Operational Risk in Incident Management: a Cross-fertilisation between ISCRAM and IT Governance

Gerd Van Den Eede
Vlekho Business School, Belgium
gvdeede@vlekho.wenk.be

Bartel A. Van de Walle
Tilburg University, The Netherlands
bartel@uvt.nl

ABSTRACT

The objectives of the research reported by the authors in this paper are threefold. First, the authors want to fine-tune the rresearch methodology on risk identification based on cognitive mapping techniques and group decision support systems (GDSS) developed earlier (Rutkowski et al., 2005). Second, the authors want to determine how High Reliability Theory (HRT) - through the characteristics of High Reliability Organisations (HROs) - can be applied in the particular organisational context of an important economic sector like banking. Third, the authors want to inquire into how Information Systems for Crisis Response and Management can benefit from experiences gained in a mainstream context. More specifically, the use of the Information Technology Infrastructure Library (ITIL) methodology will be explored from the perspective of Incident Management as a sub-process of ICT management.

Keywords

High Reliability Theory, Normal Accidents Theory, learning organisation, knowledge management, cognitive mapping, Group Decision Support Systems, operational risk, incident management, IT governance, financial institution, ISCRAM.

INTRODUCTION

In recent years the business world has experienced major operational losses. Business failures like Barings, Enron, Worldcom and Parmalat are still fresh in memory and caused a shift from the initial emphasis on commercial risks towards the process of managing operational risks. Whereas the US Sarbanes-Oxley Act is determining operational risk management in general, the Basel II Capital Accord more specifically is steering the financial institutions in their effort to get control of operational threats they might encounter. As most of the operational risks in banking and insurance are linked to information and communication technology (ICT), this functional department gets a lot of attention lately. A financial institution traditionally runs various ICT processes which all need investigation in terms of risk identification, assessment and mitigation.

The authors are involved in the process of risk identification in Incident Management as one of the ICT sub-processes at a major financial institution. They are using a methodology that is based on the techniques of cognitive mapping and group decision making that has been applied in an earlier project (Rutkowski *et al*., 2005). The deep-seated objective of this bank's senior management is to realise a higher reliability of its ICT organisation in combination with a high degree of flexibility. In this respect this objective comes down to becoming a Learning Organisation (Wishart, 1996) by examining the characteristics of High Reliability Organisations (HROs) (Van Den Eede *et al*, 2004) and transposing them to their own more mainstream - but large and complex - organisational context (Grabowski *et al.*, 1997).

The objectives of the research reported by the authors in this paper are threefold. First, the authors want to fine-tune the rresearch methodology on risk identification based on cognitive mapping techniques and group decision support systems (GDSS) developed earlier (Rutkowski *et al*., 2005). Second, the authors want to determine how High Reliability Theory (HRT) - through the characteristics of HROs - can be applied in the particular organisational context of an important economic sector like banking. Third, the authors want to inquire into how Information Systems for Crisis Response and Management (or ISCRAMs) can benefit from experiences gained in a mainstream context. More specifically, the use of the Information Technology Infrastructure Library (ITIL) methodology will be explored from the perspective of Incident Management as a sub-process of ICT management.

THE ORGANISATIONAL CONTEXT

Basel II Regulatory Framework

While the financial stability of a major bank certainly is critical to its customers, the financial stability of the international banking system overall is critical to everyone. The existence of business continuity plans to ensure the ability to operate on an ongoing basis and limit losses in the event of severe business disruption is of public interest. Therefore, these days, through the revision of the original Basel Capital Accord (known as Basel I), the banking industry is undergoing thorough changes in the way it thinks about operational risk and security. The Basel-based Bank for International Settlements (BIS) sets standards for the key banks in major countries with global stability in mind (Geer, 2004). This Basel II Capital Accord (known as Basel II) in this respect is a regulatory framework governing risk management practices. A special emphasis is placed on operational risk as a new category of risk that could be defined as "the risk of losses resulting from inadequate or failed internal processes, people and systems, or external events" (Chorafas, 2004). Basel II champions the adoption of operational risk management processes and builds on three pillars:

1. Minimum capital requirement as a specification of the the capital reserves a bank must hold to cover against risk exposure. In that sense it introduces risk management techniques based on statistical analysis, which provide a more accurate view of capital adequacy.

2. Supervisory review of capital adequacy which requires banks to submit their risk management capabilities to examination by a supervisory committee. This requirement reflects the need for banks to base their judgements on risk and capital adequacy on more than just capital calculations.

3. Public disclosure because an increased transparency allows the market to see that financial institutions are taking a responsible approach to risk management. This can lead to improved access to capital on the money markets and lower insurance costs.

The deadline for the implementation of Basel II is end 2006; however, to comply with this deadline, banks need to start reviewing their risk management strategies today. It may be presumed that other industries will follow. Basel II will be the key driver for innovation in all sectors, just like the US Sarbanes-Oxley Act already is playing this role for organisations reporting to US stakeholders (Mayer, 2004). In doing so, it will transform operational risk from an obscure financial benchmark into a fundamental business consideration (Geer, 2004).

The financial institution

The organisation at which we were able to carry out our research is a financial services group which is active in the fields of banking, insurance and asset management. It is represented in 30 different countries and offers a full range of financial services to retail customers, businesses and multinational corporations. It has a key position in several European countries. The holding was created in the late nineties through the merger of two banking groups and one insurance company and now serves some 12 million customers and employs about 50.000 people. It holds a Euro zone top 20 ranking in terms of market capitalisation. Its IT department consists of more than 2000 employees.

The department might be considered working under particularly demanding conditions as nearly all critical business processes are relying on their services for their performance. The means and methods by which the department ensures safety and reliability, under continuous pressure to increase efficiency and decrease the potential for human error, are very costly in personal, economic as well as organisational terms. What has made it possible for the department to obtain the necessary financial, organisational and human resources has been the department's credibility in claiming that performance at the expected levels of safety and performance would not be possible otherwise (Rochlin, 1996). In that perspective, the organisation tends to become an HRO as it is e.g. characterised by senior leadership support for safety, redundancy, continuous operations and training, a decentralized decision-making authority, a shared consensus and an ability to learn from mistakes and simulations.

ICT process reliability: Over sizing is also Reliability

As in engineering, oversizing ICT processes in terms of redundancy is one way to cope with reliability matters. This is obviously no longer to be taken for granted or even possible because costs and time drive the world's economy. An accurate prediction of the reliability of infrastructure and processes is obviously highly desirable. Optimistic (too high) or non-credible reliability predictions have led to unanticipated disasters; and pessimistic (too low) reliability predictions can lead to over expensive products/processes (Düpow *et al*., 1997).

THINKING ABOUT RISK

Risk identification is not to be taken for granted

A large range of literature deals with risk management issues but is mostly assuming that management is well equipped to recognize risky situations and identify individual risks (McLucas, 2003). The research design underlying this article suggests that the assumption that managers have detailed understandings of the nature of risks is at best, highly questionable and at worst dangerous. With McLucas (2003), we suggest that a non-expert, knowing or seeing what can be reasonably known or seen can make reasoned and sound choices about risks and risky situations, often long before they develop into sinister consequences. Another observation is that if risks are being effectively managed as a matter of routine, nobody becomes aware of just how effective careful risk-management actions have proven to be. Therefore little or no credit can be gained by being an effective risk manager, whereas poor risk management is certain to result in failure. This is known as the risk management paradox (McLucas, 2003).

For these reasons, we believe that an action research project in the risk identification and risk assessment process is useful. Communication and coordination should be supported to avoid what is known as groupthink (Janis) or internal focus and to favor the development of shared meaning between the different units of the organisation (Rutkowski *et al*., 2004).

Through our research however, we could see that the bank's senior management is not only driven by regulating frameworks (Basel II and other) in their effort to manage risk. The gaining of reliability in this respect is rather a prerequisite for their intention of becoming a Learning Organisation, apart from external pressure to do so. Threat-rigidity for that matter is not a good strategy as threat reduces flexibility, due to – in general – a restriction of information and a constriction of control (Barnett *et al*., 2000). The approach therefore might be one of response flexibility meaning that flexibility may occur under crisis conditions when top managers lead a response to latent rather than existent threats, encourage generating knowledge rather than restricting information and promote decentralizing rather than constricting control (Barnett *et al*., 2000).

Two dominant schools of thought: HRT vs. NAT

Theory discerns between two dominant schools on the origins of accidents and reliability: High Reliability Theory (HRT) with Todd La Porte as principal advocate and Charles Perrow's Normal Accidents Theory (NAT) (Rijpma, 1997; Rochlin, 1996).

The basic thesis of NAT is that accidents are inevitable in complex, tightly-coupled technological systems, like the IT systems and processes of a major financial institution. The advice here is to reduce complexity as the materialization of risk is 'normal'. Reduction of complexity in an ever more demanding commercial world and sharp profit-margins is not obvious, though. Research from the Berkeley school on HRT, suggests the existence of an organizational design that increases reliability of complex systems. In general, HRT focuses on decentralisation (Weick, 1987), redundancy (van Fenema, 2003), and conceptual slack (Grabowski *et al*., 1997). It puts a large emphasis on the emergence of a culture of safety. Table 1 provides a view on how HRT deals with the objections of NAT concerning complex and tightly-coupled systems (Roberts, 1990). In this paper, the authors take HRT as a starting point for their analysis.

Table 1 Dysfunctional characteristics in hazardous organizations and responses designed to lessen their effect.

Complexity	
Characteristics	*Responses*
potential for unexpected sequences	continuous training
	Redundancy
complex technologies	continuous training
	responsibility and accountability at all levels
potential for systems serving incompatible functions to interact	job design strategies to keep functions separate
	Training
indirect information sources	many direct information sources
baffling interactions	training of specialized language
	flexible exercises

Tight coupling	
Characteristics	*Responses*
Time dependent processes	Redundancy
invariant sequences of operations	job specialization
	system flexibility hierarchical differentiations
Only one way to reach goal	Redundancy
	system flexibility
Little slack	bargaining and negotiation
	system flexibility

Systemic risk

The current IS risk paradigm of an individual decision maker and the simple causal model of risk is inadequate for understanding risk control/mitigation in complex socio-technical systems. Since such systems are characterized by interactive complexity and tight coupling, risks increasingly become systemic. Luo Carlo and co-workers (Luo Carlo *et al*., 2004) define "systemic risk" as a risk that originates from multiple sources, affects multiple agents and propagates quickly among individual parts or components. The probability of breakdowns at the system level can be caused by the domino effect triggered from a sudden unexpected event. Since the source of a systemic risk cannot be pinpointed and often resides in the unpredictable interactions among different parts or components, systemic risks cannot be addressed by controlling or mitigating the top ten risks identified by periodical risk review meetings based on group consensus (Luo Carlo *et al*., 2004).

How high-reliability principles could apply to mainstream organisations

We posit that an investigation in how organizations can rely upon organising mechanisms characteristic of HROs could be favorable for their risk-proneness. However, little HRO research to date has provided substantial empirical evidence on how high-reliability principles could apply to mainstream organizations (Luo Carlo *et al*., 2004). Especially for a large and extremely business critical process like ICT in a leading economic industry like banking, in the hazardous and risk sensible context of the post 9/11 era, the research results might be of interest for the way reliability is secured in other highly competitive reliability-seeking organisations.

Yet, not only does an organisation have to be reliable, it also needs to be flexible enough to remain competitive in a highly demanding and changing business environment. The need for becoming a Learning Organisation (Wishart *et al*., 1996) is eminent and comes down to combining flexibility and reliability. Unfortunately, as Figure 1 shows, it seems that these two virtues are quite incompatible or conflicting by definition. In this research however, we precisely wish to illustrate that this is not necessarily the case. Based on our study of literature on High Reliability Organisations (HROs) (Van Den Eede et al., 2004), we argue that mainstream organisations simultaneously can be innovative ('organic i.e. adhocratic structures work best' (Courpasson, 2000) and yet be able to implement and control these innovations ('bureaucratic structures work best'). As such, we will examine whether mainstream organisations can learn from HROs to become truly Learning Organisations. We draw on the work of Mahinda and Whitworth (2004) for the in-depth exploration of flexibility and reliability in the information systems' (IS) robustness underlying this Learning Organisation.

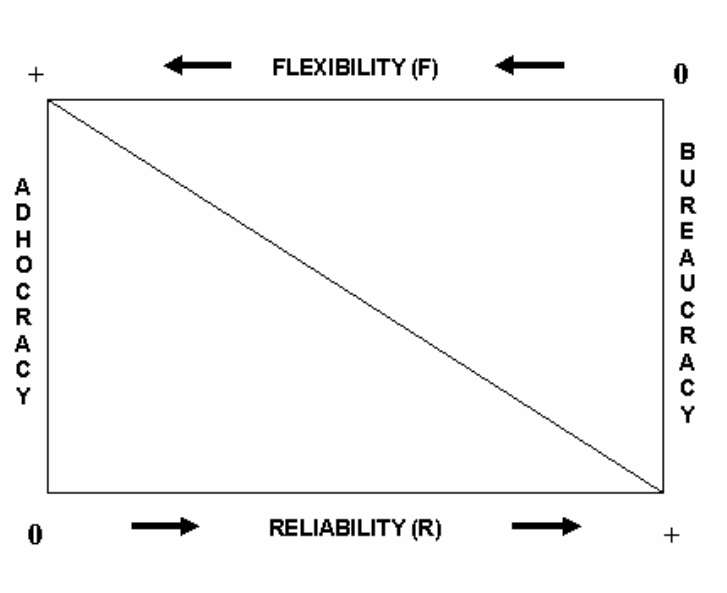

Figure 1. Interrelationship between reliability and flexibility

Although the issue is IT related, our research questions focus on several disciplines and business domains:

- Human Resources (HR) (Vogus, 2003): recruitment, training, intrinsic and extrinsic motivation, succession
- Knowledge Management (KM) (Van Den Eede *et al*, 2004): Sensemaking (Nathan, 2004), Competence Management, knowledge sharing, decision making
- Organisational structure: hierarchy, communication, delegation, centralisation vs. decentralisation, resilience, checks and balances, awareness of the 'big picture' (Roberts, 2001), transactive memory (van Fenema, 2003)
- Infrastructure and technology : technology used, coupling of systems (Grabowski *et al*., 1997), flexibility by detection, flexibility by response, flexibility by adaptation, reliability by modular design, reliability by redundancy, reliability by recovery (Mahinda *et al.*, 2004).
- Processes: existence and nature of procedures, procedures for threatening escalation of incidents, existence of/authorisation for by-passes, registration of incidents etc.
- Culture: preoccupation with failure, reluctance to simplify interpretations, requisite variety in terms of imagination, improvisation, story-telling, vision of management.

How ISCRAM can benefit from experiences gained in a mainstream context

This research also looks at the paradoxical role of ICT in risk control/mitigation in complex systems. On the one hand ICT tends to increase complexity and tight-coupling of complex systems. On the other hand ICT and its related processes can show experience in managing for reliability. A concept like IT-governance has an important track record and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives. In summary (Gray, 2004) the benefits that IT governance brings are that it ensures:

- joint responsibility for planning and executing IS/IT in the business;
- clearer understanding of objectives and expectations;
- clearer visibility of issues and priorities;
- transparency and better comprehension of IT activities and performance and delivers over time
- alignment of IT with business needs;
- improved value delivery (operational and project);
- optimised costs;
- management of IT related risks; and
- improved quality of service.

CObiT

CObiT (Control Objectives for Information and related Technology) is the IT governance framework that connects business risk, control needs and technical issues. It presents IT activities in a manageable and logical structure, and documents good practice across this structure. This helps to optimise information investments and provides a benchmark to be judged against (Gray, 2004).

ITIL

For the management of the exploitation of its services an Information and Communication Technology (ICT) organisation can use ITIL (Information Technology Infrastructure Library). The ITIL method emerged when in the UK the public sector started privatising the exploitation of ICT and the principal wanted to have a grip on the services provided by these privatised ICT departments. This called for the gaining of insight in the tasks to be dealt with by an ICT organisation. Not only the description of tasks viewed apart is important, but also the relationship between various tasks and the course of the processes within the various tasks must be clear. Implementation of ITIL must lead towards implementation of process management supplying services meeting a certain service level (Thiadens *et al*., 2000).

Although ITIL covers a number of areas, its main focus is on IT Service Management (ITSM), which in itself is generally divided into two main areas: Service Support and Service Delivery. Together, these two areas consist of disciplines that are responsible for the provision and management of effective IT services (http://www.itil-itsm-world.com/what.htm).

IT Governance and ISCRAM?

One of the objectives of this research is to investigate whether/how emergency and crisis management organisations can learn from IT Governance best-practices like CObiT and ITIL. In other words: can the Crisis Management process be structured/organised in such a way that the system behaves as a Learning Organisation? We believe it may draw lessons from IT Service Management as the way this process is organised resembles the way ISCRAM should/could be managed: client-oriented, process-oriented and based on best-practices available in the public domain.

RESEARCH DESIGN

For an overview and detailed discussion of the original research methodology on which this work is based, we refer to Rutkowski (Rutkowski et al., 2004; 2005). We limit our discussion here to those elements that have been added by the authors to the original research design.

Phase I – Preparation

During Phase I, several meetings are scheduled to fully prepare for the research project. These include meetings with General ICT Management, Operational Risk Management on a bank holding level, ICT Security Management, and ICT Incident Management. During these sessions the scope, interdependences, timing, budget and approach are finetuned between the bank and its academic partners. A coordinating meeting was organised during which all participants were informed on the project and given the possibility to ask questions or provide feedback and additional remarks.

Phase II – Interviews

At the second phase, interviews are scheduled with various participants/stakeholders of the incident management process. The purpose of these interviews is to gather a broad view on possible risks concerning the IM process. For this purpose two business domains have been selected that together provide a rich and varied context, leading to more than twenty interviews in total. The participants in these interviews are managers from both business domains, ICT domains, ICT audit, Operational Risk department, senior management and the ICT security department..

The purpose of these time-consuming interviews is to gain a deeper insight into the potential risks and to avoid groupthink. Janis originally defined groupthink as "*a mode of thinking that people engage in when they are deeply involved in a cohesive in-group, when the members' strivings for unanimity override their motivation to realistically appraise alternative courses of action*". According to this definition, groupthink occurs only when cohesiveness is high. It requires that members share a strong "we-feeling" of solidarity and desire to maintain relationships within the group at all costs. When colleagues operate in a groupthink mode, they automatically apply the "*preserve group harmony*" test to every decision they face (Janis).

Phase III – Mapping interviews into individual & collective Cognitive Maps (Phase IV)

The technique used in this phase to register and elicit the perceived risks is Cognitive mapping (Ackermann, 2004), which may be defined as a set of techniques for studying and recording people's perceptions about their environment. These perceptions are recorded graphically in the form of a mental map that shows concepts and relationships between

concepts (Sheetz *et al*., 1994). The tool that will be used is Decision Explorer (© Banxia.com). Each individual interview will be transformed in an individual cognitive map, and all individual cognitive maps will be combined into an aggregated cognitive map representing the way operational risk concerning Incident Management is perceived.

Phase IV – Workshop

The aggregated cognitive map will be the starting point for this Phase 4 workshop for which the authors will be acting as facilitators. The purpose of the workshop is to decide on the risk identification, risk assessment and risk control measures. The result will be an advice - for which there is a shared ownership - to senior management on how to manage risks concerning Incident Management.

The software to be used will be GroupSystems (© GroupSupport.com), which is a facilitator driven group decision support system (GDSS) that can be used to carry out a variety of strategic management and decision making processes effectively and with high levels of group participation, ownership and commitment. A key benefit of using this GDSS can be a more efficient use of meeting time, through the ability to surface and 'parallel process' more contributions from a greater number of participants than is possible using manual facilitation techniques alone. The individual participants are able to anonymously enter their ideas on their personal computers which are all connected by means of a local area network to a central computer, from which the output is projected on a publicly visible space using a data projector. The GroupSystems tool will be used to rank the identified risks by exploring and making explicit individual and group preferences. The advantage of anonymous data entry by the individual group members is that sensitive issues can be more easily brought into the open and discussed objectively without fear of reprisal.

Phase V – Analysis of the research outcomes of the previous phases

Experience will be gained from the outcomes of the previous phases in terms of the reliability-flexibility issue. A tentative conclusion on the basis of the available data will be directive for the conduct of broader questionnaire and observation protocol. In addition, we will analyse team research literature, as an organization's initial crisis response is usually provided by crisis response teams (Bigley *et al*., 2001). The composition, tasks and functioning of such teams has been actively discussed in recent literature (Rasker, 2002). Of particular interest is the phenomenon of 'threat rigidity', i.e., the behavior of groups to rigidly 'stick to the book' rather than developing flexible approaches to unforeseen events.

Phase VI – Field survey

This theoretical research will be followed by field observations of 'real' crisis response and management teams as they train for responding to a crisis. In particular, we will study the practices of such teams as they deal with (simulated) crises by conducting semi-structured interviews and recording observations. The focus of our observations and interviews will be on factors that may affect (i.e. contribute or prevent) team reliability. For example, a recent field study reported on the importance of learning and trust in trauma resuscitation teams (Xiao *et al*., 2001). As learning and trust are core components of Knowledge Management (KM), we will also investigate the possible contribution of KM to increase our understanding of high reliability team response.

Phase VII – Laboratory experiment

The results of our field study will be used for developing a laboratory experiment to isolate and validate a limited number of key factors that may contribute to reliable team responses. The experiment will have a factorial design, based on the selected reliability factors. Subjects will be students at the authors' respective institutions, who will be assigned in teams, responding to a crisis scenario and distributed according to the conditions defined for the experiment.

CONCLUSION

Preliminary field observations as well as literature on HRT, show that the hypothesis of a cross-fertilisation between ISCRAM and IT Governance can be formulated. On the one hand, mainstream methodologies like ITIL show great resemblance with the way Incident Management in Crisis Management Organisations is dealt with. On the other hand, we believe there is a similarity between the characteristics of HROs and mainstream organisations, meaning that the lessons learned can be transposed. The validation of this double hypothesis will be the subject of our future research.

REFERENCES

1. Ackermann, F., Eden, C. and Cropper, S. (2004) Getting Started with Cognitive Mapping. www.phrontis.com
2. Barnett, C and Pratt, M. (2000) From threat-rigidity to flexibility: Toward a learning model of autogenic crisis in organizations, Journal of Organizational Change Management, 13, 1, 74-88.
3. Bigley, G. and Roberts, K. (2001) The Incident Command System: High Reliability Organizing for Complex and Volatile Task Environments, Academy of Management Journal, 44, 6, 1281-2000.

4. Chorafas, D. (2004) Operational risk control with Basel II: Basic principles and capital requirements, Elsevier.
5. Courpasson, D. (2000) Managerial Strategies of Domination: Power in Soft Bureaucracies, Organization Studies, 21, 1, 141-161.
6. Düpow, H. and Blount, G. (1997) A review of reliability prediction, Aircraft Engineering and Aerospace Technology, 69, 4, 356-362.
7. Geer, D. (2004) Basel II – Being Security Conscious. http://www.itsecurity.com/papers/stake1.htm.
8. Grabowski, M. and Roberts, K. (1997) Risk Mitigation in Large Scale Systems: Lessons from High Reliability Organizations, California Management Review, 39, 4, 152-162.
9. Gray, H. (2004) Is there a relationship between IT governance and corporate governance?: What improvements (if any) would IT governance bring to the LSC?
10. Janis, I. Groupthink, A First Look at Communication Theory (Em Griffin)
11. Luo Carlo, J., Lyytinen, K. and Boland, R.(2004) Systemic Risk, IT Artifacts, and High Reliability Organizations: A Case of Constructing a Radical Architecture, Sprouts: Working Papers on Information Environments, Systems and Organizations, 4, Article 4.
12. Mahinda, E. and Whitworth, B.(2004) Evaluating Flexibility and Reliability in Emergency Response Information Systems, Proceedings of ISCRAM2004 (Eds. B. Carle and B. Van de Walle), 93-98.
13. Mayer, A. (2004) Preparing for Basel II by Optimizing Sarbanes-Oxley, Journal of Bank Cost & Management Accounting, 16, 3, 27-33.
14. McLucas, A. (2003) Decision Making: Risk Management, Systems Thinking and Situation Awareness, Argos Press.
15. Nathan, M. (2004) How past becomes prologue: A sensemaking interpretation of the hindsight-foresight relationship given the circumstances of crisis, Futures, 36, 181-199.
16. Rasker, P. (2002) Communication and Performance in teams. Ph D. Thesis, Universiteit van Amsterdam.
17. Rijpma, J. (1997) Complexity, Tight-Coupling and Reliability: Connecting Normal Accidents Theory and High Reliability Theory, Journal of Contingencies and Crisis Management, 5, 1, 15-23.
18. Roberts, K. (1990) Managing High Reliability Organizations, California Management Review, Summer, 101-113.
19. Rochlin, G. (1996) Reliable Organizations, Present Research and Future Directions, Journal of Contingencies and Crisis Management, 4, 2, 55-59.
20. Rutkowski, A-F, Van de Walle, B. and van Groenendaal, W. (2005) When Stakeholders Perceive Threats and Risks Differently: The Use of Group Support Systems to Develop a Common Understanding and a Shared Response, *Journal of Homeland Security and Emergency Management*, 2, 1.
21. Rutkowski, A-F, van Groenendaal, W. and Van de Walle, B. (2004) Decision Support Technology to Support Risk Analysis and Disaster Recovery Plan Formulation: Towards IT and Business Continuity, Proceedings of ISCRAM2004 (Eds. B. Carle and B. Van de Walle), 3&4/5, 127-132.
22. Sheetz, S., Tegarden, D. and Kozar, K. (1994) A group support systems approach to cognitive mapping, Journal of Management Information Systems, 11, 1, 31-57.
23. Thiadens, T. and Spanjersberg, H. (2000) Beheerst beheren: Beheer van ICT voorzieningen uit managementoptiek.
24. Van Den Eede, G., Kenis, D. and Van De Walle, B. (2004) Combining Flexibility and Reliability for Mainstream Organisational Learning, *Proceedings of the 5th European Conference on Knowledge Management*, 851-860.
25. van Fenema, P. (2003) Collaborative Elasticity and Breakdowns in High Reliability Organizations: Contributions from Distributed Cognition and Collective Mind Theory, CSAPC 03 Workshop, Amsterdam, 16/11/2003.
26. Vogus, T. and WELBOURNE, T. (2003) Structuring for high reliability: HR practices and mindful processes in reliability-seeking organizations, Journal of Organizational Behavior, 24, 877–903.
27. Weick, K. (1987) Organizational Culture as a Source of High Reliability, California Management Review, 29, 2, 112-127.
28. Wishart, N. and Elam, J. (1996) Redrawing the Portrait of a Learning Organization, Academy of Management Executive, 10, 1, 7-20.
29. Xiao, Y. and Moss, J. (2004) Practices of High Reliability Teams: observations in Trauma Resuscitation, http://hfrp.umm.edu/coordination/Xiao%20Moss%20hfes%202001-camera%20ready.pdf.