.55-71.

443. Weeks E (2000) "The Practice of Deliberative Democracy: Results from Four Large-Scale Trials", *Public Administration Review*, Vol.60 (4), pg.360-372.

444. Wenger M R (2006) "Information Security and the Psychological Contract: A Trust Perspective", *Proceedings of the 5th Annual Security Conference*, Las Vegas: US, 19-20 April 2006.

445. Weick K E (1987) "Organizational Culture as a Source of High Reliability", *California Management Review*, Vol.29 (2).

446. Weick K E (1990) "The Vulnerable System", *Journal of Management*, Vol.16, pg.571-593.

447. Weick K E and K M Sutcliffe (2001) *Managing the Unexpected: Assured High Performance in an Age of Complexity*, San Francisco, CA: Jossey-Bass.

448. Weick K E and K M Sutcliffe (2007) *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*, 2nd edition, San Francisco, CA: Jossey-Bass.

449. Weick K E, K M Sutcliffe, and D Obstfeld (1999) "Organizing for High Reliability: Processes of Collective Mindfulness", in B M Staw and R I Sutton (eds.) *Research in Organizational Behaviour: Volume 21*, Greenwich, Conn.: JAI Press.

450. Weiss J (1986) *Weber and the Marxist World*, London, UK: Routledge and Kegan Paul.

451. Weiss J W and R K Wysocki (1992) *5-Phase Project Management: A Practical Planning and Implementation Guide*, US: Perseus Books Publishing.

452. Westerbeek H, A Smith, P Turner, P Emery, C Green and L van Leeuwen (2005) *Managing Sport Facilities and Major Events*, St Leonards, Australia: Allen & Unwin.

453. Weyman A and C Kelly (1999) *Risk Perception and Communication: A Review of the Literature*, Health and Safety Laboratory, CRR 248/1999.

454. Whitman M E (2003) "Enemy at the Gate: Threats of Information Security", *Communications of the ACM*, Vol.46 (8), pg.91-95.

455. Whitman M E and H J Mattord (2005) *Principles of Information Security*, Canada: Course Technology.

456. Wiant T L (2003) *Policy and Its Impact on Medical Record Security*, PhD Thesis, Kentucky, US: University of Kentucky.

457. Wiedemann P, Clauberg M, and Schutz H (2003) "Understanding Amplification of Complex Risk Issues: the Risk-Story Model Applied to the EMF", in Pidgeon N, Kasperson R E, and Slovic P (eds.) *The Social Amplification of Risk*, Cambridge: Cambridge University Press.

458. Wildavsky A (1988) *Searching for Safety*, New Brunswick, NJ: Transaction Books.

459. Wilde G J S (1994) *Target Risk*, Toronto, Canada: PDE Publications.

460. Williams W (1998) *Honest Numbers and Democracy*, Washington, DC: Georgetown University Press.

461. Williamson J and A Weyman (2005) *Review of the Public Perception of Risk, and Stakeholder Engagement*, Health and Safety Laboratory, HSL/2005/16. Available at: http://www.hse.gov.uk/research/hsl_pdf/2005/hsl0516.pdf (last accessed: 19/01/2009).

462. Wilson R and E Crouch (1982) *Risk/Benefit Analysis*, Cambridge, MA: Ballinger Publishing Co.

463. Witkin H A, C A Moore, D R Goodenough and P W Cox (1977) "Field-dependent and Field-independent Cognitive Styles and their Educational Implications", *Review of Educational Research*, Vol.47 (1), pg.1-64.

464. Wood C, B Dipper, and C Jones (2000) "Auditing the Assessment of the Environmental Impacts of Planning Projects", *Journal of Environmental Planning and Management*, Vol.43 (1), pg.23-47.

465. World Bank (1994) *An Overview of Monitoring and Evaluation in the World Bank*, Report No.13247, Washington, DC: Operations Evaluation Department, World Bank.

466. World Bank (1992) *Economic Analysis of Projects: Towards a Results-Oriented Approach to Evaluation*, ECON Report, Washington, DC: World Bank.

467. Wynne B (1992) "Risk and Social Learning: Reification to Engagement", in S Krimsky and D Golding (eds.) *Social Theories of Risk*, Westport, CT: Praeger, pg.257-297.

468. Yates J F (2003) *Decision Management: How to Assure Better Decisions in Your Company*, San Francisco, CA: Jossey-Bass.

469. Yayla A and Q Hu (2005) "The Impact of Security Breaches on the Value of Stocks: Differences between E-Commerce and Traditional Firms", *Proceedings from the 4th Security Conference*, Las Vegas, US.

470. Yin R K (1989) *Case Study Research: Design and Method*, Newbury Park, CA: Sage Publications.

471. Yoshikawa M (1987) "The Double-swing Model of Intercultural Communication Between the East and the West", in M Kinkaid (ed.) *Communication Theory: Eastern and Western Perspectives*, London: Academic Press/ Harcourt Brace Jovanovich College Publishers, pg.319-329.

472. Zinn J (2004a) "Literature Review: Economics and Risk", *SCARR Working Paper (2004/2)*, Canterbury, UK: University of Kent.

473. Zinn J (2004b) "Literature Review: Sociology and Risk", *SCARR Working Paper (2004/1)*, Canterbury, UK: University of Kent.

474. Zinn J (2006) "Recent Developments in Sociology of Risk and Uncertainty", *Forum: Qualitative Social Research*, Vol.7 (1). Available at: http://www.qualitative-research.net/index.php/fqs/article/view/68/140 (last accessed: 19/01/2009).

475. Zinn J (2006) "Risk, Social Change and Morals: Conceptual Approaches of Sociological Risk Theories", *SCARR Working Paper (2007/17)*, Canterbury, UK: University of Kent.

476. Zinn J and P Taylor-Gooby (2006a) "Risk as an Interdisciplinary Research Area" in P Taylor-Gooby and J Zinn (eds.) *Risk in Social Science*, Oxford, UK: Oxford University Press, pg. 20-53.

477. Zinn J and P Taylor-Gooby (2006b) "The Challenge of (Managing) New Risks" in P Taylor-Gooby and J Zinn (eds.) *Risk in Social Science*, Oxford, UK: Oxford University Press, pg. 54-75.