

---

# From Information Security Management to Enterprise Risk Management

Margareth Stoll

---

## Abstract

Organizations are faced with increasing complexity, uncertainty and enhanced threats from a wide range of forces. Depending on how this situation is handled, it can become risk or opportunity to erode or enhance business value. In addition, organizations have to meet most different stakeholders', legal and regulatory risk management requirements. Thus, comprehensive enterprise risk management has become key challenge and core competence for organizations' sustainable success. Given the central role of information security management and the common goals with enterprise risk management, organizations need guidance how to extend information security management in order to fulfill enterprise risk management requirements. Yet, interdisciplinary security research at the organizational level is still missing. Accordingly, we propose a systemic framework, which guides organizations to promote enterprise risk management starting from information security management. The results of our case studies in different small and medium-sized organizations suggest that the framework was useful to promote enterprise risk management in an effective, efficient, cost-effective and sustainable way. New insights for practice and future research are offered.

---

## Keywords

Information security management • Risk management • Enterprise risk management • Framework • ISO 27000 • ISO 31000 • COSO

---

## Introduction

### Starting Situation

Uncertainty and risks are growing due to increased dynamic, complex and interrelated economy and enhanced threats from a wide range of forces, such as financial instability, political movements and terrorism, societal requirements, extreme nature events due to climate change, product recalls over more levels of the supply chain, pandemics, technical failures, frauds, espionage, sabotage, cyber-attacks and

others. In the last years there were different low-probability and high-impact events, Black Swan events [1], which are almost impossible to forecast (e.g., drought, earthquake, floods, cyber-attacks). Depending on how uncertainty is handled, it can become opportunity or threat [2]. Thus, organizations have to meet most different stakeholders' risk management requirements to promote trust and long-term organizations' success. More and more organizations are reducing their business risks by seeking assurance that their supplier and partners are properly managing their risks. In the last years the number of certificates for information security management accordingly ISO/IEC 27001, for example, was growing worldwide over 20 % per year and for food safety accordingly ISO 22000 more than 34 % [3]. Since more than 10 years regulatory and legal authorities require increased corporate responsibility [4] with a broad

---

M. Stoll (✉)  
University of Innsbruck, Technikerstr. 21a, 6020 Innsbruck,  
Tyrol, Austria  
e-mail: [margareth.stoll@uibk.ac.at](mailto:margareth.stoll@uibk.ac.at)

focus on most different risks [5] (e.g., Sarbanes-Oxley Act (SOX), SEC Rule 33-9089, the King Reports in South Africa, the EU company directives [6] and national laws [7]). The major ratings agencies have integrated enterprise risk management into their financial reviews and company ratings [8, 9].

Thus enterprise risk management—the generic, systemic approach to identify and manage all the risks facing an organization related to their strategic objectives—has become key challenge and opportunity for modern organizations. It is a key differentiator for competitive advantages and sustainable organizations’ success (cf. [10–12]). Enterprise risk management is a new topic overall for nonfinancial companies [2]. It has become core topic in management accounting. Nevertheless, many organizations treat enterprise risk management as compliance exercises and hinder their performance and flexibility [13]. Effective and coherent managed uncertainty across the whole organization enhances risk information and awareness [8], decreases uncertainty (e.g. stock price volatility [9]), reduces expected costs of external capital [14], facilitates informed decisions [4] and resource allocation [8], promotes performance in business operations [8, 15], ensures accountability, transparency and governance [4] and improves strategic planning, reputation and organizations’ value [8–10].

## Purpose of the Article

Traditionally, organizations managed risks in “silos” [9, 16], such as finance, market, compliance, regulation, infrastructure security, product safety, quality, health and safety, reliability and capacity of the production or service, global supply chain and logistics, litigation, governance, information security, environmental impacts, human resources, intellectual property rights, innovation and others. But risks interrelate in a cybernetic way (e.g. necessary health data to reduce safety risks or economic information to reduce financial risks can be critical for data protection). Recently organizations adopt more comprehensive approaches and aggregate the results of the different risk assessments into an organization-wide risk profile [17]. The Committee of Sponsoring Organizations (COSO) of the Treadway Commission and the International Standard Organization by ISO 31000 issued generic frameworks for enterprise risk management. Apart from larger organizations in sectors with tradition in risk assessment (e.g., banking, assurance), enterprise risk management is still in the early stages of development and implementation [4, 18].

Given the central role of knowledge, information and supporting technologies, information security—the availability of all essential assets, confidentiality, data integrity and legal/regulatory compliance—is one of the most

important challenges for today’s organizations [19]. At the end of 2010 more than 15,600 organizations worldwide were implementing information security management and obtained certification accordingly ISO 27001 [3]. Several best practices (e.g., COBIT, ITIL) and national guidelines (e.g., NIST 800-53, German IT Security Guidelines) for information security management are widely used in practice. Despite the common goals of information security and enterprise risk management, they provide no guidance to promote enterprise risk management by information security management. Accordingly Ashby’s Law of Requisite Variety [20] the given complexity and dynamic requires a systemic approach. Thus, organizations need a meta-model, which integrates the different parts to a whole. This offers great advantages to identify those areas where efforts return most value. Since some years there are calls for more interdisciplinary security research [21, 22] and for studies at the group and organizational level [21]. Despite these, we found no systemic framework for extending information security management to enterprise risk management.

## Research Question and Approach

How can we extend information security management accordingly IEC/ISO 27001 to fulfill enterprise-specific stakeholders’, business and legal/regulatory enterprise risk management requirements? We expect, that our systemic framework guides organizations to promote enterprise risk management by security management in an effective, efficient/cost-effective and sustainable way. The framework was implemented and tested in different small and medium-sized organizations. The case study results were collected by established process and system measurement methods and by interviewing managers and collaborators.

## Structure of the Article

Firstly we review previous approaches, describe the requirements for enterprise risk management (section “[Previous Research and Requirements for Enterprise Risk Management](#)”) and present the core requirements of information security management accordingly ISO/IEC 27001 (section “[Core Requirements of Information Security Management Systems](#)”). Our integrated framework for enterprise risk management based on information security management (section “[Integrated Framework](#)”) and its implementation (section “[Implementation](#)”) are presented. We report about the case study results in different small and medium-sized organizations (section “[Project Experiences and Results](#)”) with the achievement of project objectives (section “[Achieving the Project Objectives](#)”) and discuss obtained findings,

limitations and implications for practice and research (section “[Findings, Limitations and Implications](#)”). We conclude by summarizing our experiences (section “[Conclusion](#)”).

---

## Previous Research and Requirements

### Previous Research and Requirements for Enterprise Risk Management

For a long time, information security was seen as a technical job and an integral part of the IT department [23]. Corresponding frameworks start at the process level and go down through all technical levels accordingly an IT enterprise architecture approach (e.g., [24–26]). But there are huge potential threats and organizations need to invest security efforts effectively. Governance oriented frameworks integrate or align the security strategy to the organizational and IT strategy and deduce policies, standards and procedures for the tactical and operational level. Operational measurement data are reported back to middle and top management (e.g., [27–29]). Due to the great impact of human-caused incidents recently a lot of research regards people-oriented issues, such as awareness, policy compliance, trust and others (cf. [21, 22]). Several best practices (e.g., COBIT, ITIL) and national guidelines (e.g., NIST 800-53, German IT Security Guidelines) are widely used in practice.

COSO provides a strategic-aligned, generic framework, which requires to: align risk appetite and strategy, enhance risk response decisions, reduce operational surprises and losses, identify and manage multiple and cross company risks, seize opportunities and improve the deployment of capital [30]. ISO 31000 provides principles, a framework and a process for managing risks [11].

Based on research results, COSO and ISO 31000 the main success factors of enterprise risk management are to create value, be committed by board management, become integral part of all organizational processes and decision making, address explicitly uncertainty, be systematic, structured and timely, base on best available information, be tailored to the organizations’ specific context, take into account human and cultural factors, be transparent and inclusive, respond to changes in a dynamic, iterative and responsive way and facilitate the continual improvement of the organization [8, 11, 18, 30]. Organizations typically concentrate on managing known risks, which prevent them from seeing new risks [31]. Thus, the continual communication and consulting with internal and external stakeholders and the ongoing monitoring and improvement are essential success factors [11, 18, 30]. Enterprise risk management requires an interdisciplinary risk management team with collaborators of all levels [4, 11, 18, 30]. Insider threats (such as theft, fraud, violation of intellectual property) have caused the majority

of economic losses and they are still growing [32]. Tools, processes, methods, technology and risk culture must be optimally harmonized, aligned with corporate objectives and continually improved [11, 30–34].

### Core Requirements of Information Security Management Systems

The ISO/IEC 27001 family for information security management requires following core principles [35]:

- The defined corporate security policy regards legal/regulatory requirements and is approved by the management.
- A risk assessment must be conducted to establish the risk treatment plan in order to reduce risks to acceptable levels of risk. For the identified remaining risks the business continuity plan must be developed, implemented, maintained, tested and updated regularly.
- The needed resources must be determined and provided. All collaborators must be competent to perform their tasks. They must be aware of their activities’ security impact and how they can contribute to achieve established objectives.
- The effectiveness, adequacy and compliance of the management system must be continually improved using measurements, monitoring, audits, management reviews and by applying corrective and preventive actions in sense of a PDCA (plan, do, check, act) cycle.

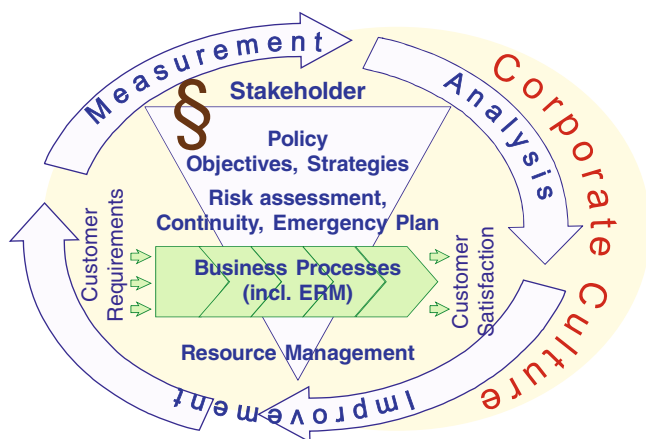
The management system must be systematically documented, communicated, implemented and continually improved.

---

## Integrated Framework

Based on previous research, the requirements of enterprise risk management and the presented core requirements of ISO/IEC 27001 (see section “[Previous Research and Requirements](#)”) we developed an integrated framework in order to fulfill enterprise-specific stakeholders’, business and legal/regulatory enterprise risk management requirements by extending information security management:

- The security policy is extended by risk management aspects to an integrated corporate policy (see top of Fig. 1). Thereby the requirements of all stakeholders, as well as legal and regulatory requirements are regarded. Appropriate corporate risk objectives and strategies are established.
- Risk assessments are conducted to establish the risk treatment plan in order to reduce risks to acceptable levels of risk. For the identified remaining risks, potential emergency situations and accidents business continuity and emergency plans accordingly adequate standards, such



**Fig. 1** The integrated framework

as ISO 22320 and ISO 22301 are developed (see the text under the top of Fig. 1).

- For all business processes risk objectives are deduced from corporate objectives by regarding business, legal and regulatory requirements and contractual obligations, specific conditions, uncertainties, threats, infrastructures and supporting services or technologies. The processes are analyzed and optimized accordingly these objectives (see middle of Fig. 1: main business processes start from the first contact with the customers and their requirements and end with the delivery of the products/services and the satisfaction of the customers). Thereby the identified risk treatments, business continuity and emergency plans are suitably integrated into the operational processes. They are implemented, maintained, tested and updated regularly to ensure effectiveness. The process description establishes for all process steps the associated responsible and accountable function and relevant risk management requirements. Thus, clear and traceable roles and responsibilities are assigned.
- The resource management deduces specific competence objectives from corporate and process objectives for all organizational functions and partners of the supply chain. Appropriate trainings or other actions are taken to achieve and maintain these objectives. Their effectiveness is evaluated. In that way the collaborators' awareness for risk management is constantly identified and improved. The organization defines, plans and provides the necessary resources, tools and instruments to obtain and improve the established objectives (see bottom of Fig. 1).
- The effectiveness and adequacy of the established enterprise risk management and the achievement of the objectives are evaluated periodically by suitable methods for monitoring and measurement (see the circle in Fig. 1). It is improved continually in accordance to established processes in sense of a PDCA cycle.

- A main success factor for enterprise risk management is adequate risk awareness of all collaborators and partners. Risk management must become part of corporate culture (see right of Fig. 1).

## Implementation

### Policy, Objectives and Strategies

Starting from internal and external stakeholders' and legal/regulatory requirements, key drivers and trends, contractual obligations, the characteristics of the business, the organization with its values, beliefs, ethic, culture, capabilities, capital, people, structures, its environment (culture, politic, finance, economic, nature, market and competition), resources, assets/ technology and all other particulars and requirements we extend based on Quality Function Deployment [36] the information security policy to the comprehensive corporate policy including risk aspects. The policy is elaborated with all key decision makers, stakeholders' representatives, if possible, and depending on the corporate culture preferably with collaborators of all levels and functions in an interdisciplinary approach. Based on the balanced scorecard [37] we define the priorities for conflicting interests and deduce enterprise risk management objectives and strategies from corporate policy. Depending on the size of the organization, we restrict the scope of enterprise risk management and define necessary boundaries. By establishing the policy, objectives and strategies we consider especially uncertainty and societal, legal/regulatory risks and requirements for all markets. Thus the entire organization is focused on enterprise-specific stakeholders', business and legal/regulatory enterprise risk management objectives.

### Risk Assessment, Risk Treatment and Business Continuity Plan

Risk assessments for all relevant risk categories are conducted to establish risk treatment plans in order to reduce risks to acceptable levels of risk. Based on the established corporate policy we define the required risk criteria and risk levels for all relevant different sources of risk. After we identify for the specific organization the potential threats and risks for achieving established objectives, the likelihood of events, the areas and impacts of this events, the controls currently implemented, estimate the levels of remaining risks regarding the implemented controls (required level \* likelihood \* impacts) and elaborate for the remaining higher risks adequate risk treatments. Thereby we apply a systemic

approach and regard the risks' interrelations. The board management approves whether the risks are acceptable or further risk treatments are to propose. For the established risk treatments control objectives and controls are selected and approved. Based on scenario analysis we define low-probable and high-impact events, the black swans. For the black swans and the identified remaining risks integrated business continuity and emergency plans are developed accordingly ISO 22320 and ISO 22301.

### Process Analysis and Process Improvement

The management process, all business processes including supporting processes, resources processes and optimization processes are analyzed bottom up by interviewing the concerned collaborators. Based on process reengineering [38] all processes are optimized to meet deduced strategic-aligned risk objectives, as well as process-specific enterprise risk management requirements and uncertainties. In that way enterprise risk management is coherently and effectively integrated into all processes. The established measures from the risk treatment and business continuity/emergency plans are suitably integrated into relevant operational processes. We integrate, for example, appropriate risk assessments in sales processes and suppliers' selection, adequate health and safety and environmental measures into information security controls, recurring maintenance programs and plans into technical and infrastructure services. In that way we regard enterprise risk management by the development or change of products/services, processes, procedures, regulations, organizational structure, infrastructures, sites, supply chain, logistics, markets and others. Thus risk treatments, continuity and emergency measures are implemented, maintained and updated regularly to ensure that they are effective. Their efficacy following incidents or critical accidents is periodically tested. Function profiles and required competences are deduced from the established roles to the different functions at the single process steps. In that way clear and traceable roles and responsibilities are assigned to all collaborators and partners.

### Resource Management

The organization determines and provides and improves necessary resources, infrastructures, tools and instruments to meet the established enterprise risk management objectives. Appropriate infrastructures and resources promote ongoing adequate enterprise risk management for long-term organizations' success. Training and competence objectives are planned and implemented in accordance to the defined human resource processes. Thus the risk awareness

and necessary competences of all collaborators and partners are promoted systematically and structured. The effectiveness is evaluated and when necessary, corrective actions are taken.

### Corporate Culture

It is important to understand the culture of the organization, which influences profoundly employees' behavior [39]. We need an organizational culture that encourages employees to take ownership of risks and weight their potential rewards and hazards [32, 34]. Executives are responsible or have great impact for communicating the right risk culture [40]. They must lead by example and have to encourage/evaluate the collaborators and partners in following these principles. The extensive research for an adequate information security culture (cf. [21, 22]) provides guidance.

### Continually Improvement

The achievement of deduced process's risk objectives is controlled by measurement methods and targets. When they are not achieved, corrective and eventually preventive actions are taken. Accordingly ISO/IEC 27001 all corrective actions, improvements or changes are elaborated by the interdisciplinary risk team. They are documented, approved, communicated, implemented and their effectiveness is evaluated. Collaborators' ideas, the results of periodically internal and external audits and stakeholders' feedbacks provide further improvements. Thus enterprise risk management is constantly evaluated and when necessary adjusted and improved.

### System Documentation

In accordance to ISO/IEC 27001 the established corporate policy, objectives, strategies, processes, risk assessment and risk treatment plan, business continuity/emergency plan, function profiles, templates, checklists, policies, procedures and others are documented and communicated traceably to concerned collaborators/partners in order to become part of corporate culture (see section "[Corporate Culture](#)").

---

### Project Experiences and Results

The integrated framework for enterprise risk management based on information security management (ISM) was implemented in different small and medium sized organizations (from 25 to 200 collaborators). To summarize,



the integrated framework was easy to understand and adaptable for organizations' specific requirements. It was useful and appreciated by all organizations to meet in common enterprise-specific stakeholders', business and legal/regulatory enterprise risk management requirements.

## Achieving the Project Objectives

The following case study results were collected by established process and system measurement methods and by interviewing managers and collaborators [38, 41]:

- **Effectiveness:** the fulfilment of established objectives is periodically controlled by defined measurement methods. When necessary, appropriate corrective/ preventive actions are implemented and their effectiveness controlled. The organizations met their planned objectives in average more than 92 %. The risk of non-payment, for example, could be reduced constantly over 6 years from 0.8 to 0.4 %.
- **Efficiency and cost reduction:** Integrating enterprise risk management into existing ISM uses synergies and reduces the efforts and costs about 10–20 %. The advantages are still higher during implementation, when additionally only the risk assessment is continually adopted and improved.
- **Sustainable enterprise risk management:** The strategic-aligned, tight integration of enterprise risk management into all programs, projects and measures, the collaborators' involvement and the continual controlling of the objectives' accomplishment enhances sustainable risk management. In addition it is ongoing promoted by the ideas, optimizations and suggestions of the collaborators and further structured, systematic improvements (see section "[Continually Improvement](#)"). The awareness for risks and opportunities was ongoing maintained. Potential opportunities are recognized early and transformed to competitive advantages for sustainable organizations' success.

## Findings, Limitations and Implications

The discussions in the cross-functional team during the extension of the ISM increased severely the risk awareness of the involved collaborators. Our case study results underline the importance of an adequate corporate culture and the essential role of executives (see section "[Corporate Culture](#)"). Due to the central role of legal/regulatory requirements and the impact of regional culture the implementation of the framework should be analyzed in other countries and multinational concerns. Further studies are needed also in large organizations.

All relevant legal and regulatory requirements are analyzed, implemented and maintained by the defined improvement processes. The reduced liability by increased legal/regulatory compliance and transparency, and the enhanced risk information for informed decisions were especially appreciated by board managers and CEOs. The collaborators appreciated the increased performance in business operations, for example by reduced outstanding payments.

The extension of ISM for enterprise risk management requires a suitable adapted security management. It must be ongoing and effectively implemented. Due to continual changing of the internal and external context an effectively, strong strategic-aligned implementation and the continual improvement are essential success factors.

Extending and concurrently simplifying processes, risk measurement/controlling (consistent with Gates et al. [8]) and overall maintaining ongoing risk awareness were great challenges for the organizations. Based on the results from the literature research and these challenges we call for more interdisciplinary, systemic information security and enterprise risk management research in most different directions. This integrated framework can be used as meta-model to structure the research streams and to promote interdisciplinary research at the organizational and inter-organizational level.

While Delarosa [42] describes the large efforts for enterprise risk management, our integrated, systemic framework uses synergies to introduce enterprise risk management efficiently, resources carefully and promptly. In addition, it can be implemented successively by integrating ongoing more risk disciplines. Thus, it provides an optimal enterprise risk management approach, overall for small and medium-sized organizations.

Sufficient and appropriate resources (e.g., personnel resources, infrastructures) and technology (e.g., production systems, technical equipment, IT systems) are important success factors to maintain ongoing the risk level accordingly established risk objectives in order to convert uncertainty into opportunities for long-term organizations' success.

This integrated, systemic comprehensive risk management framework requires from the information security manager profound risk assessment skills and basic understanding in the different other risk disciplines and corresponding legal/regulatory requirements. Teaching and trainings should regard these comprehensive competences' requirements.

Due to the excellent project experiences organizations should extend enhanced security management to enterprise risk management in accordance to this integrated framework in order to fulfill enterprise-specific stakeholders', business and legal/regulatory risk requirements for sustainable organizations' success.

## Conclusion

Due to increased complexity, uncertainty and threats from a wide range of sources and enhanced stakeholders' and legal/regulatory requirements enterprise risk management has become key challenge and core competence for organizations' sustainable success. Based on our case studies' results the systemic framework guides organizations to enhance enterprise risk management starting from information security management in an effective, efficient, cost-effective and sustainable way. Thus, it offers great opportunities, overall for small and medium-sized organizations, operating in innovative, volatile markets with high strategic, financial, operational and technical risks. We call for more interdisciplinary information security and risk management research in most different directions and at all organizational and interorganizational levels.

**Acknowledgment** The research leading to these results was partially funded by the Tyrolean business development agency through the Stiftungsassistentz QE—Lab.

## References

1. N. Taleb, *The Black Swan, The Impact of the Highly Improbable*, Random House, New York, 2007.
2. M. Power, *Organized Uncertainty*. Oxford University Press, New York, NY 2007.
3. International Standard Organization (ISO). ISO Survey of Certifications 2010, <http://www.iso.org/iso/iso-survey2010.pdf>.
4. I. Brown, A. Steen and J. Foreman, "Risk management in corporate governance: A review and proposal," *Corporate Governance: An International Review*, vol. 17, no. 5, pp. 546-558 2009.
5. B. Windram and J. Song, "Non-executive directors and the changing nature of audit committees," *Corporate Ownership and Control*, vol. 1, pp. 108-115, 2004.
6. European Commission. "Company laws", [http://ec.europa.eu/internal\\_market/company/official/index\\_en.html](http://ec.europa.eu/internal_market/company/official/index_en.html).
7. Corporate Law and Governance, "Corporate Law and Governance", <http://corporatelawandgovernance.blogspot.it/>.
8. S. Gates, J. Nicolas and P.L. Walker, "Enterprise risk management: A process for enhanced management and improved performance," *Management Accounting Quarterly*, vol. 13, no. 3, pp. 28-38 2012.
9. R.E. Hoyt and A.P. Liebenberg, "The value of enterprise risk management," *Journal of Risk & Insurance*, vol. 78, no. 4, pp. 795-822 2011.
10. V. Arnold, T.S. Benford, C. Hampton and S.G. Sutton, "Enterprise risk management as a strategic governance mechanism in B2B-enabled transnational supply chains," *J.Inf.Syst.*, vol. 26, no. 1, pp. 51-76 2012.
11. International Standard Organization (ISO), ISO 31000:2009, *Risk management - Principles and Guidelines*, 2009.
12. N. Taleb, D. Goldstein and M. Spitznagel, "The Six Mistakes Executives Make in Risk Management", *Harvard Business Review*, vol. 87, pp. 78-81, Oct2009.
13. S.G. Sutton, V. Arnold, T. Benford and J. Canada, *Why Enterprise Risk Management is Vital: Learning from Company Experiences with Sarbanes-Oxley Section 404 Compliance*, Altamonte Springs, FL: Institute of Internal Auditors Research Foundation, 2009.
14. L.K. Meulbroek "Integrated Risk Management for the Firm", *Journal of Applied Corporate Finance*, vol. 14, pp. 56-70, 2002.
15. P.M. Collier, *Fundamentals of Risk Management for Accountants and Managers*, Elsevier, 2009.
16. M.K. McShane, A. Nair and E. Rustambekov, "Does enterprise risk management increase firm value?" *Journal of Accounting, Auditing & Finance*, vol. 26, no. 4, pp. 641-658 2011.
17. D. Espersen, "Trends in enterprise risk management, Risk management. Bank Accounting and Finance, December: 45-50, 2002
18. C. McDonald, "Few firms see themselves as 'advanced' on use of enterprise risk management," *National Underwriter / P&C*, vol. 114, no. 15, pp. 25-25 2010.
19. Ernst & Young. "Into the cloud, out of the fog, Ernst & Young's 2011 Global Information Security Survey" <http://www.ey.com/Publication>.
20. W.R. Ashby, *Introduction to Cybernetics*. Methuen, London, 1956.
21. F. Bélanger and R.E. Crossler, "Privacy in the digital age," *MIS Quarterly*, vol. 35, no. 4, pp. 1017-A36 2011.
22. P.A. Pavlou, "State of the information privacy literature : Where are we now and where should we go?" *MIS Quarterly*, vol. 35, no. 4, pp. 977-988 2011.
23. G. Dhillon and J. Backhouse, "Current directions in IS security research" *Information Systems Journal*, vol. 11, no. 2, pp. 127-153 2001.
24. A.R. McGee, S.R. Vasireddy, S.R. Chen Xie, D.D. Picklesimer, U. Chandrashekhar and S.H. Richman, "A framework for ensuring network security," *Bell Labs Technical Journal*, vol. 8, no. 4, pp. 7-27 2004.
25. J. Sherwood, A. Clark and D. Lynas, *Enterprise security architecture : a business-driven approach*. San Francisco: CMP Books, 2005.
26. D. Trèek, "An integral framework for information systems security management," *Comput.Secur.*, vol. 22, no. 4, pp. 337-360 2003.
27. A. Da Veiga and J.H.P. Eloff, "An information security governance framework," *Inf.Syst.Manage.*, vol. 24, no. 4, pp. 361-372 2007.
28. S. Sowa, L. Tsinas and R. Gabriel, "BORIS -Business ORiented management of Information Security" in *Managing Information Risk and the Economics of Security*, E.M. Johnson, Ed. New York, NY: Springer US, 2009, pp. 81-97.
29. S.H. von Solms and R.v. Solms, *Information security governance*. New York, NY: Springer, 2009.
30. Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management - Integrated Framework*, AICPA, New York, NY, 2009.
31. J. Rosenoer and W. Scherlis, "Risk Gone Wild", *Harvard Business Review*, vol. 87, pp. 26, May2009.
32. G. Campbell, R. Lefler, *Security Alert*, *Harvard Business Review*, vol. 87, pp. 104-105, Jul/Aug2009
33. T. Bishop and F. Hydoski, "Mapping your fraud risks", *Harvard Business Review*, vol. 87, pp. 76, Oct2009.
34. R. Kaplan, A. Mikes, R. Simons, P. Tufano and M. Hofmann, "Managing risk in the new world", *Harvard Business Review*, vol. 87, pp. 69-75, Oct2009.
35. ISO/IEC27001, ISO/IEC 27001:2005, *Information Technology, Security techniques, Information security management systems requirements*. Geneva: International Standard Organization, 2005.
36. Y. Akao, *Quality Function Deployment, integrating customer requirements into product design*, Productivity Press, Portland, 1990.
37. R. Kaplan and D. Norton, *The balanced scorecard, translating strategy into action*, Harvard Business School Press, Boston, 2008.
38. T.H. Davenport, *Process innovation*. Boston, Mass: Harvard Business School Press, 1993.

- 
39. B. Bulgurcu, H. Cavusoglu and I. Benbasat, "Information security policy compliance" *MIS Quarterly*, vol. 34, no. 3, pp. 523–A7 2010.
40. D.W. Straub and R.J. Welke, "Coping with systems risk: Security planning models for management decision making," *MIS Quarterly*, vol. 22, no. 4, pp. 441–469 1998.
41. G. Walsham, "Doing interpretive research," *European Journal of Information Systems*, vol. 15, no. 3, pp. 320–330 2006.
42. DelS. Delarosa, Cultivating the best board, *Internal Auditor*, August, pp. 69–75, 2006



Innovations and Advances in Computing, Informatics,  
Systems Sciences, Networking and Engineering

Sobh, T.; Elleithy, K. (Eds.)

2015, XIV, 629 p. 400 illus., 188 illus. in color.,

Hardcover

ISBN: 978-3-319-06772-8