After Information Security – Before a Paradigm Change (A Complex Enterprise Security Model)

Pál Michelberger Jr.

Óbuda University, Keleti Károly Faculty of Business and Management, Institute of Management and Organisation, Népszínház u. 8, H-1081 Budapest, Hungary
e-mail: michelberger.pal@kgk.uni-obuda.hu

Csaba Lábodi

QLCS Kft., Cholnoky J. u. 1/a, H-8200 Veszprém, Hungary
e-mail: csaba.labodi@gmail.hu

Abstract: Security management for business enterprises is currently undergoing major changes. Instead of the separate regulation of distinct areas (guarding infrastructure, work safety, security technology, information security, etc.) there is an emerging holistic approach based on new management methods and company culture. Partly as a result of existing traditions, the professional business background to the implementation of these changes is rather fragmented and may not yet exist at all. Our survey calls attention to a new opportunity. In our opinion the expected level of company security and business continuity may be reached departing from information security-related international standards and recommendations, by business risk analysis and compliance with a wide range of security expectations.

Keywords: information security; risk analysis; business continuity; process security; enterprise security model

Introduction

The spread of standardised information security management systems clearly attests to the rise in the demand of enterprise security [17]. Protecting information is nevertheless not a sufficient measure in itself. Maintaining reliability and satisfying business partners' demands in time, volume and quality requires much more. The tools of enterprise value generation as well as major and subordinate processes also have to be made secure. Enterprise security and disaster recovery plans and ideas, already known in connection with information security, may

serve as a good starting point for the creation of a holistic business enterprise security model. The present paper departs from the demands of the information security management system, discusses enterprise risk analysis and surveys various international security-related standards and recommendations. After summarising real-life experience, an attempt will be made to compile a complex enterprise security model that can deal with real-life threats.

Business enterprise security management is able to control the critical processes and tools of an enterprise to reach company targets derived from strategic plans. This means an uninterrupted series of planning, organisation, management and control and coordination activities that guarantee a desired and sustainable level of security for all internal and external parties of the enterprise. Instead of technical issues, the workings of the organisation system gain focus, allowing the measurement, continuous development and optimisation of security aims [2].

1 The Point of Departure: Information Security

Information is value for the enterprise, being a basis for managerial decisions and business success. It may be relevant with respect to products, services, technological know-how and available resources as well as business partners. If lacking or false, inaccurate or delivered into unauthorised hands, information may cause damage to the organisation. It must therefore be protected.

Information security is a far more complex issue than IT security. Today it is not enough to think in terms of firewalls, reliable hardware and well-defined identification systems. A conscious buildup of technological background is no longer sufficient.

The integrity, availability, and confidentiality [23] of information is primarily threatened by negligent handling or purposeful damage caused by internal employees (through company information management systems and the intranet) and strategic partners with access to company databases through the internet, extranet or Electronic Data Interchange (suppliers, retailers, cooperation partners and financial service providers).

Several other qualities, such as accuracy, accountability, non-repudiation, and dependability may also be linked to information security.

Generally, it is the handling of information and information carriers that is regulated in order to protect information property. This is independent from the form the information is presented in. Protection functions well if the information to be protected is defined, along with internal and external threats, the risks posed by these, and the regulations and means of protection [24].

The aim of information security is to ensure the continuity of business in a structured manner and mitigate damage caused by security events. Information security may be achieved by the application of protective measures, taking risks into consideration. These consist of regulations defining enterprise processes, the enterprise structure reflecting these processes, and the regulated operation of IT tools (hardware, software, telecommunications devices) appropriate to them [11].

In order to ensure the long-term operation of business organisations, the application of a system providing security is necessary (instead of means and devices that give a false sense of security).

Several interconnected dimensions or levels of security may be defined [9];

- Information technology infrastructure level (hardware, software and network protection)
- Information management level (data entry, modification, deletion, information gathering and data query)
- Conduct of affairs/Workflow level (process management, workflow)
- Organisational level (information security strategy, risk management)

The creation of n environment supportive of information security is also important, which means an accepted information security policy, clearly defined areas of responsibility, training, and the assurance of financial resources. In addition, this involves the full registration of IT devices and documentation, risk assessment (for IT devices and the challenges of the environment), and the handling of user authorisations (for access to documentation, networks, servers, workstations, application software, and the information itself). This means the assurance of business continuity and disaster recovery based on not only information security, but also on a process-centred vision [1].

The Business Continuity Plan (BCP) ensures the availability of business process backup IT resources at given times and functional levels as well as the minimalisation of damage caused by unexpected events. It is important for this document to include potential threats to the various processes, the likelihood of their occurrence, and the damage potentially resulting from the breakdown of the process. It is in the course of the so-called Business Impact Analysis (BIA) that procedures for the maintenance of operations are determined (Fig. 1).

The Disaster Recovery Plan (DRP) contains substitute solutions for the case of major damage and events resulting in the breakdown of information technology service. The aim is to facilitate the minimalisation of negative effects and the fast restoration of original circumstances at acceptable costs. This plan must also include supplementary measures and tools for the case of a limited availability or complete breakdown of resources that ensure the continuity of processes critical for the existence of the organisation. The Disaster Recovery Plan is thus usually linked to the Business Continuity Plan. Good BCPs and DRPs examine

organisational processes and consider the links and ties between these two. They contain practicable and risk-commensurate intervention orders, are known and accepted by the higher management of the organisation, and constantly undergo testing, maintenance and development.

The preparation of the business continuity and disaster recovery plans involves the surveying of all organisational processes and thus may take a long time (several months in certain cases) to introduce. An external adviser may have to be employed to process the internal interviews and systematise results. At the same time, internal experts in full knowledge of the organisation's workings are also needed to construct the complete system. This means considerable costs, both for introduction and maintenance. The education and continuous training of responsible leaders and subordinate workers must be a top priority.

In the course of the business impact analysis, the processes of the organisation are classified according to risk levels (low, medium or high priority). The Maximum Tolerable Downtime (MTD) is determined. The effects and probability of potential threats are also examined.

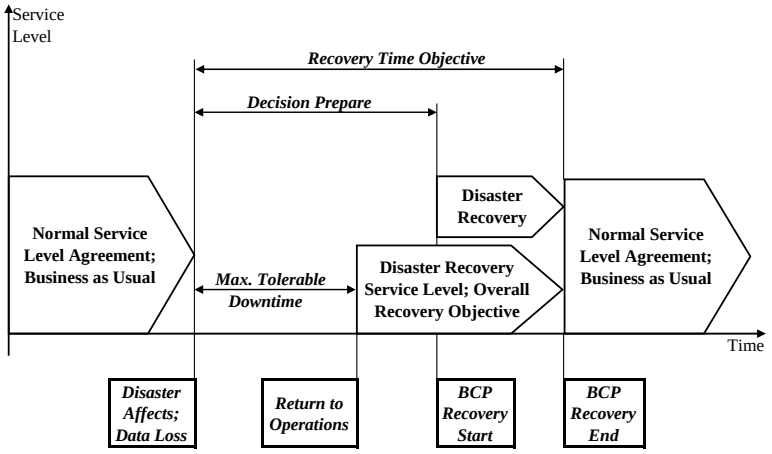

Figure 1
The Business Continuity Plan Model

2 Enterprise Risk Analysis

Risk is the potential occurrence of events or disturbances within the enterprise and in its environment (including its markets, etc.…) that endanger the fulfillment of customer demands or the security of any involved enterprise parties (stake- and stockholders).

The risk of security-related incidents may be expressed with a money/time unit quantity or, if it is not definable in this manner, with a "mark" showing the magnitude and tolerability of the risk [3]. Risk depends on the probability of harmful event occurrence as well as the resulting damage calculated in terms of finances (Fig. 2).

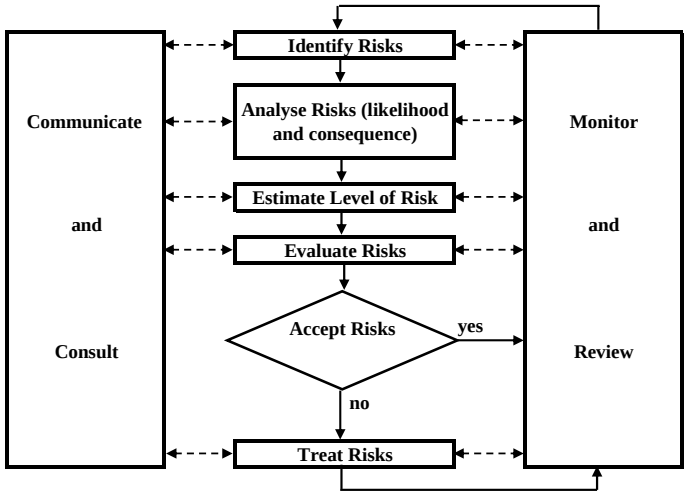

Figure 2
The process of risk management (based on Standards Australia, AS/NZS 4360 [32])

In the absence of accurately definable data related to potential risks, the umbrella term 'vulnerability' has been introduced instead of the traditional risk-centred approach. The vulnerability factors of supply chains may be classified into five groups [6], which may be complemented by two further risk sources [7]:

1) disturbances in the value-added process (manufacturing, purchasing, storage, delivery, scheduling)
2) control (non-existence or failure)
3) demand (lack of information, unpredictability, unexpected events)
4) supply (unreliability, lack of capacity, vis major)
5) environmental (economic and political events, accidents, natural disasters)

and

6) enterprise structure (if non-conformance with enterprise processes)
7) a supply or sale chain or a "network" composed of several individual companies (disturbances in communication or uncertainties in cooperation)

These seven points embrace virtually all security perspectives and thus may serve as a foundation for our security model with respect to enterprise functional risk analysis.

3 Standards and Recommendations for the Basis of Enterprise Security

There exist several internationally recognized and accepted documents in this area. We shall mention a few of these – the ones we deemed important based on our own professional perspective. Naturally, there are various other standards and recommendations that could be introduced and adapted to serve enterprise security.

Most regulations listed below are process-centred.

The joint application of standards and recommendations is no thought of evil. The structures of e.g. ISO 14001 and ISO 27001 standards are quite similar. An integrated environmental and information security management system may be created and run on these. Regulations based on the COSO enterprise risk management framework [16] may easily be introduced to a framework built on ITIL and/or CObIT [12].

3.1 ISO 14000

Enterprises may use an environment-centred standardised management system in support of their environment protection tasks in the course of their operations. Among other targets, this standard aims to lower the environmental impact resulting from enterprise operation, promote corporate image and make concerned parties interiorise environment-related behaviour patterns.

According to the standard, the environment-centred management system deals with those enterprise activities that have an impact on the environment, risk assessment, compliance with operation-related legal and other security requirements and the achievement of a still acceptable environmental impact level. The resources and capabilities for an environmentally conscious operation are defined along with forms of internal and external communication. Preparation guidelines for emergency situations, troubleshooting, controlling and prevention are also regulated. The standard does not include concrete requirements and control measures. Its implementation is primarily ethically driven with legal and economic factors gaining ground [18, 19].

3.2 BS OHSAS 18001

The main resource for enterprises is the well-trained, value-creating employee. Workplace health protection and security are effectively supported by a management system constructed according to the BS OHSAS 18001 standard [20]. Its primary aim is the definition and management of risk events that may negatively affect workers' performance or may cause an accident or health damage.

The management system handles the risks of work processes with a view toward the relevant legal environment as well as security requirements and targets characteristic for the given enterprise. It also regulates workplace health maintenance tasks. It is a valuable tool for the observation and evaluation of processes, and also for the definition of resources and capabilities necessary to maintain the management system. It prescribes the documentation and after-the-event investigation and evaluation of hazardous occurrences. Reactions to hazardous situations and corrective preventive activities are prioritised. The system standard does not prescribe concrete requirements or control methods but its application results in target-oriented and process-centred enterprise operation. By its application a further step may be taken towards the creation of a work environment that serves the better protection of human resources [21].

3.3 ISO/IEC 38500

An international standard that may also serve as a management framework, ISO/IEC 38500 of Australian origin is an aid for the intra-enterprise management of information and communication technologies [22]. Based on the document, a management cycle may be created (Fig. 3) which regulates the intratechnological support of business processes, evaluating and controlling them. Here managerial responsibility is also tackled along with information technology aspects of enterprise strategy, the acquisition of IT tools, their performance, compliance with business targets, and human behaviour.

The elements of the GRC model based on the standard are as follows

- Governance – enterprise targets, processes and the organisation running these processes, with special emphasis on IT supporting the targets;
- Risk Management – the identification of expected events and related risks, the definition of an acceptable security level for all enterprise processes and supporting IT tools (COSO ERM);
- Compliance – the enterprise must comply with internal prescriptions and laws, standards and contractual requirements.

The application of the model involves the creation of a comprehensive requirements list which is continuously adapted to changing circumstances. Management is aware of the risks as well as what expectations it has to fulfill in the given moment. This is a self-maintaining management circle which may lead to risk-based managerial decisions. It handles corporate strategy as well as financial processes and workflow, technology and employees.

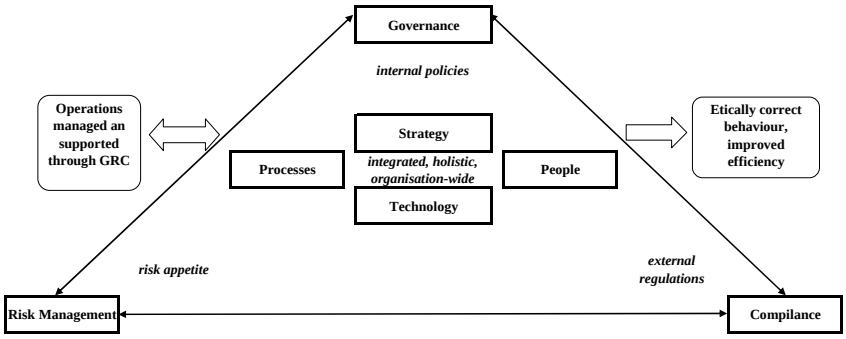

Figure 3
The GRC model [10]

3.4 ISO/IEC 27001

ISO/IEC 2700x is an information security management system or standard package of British origin providing guidance to information security activities [33]. Companies define security requirements and related measures on the basis of business objectives and organisational strategy. Information security (integrity, confidentiality, and availability) is treated with special emphasis. It is not linked to any sort of information technology. The standard (ISO/IEC 27001) [23] divides company operations and the related requirements into 11 protection areas and, within these, 39 targets and 133 protection measures. The information security management system, once it has been implemented and documented, may be accredited by an independent accreditation organisation (ISO/IEC 27002) [24]. In the standard package there appear a few supplementary sections, presented as individual standards (e.g.: ISO/IEC 27005 information security risk management standard with advice on selecting appropriate risk analysis and management tools and methods). Development never stops. There are plans for further standards (e.g.: implementation guide – ISO/IEC 27003; guidance on information security management for sector-to-sector communication – ISO/IEC 27010; information security in telecommunication – ISO/IEC 27013).

3.5 CObIT

The ISACF (Information Systems Audit and Control Foundation, IT Governance Institute, USA) has developed a recommendation entitled "CObIT" (Control Objectives for Information and related Technology) [14].

Practically, this material is a management tool which helps users to understand and handle risks and advantages connected to information and information technology. This internationally approved and developed "framework" was created primarily for business enterprises and is aimed at harmonising information technology services and the operational processes of the organisation as well as facilitating the measurability of the security and management features of information technology services.

CObIT is a collection of documents grouping best practices according to a set of criteria. In order to ensure the necessary information for the fulfillment of organisational (business) aims, information technology resources must be managed within a framework of connected procedures. With its use, we may bridge the gap between business risks, control requirements, and issues of technical nature. The system may be used by the higher management, the users, IT professionals, and the controllers of the information system at the same time. The real aim of COBIT is the achievement and maintenance of information technology security at a minimum risk and maximum profit…

Its structure is as follows:

- Executive Summary
- Framework

Control Objectives (34 processes, or process + management guidelines and maturity model + management guidelines, critical success factors, Key Goal Indicators, to define target levels of performance; and Key Performance Indicators, to measure whether an IT control process is meeting its objective) Supplements (summary overview, case studies, frequently asked questions)

The recommendation defines 34 "management" goals in connection with information technology processes, dividing them into four areas:

1 Plan and Organise,

2 Acquire and Implement,

3 Deliver and Support,

4 Monitor and Evaluate.

There are 215 specific and detailed control objectives throughout the 34 high-level IT processes.

3.6 ITIL

The ISO/IEC 20000-1, -2 standard [25, 26] was created on the basis of and in harmony with the British-developed ITIL (Information Technology Infrastructure Library), dealing with the operation issues of information systems (Fig. 3) [15]. The first part of the document is a set of formal requirements concerning acceptable information technology services, while the second part is a guide to service management and auditing according to the first part. Service management activities are connected to the currently popular PDCA model, which is applied in several standards.

In addition to the management system, the issues of planning and implementation of information technology systems, and the planning and creation of new services, there are five basic areas of complete service management:

- Service security (service level, service reporting, capacity, service continuity, availability, information security, budgeting and accounting for IT services)
- Management processes (configuration and change management)
- Release (documents, operational description distribution management, the documentation of approved modifications)
- Solution processes (incident and problem management)
- Relationship (customer service, business and supplier relationship management)

3.7 BS 25999

The British standard package concerning business continuity (BS 25999-1, -2) [27, 28] also facilitates the creation of a corporate process management system. It is applicable to all types of organisations. The assessment of potential threats and risk factors is the result of a complex impact analysis (Business Impact Analysis, BIA). The key products of the company and the steps in their manufacturing as well as service support processes-, and the maximum acceptable period of business breakdown and dependence on external business partners are examined. Based on the impact analysis the company creates a Business Continuity Plan which helps avoid problems even in case of unexpected events (natural disaster, shortage of raw materials, utility failure, labour force shortage, breakdown of technological equipment, IT problems, customer complaints, etc.). The firm retains its good reputation and is able to carry on value-added processes and maintain connections with business partners.

3.8 Supply Chain Continuity Models and Standards

According to the definition established by the US Supply Chain Council (SCOR model) [8], a supply chain comprises all activities connected to manufacturing and delivery, from the suppliers' suppliers to the final consumers. The five major processes determining the supply chain are

1 planning (supply/demand analysis and the determination of quality, quantity and scheduling factors for products or services),

2 sourcing (raw materials, spare parts and cooperational services),

3 making (the manufacturing of spare parts and assembly),

4 delivery (stockpiling, order management, distribution, and serving the final consumers),

5 returning (handling faulty or superfluous products and maintenance needs, customer service work).

Here we do not see the accumulation of discrete results reached by individual organisations within the supply chain but synergic effects are created in various domains of production due to the allocation of resources. At the same time this is also true for risks. The management of the supply chain means conscious collaboration on behalf of the companies. Its existence is accepted by the participants as a contributing factor to the improvement of their competitive position. The members of the chain are willing to sacrifice their individual, short-term advantages to facilitate the optimal operation of the whole chain. This in turn presupposes protective activities to ensure the safety of "supply" and joint risk management. Standard package ISO 28000 may be a helpful instrument of regulation here because it includes supply chain security management requirements [29, 30, 31].

For supply chains the effective operation of the whole network is more important than the optimal resource utilisation of its individual member enterprises. The widely used and highly practicable CPFR (Collaborative Planning, Forecasting and Replenishment) process model also pushes companies into this direction [13]. The basis of demand planning is the final customer demand. The application of the model results in a consensus-based forecast which will in turn determine the plans for distribution, manufacturing and purchasing, also broken down to individual members. Supply chain members try to use forecast data as accurate as possible. This works to improve supply security.

3.9 Enterprise Risk Management

The Enterprise Risk Management framework first compiled by COSO (Committee of Sponsoring Organisations of Treadway Comission) in 1992 is designed for the use by higher management and decision-makers. It focuses on the internal

processes of the enterprise, their management and control. With constant attention to business strategy, it may be applied to almost any type of risk but is mostly used in the finance area [16].

4 A New, Holistic and Process-centred Enterprise Security Model

The basis of successful enterprise operation is the conscious assumption and management of risks. Business organisations need a type of Enterprise Risk Management (ERM) which

- identifies and handles risk factors;
- encompasses the whole organisation and the surrounding environment;
- allows managers an overview of the entire risk profile;
- aids strategic and operative decision-making.

Thus the protection of enterprise (organisational) processes may be ensured and the security of processes may be reached.

Process security may be regarded as a state: if the prescribed input factors (resources needed for the completion of the process) are ensured, the organisational units involved in the process will produce the required output (product, service, or information) in the prescribed time, quantity and quality; in the case of a disturbance, the normal course of procedure is restored with minimal effort and in the acceptable minimum time [4].

The majority of standards and recommendations discussed so far are process-centred but mostly concern one individual function area within enterprises. The execution of all organisational processes requires resources, the most important of which is information provided in the appropriate time and place and to the authorised persons – information being a fundamental precondition for value-added processes. This is why the introduction of an information security management system may serve as the foundation of a security model for the whole organisation. By the regulation of workflow – or by its restoration in case of a disturbance – the security of the "virtual functioning" of the organisation may be created. A major role in enterprise functioning may be given to the job definition of persons applying a virtual enterprise model (e.g. ERP, EAM). What data may they register, modify, delete; what data queries and transactions may they initialise? Users occupy predetermined positions that incorporate security requirements [5]. The handling of this (role analysis, -design, -management and -maintenance) is professionally termed role life-cycle.

Simultaneous with the creation of information security – as a state – the security management of further "subdomains" may follow (human resources, the environment, production, internal logistics, supply and delivery chains, infrastructure, R&D). The concept of logical physical and organisational security defined there may then be extended to other areas. By logical protection we mean the assurance of data integrity, virus and computer intervention protection and classification methods; under physical protection come plant entry, uninterrupted energy sources, surveillance, and fire and flood protection; organisational or administrative protection means protection against internal fraud or misconduct, and purposeful or accidental damage. The integration of these may substantially lower enterprise security risks.

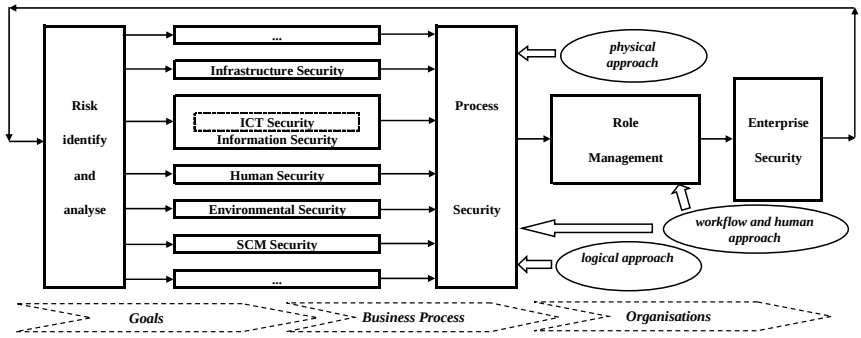

Figure 4
The attainment of enterprise security

The security of processes may in turn usher in total enterprise security (Fig. 4). A holistic security perspective takes into account and prioritises the organisation's strategic targets, the value-added processes and tools as well as supporting information technology. The management of the organisation must then work together to define and reach security targets, and should control and measure the execution of these steps [2].

Conclusions

Enterprise security is a status as well. This however cannot be regarded as static. Only continuous security activity requiring constant development and control based on risk analysis and management can be productive in the business organisations. The preliminary model introduced in this study has been made up in consideration of numerous standards and recommendations. The classical "goals – process – organisation" sequence or control loop can also be predominant here. In addition to and after the security demands of specialised enterprise areas a major role is given to processes and their representations in workflow. The latter demands the definition of jobs and responsibilities. It is we, the human beings, who are the main security risk of the organisations and the organisational security

can only be realized if the work of those participating in the processes is regulated and also if these persons are prepared to manage the unexpectedly happened risk events.

The subjects of business continuity and disaster recovery appear in standards and recommendations primarily dealing with information security. The narrowly interpreted information technology approach (BCP – Business Continuity Plan, DRP – Disaster Recovery Plan) can be extended to guarantee the conditions of any other business processes as well as to execute the tasks related to these processes in accordance with the regulations and finally in the case of malfunction normal operation can be restored.

References

[1] Aagedal, Jan Øyvind – den Braber, Folker – Dimitrakos, Theo – Gran, Bjørn Axel – Raptis, Dimitris – Stølen, Ketil: Model-based Risk Assessment to Improve Enterprise Security. Proceeding of the 6th International Enterprise Distributed Object Computing Conference (EDOC'02) September 17-20, 2002, pp. 51-64, ISBN 0-7695-1742-0, www.itsec.gov.cn (downloaded: 30 September 2011)

[2] Carelli, Richard A. – Allen, Julia H. – Stevens, James F. – Willke, Bradford J. – Wilson, William R.: Managing for Enterprise Security. Networked Systems Survivability Program, Carnegie Mellon University, 2004, p. 55 (CMU/SEI-2004-TN-046)

[3] Chapman, Robert J.: Simple Tools and Techniques of Enterprise Risk Management. John Wiley and Sons, 2006, p. 466, ISBN 13 978-0-470-01466-0

[4] Harrington, James H.: Business Process Improvement (The Breakthrough Strategy for Total Quality, Productivity and Competitiveness). McGraw-Hill, Inc. 1991, ISBN 0-07-026768-5

[5] Kern, Axel – Kuhlmann, Martin – Schaad, Andreas – Moffett, Jonathan: Observations on the Role Life-Cycle in the Context of Enterprise Security Management. SACMAT'02 Proceedings of the 7th ACM Symposium on Acces Control Models and Technologies, Monterey, CA, USA, June 3-4, 2002, pp. 43-51, ISBN 1-58113-496-7

[6] Christopher, Martin – Peck, Helen: Building the Resilient Supply Chain. International Journal of Logistics Management, Vol. 15, No. 2, 2004, pp. 1-13

[7] Smith, Gregory, E. – Watson, Kevin J. – Baker, Wade H. – Pokorski, Jay A.: A Critical Balance: Collaboration and Security in the IT-enabled Supply Chain. International Journal of Production Research. Vol. 45, No. 11, June 2007, pp. 2595-2613

[8] Supply Chain Council, Supply-Chain Operations Reference-model (SCOR). Overview. Version 10.0, 2010, http://supply-chain.org/f/Web-Scor-Overview.pdf (downloaded: 12 September 2011)

[9] Ji-Yeu Park – Rosslin John Robles - Chang-Hwa Hong – Sang-Soo Yeo – Tai-hoon Kim: IT Security Strategies for SME's. International Journal of Software Engineering and its Applications, Vol. 2, No. 3, July 2008, pp. 91-98

[10] Racz, Nicolas - Weippl, Edgar - Seufert, Andreas: A Frame of Reference for Research of Integrated Governance, Risk & Compliance (GRC). In: Bart De Decker, Ingrid Schaumüller-Bichl (Eds.), Communications and Multimedia Security, 11th IFIP TC 6/TC 11 International Conference, CMS 2010 Proceedings. Berlin: Springer, pp. 106-117

[11] Szádeczky, Tamás: Problems of Digital Sustainability. Acta Polytechnica Hungarica, Vol. 7, No. 3, 2010, pp. 123-136

[12] Wilder, Dan: The New Business Continuity Model. White paper, 2008, p. 58. www.talkingbusinesscontinuity.com/downloads/pdf/The-New-Business-Continuity-Model. (downloaded: 18 November 2011)

[13] Collaborative Planning, Forecasting and Replenishment (CPFR). Overview, 2004, Voluntary Interindustry Commerce Standards (VICS) www.vics.org (downloaded: 5 March 2012)

[14] CObIT version 4.1 Excerpt, Executive Summary, Framework, IT Governance Institute, USA, 2007 www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf (downloaded: 5 March 2012)

[15] An Introductory Overview of ITIL V3. IT Service Management Forum, 2007 www.itsmfi.org (downloaded: 6 October 2011)

[16] Enterprise Risk Management - Integrated Framework Executive Summary. Committee of Sponsoring Organizations of the Treadway Commission. September, 2004 (www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf - downloaded: 6 October 2011)

[17] www.iso27001certificates.com (downloaded continuously)

[18] ISO 14001:2004 Environmental management systems – Requirements with guidance for use

[19] ISO 14004:2004 Environmental management systems – General guidelines on principles, systems and support techniques

[20] BS OHSAS 18001:2007 Occupational health and safety management systems. Requirements

[21] BS OHSAS 18002:2008 Occupational health and safety management systems. Guidelines for the implementation of OHSAS 18001:2007

[22] ISO/IEC 38500:2008 Corporate governance of information technology

[23] ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements

[24] ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management

[25] ISO/IEC 20000-1:2011 Information technology – Service management – Part 1: Service management system requirements

[26] ISO/IEC 20000-2:2012 Information technology – Service management – Part 2: Guidance on the application of service management systems

[27] BS 25999-1:2006 Business Continuity Management, Code of Practice

[28] BS 25999-2:2007 Business Continuity Management, Specification

[29] ISO 28000:2007 Specification for security management systems for the supply chain

[30] ISO 28001:2007 Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance

[31] ISO 28002:2011 Security management systems for the supply chain - Development of resilience in the supply chain - Requirements with guidance for use

[32] AS/NZS 4360:2004 Risk management

[33] www.iso27001security.com (downloaded continuously)