Risk Management for Business Trust

Pál Michelberger

Óbuda University, Keleti Faculty of Business and Management
michelberger.pal@kgk.uni-obuda.hu

Abstract: 'Si vis pacem, para bellum', or 'if you want peace, prepare for war', as the Roman adage says. By an up-to-date version, if you want enterprise security, prepare for risk management.

This paper deals with one of the means of attaining a state of enterprise security primarily on the basis of ISO 31000, a family of standards relating to risk management well-known in trade circles. Other trust-building business models, standards, and guidelines are also discussed.

Risk management may have multiple points of linkage to contexts external or internal to, and stakeholders of, a company. From outside, it is affected by law, third-party sponsors, and international, national or local regulations. From inside, it is subject to the influence of organizational goals, investment projects, business processes, business models adopted by the organization, standards, and existing agreements with business partners.

It is appropriate for a company to give priority, among strategic objectives of its own, to control efforts based on pro-active risk analysis. If attained, enterprise security may easily become a factor of competitiveness.

Keywords: COSO, ISO 31000, ISO 27005, process security, Corporate Social Responsibility

1 Introduction

Several corporate functions (such as information security, quality management, environment management, occupational health care, maintenance, or finances) employ specific risk management practices of their own which often work independently of one another, involving a multiple load on the operations of the business, and equally affecting internal and external contexts of the company.

Consequently, a holistic and integrated approach to the management of risks does seem to be reasonable.

Conscious assumption and management of risks serve as the basis for the successful operation of an organization. A business organization needs an Enterprise Risk Management (ERM) system which is designed to

- identify and treat risk factors,
- cover the whole organization as well as its overall surroundings,
- help management to have a clear view of the whole risk profile,
- contribute to strategic and operational decision-making processes.

It will thus provide a foundation for the protection, and a means to attain security, of corporate (or organizational) processes.

Process security can be defined as a state in which, with all required inputs (or resources necessary for execution of the process) given, the organizational units responsible to fulfil process-related tasks will produce outputs (such as products, services, or information) in adequate quantity and quality in due time, and, upon any disturbance, normal operation of the process can be restored with the lowest possible use of resources within the shortest possible time.

2 Enterprise Security

Enterprise security can be defined as a state in which a business organization can maintain its functionality and value-creating processes permanently, and restore those processes in the shortest possible time upon occurrence of any unexpected event or even disaster. Another criterion of enterprise security is that the company can, on the basis of its strategic plans, keep a firm hand on its own future, while not endangering either its environment or the external or internal stakeholders through its activities. Maintenance of enterprise security requires a holistic approach, relying on ongoing risk analysis and resultant control measures. It has an impact on the layout of the organization as well, (possibly) giving rise to new security-related managerial jobs such as:

- Chief Risk Officer,
- Chief Security Officer, and
- Chief Ethics Officer.

Through control efforts underlying security, the company makes preparations, takes measures against wilful injury (instances of attack, sabotage, industrial intelligence, and fraud), and responds to incidents.

The term ‘enterprise security’ is often used to signify ‘information security’ in a special sense covering various forms of information as well as information systems (consisting of information, hardware, software, users, decision-makers, and orgware) and networks used for processing, storing, editing, forwarding and sometimes deleting information or data [1, p.7].

Data and IT security is a part of information security, and serve to contribute to the business security of the organization [19], which may, through its holistic approach to security, enhance business trust as well [4].

3 Enterprise Risk Management

For a company, such potential external or internal events or disturbances as may endanger the fulfilment of customer needs or the security of any stakeholder or stockholder of the company, constitute risks. Putting it simply, the term 'risk' means negative effects of an uncertain event. Risks will introduce uncertainty into business objectives [32]. There are 'pure' risks (always producing deleterious effects) and so-called 'speculative' risks (which may result in either gain or loss).

The ISO 31000 standard [17] contains principles, process, and supervision of risk management (Figure 1).

Enterprise risk assessment is used for identifying (more often only estimating) the degree of potential damage and probability of a negative consequence [2]. If the level of risk as derived from risk assessment is sufficiently low, i.e. if both the probability of occurrence of the incident and the degree of damage are low, the particular risk will be accepted as something the organization can co-exist with.

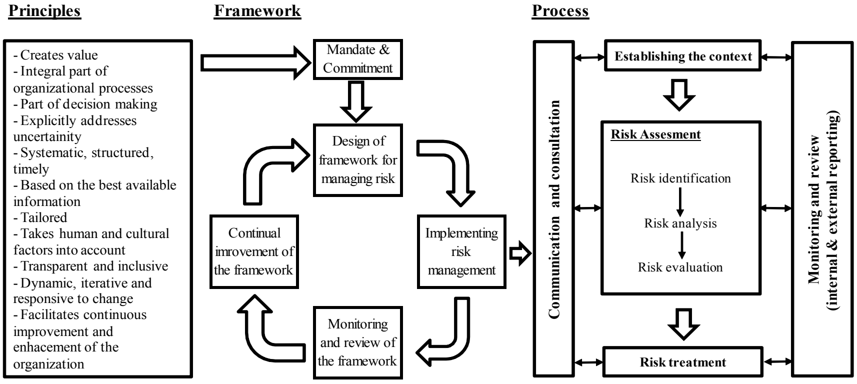
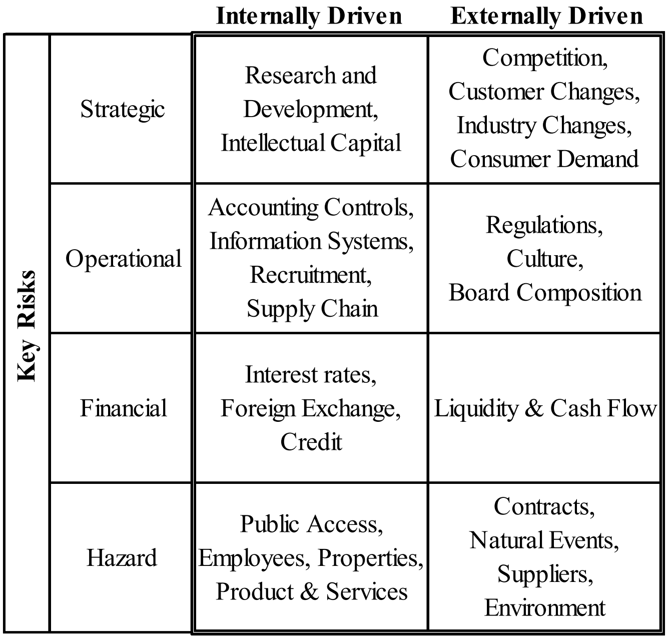

Principles
Framework
Process
- Creates value
- Integral part of organizational processes
- Part of decision making
- Explicitly addresses uncertainity
- Systematic, structured, timely
- Based on the best available information
- Tailored
- Takes human and cultural factors into account
- Transparent and inclusive
- Dynamic, iterative and responsive to change
- Facilitates continuous improvement and enhacement of the organization
Mandate & Commitment
Design of framework for managing risk
Implementing risk management
Monitoring and review of the framework
Continual imrovement of the framework
Communication and consultation
Establishing the context
Risk Assesment
Risk identification
Risk analysis
Risk evaluation
Risk treatment
Monitoring and review (internal & external reporting)

Figure 1
ISO 31000 Principles, Framework & Process [30]

Otherwise (in case of a potential or almost certain incident with considerable or critical consequences) risk treatment will follow which may involve some regular control activity aimed at reducing the probability of occurrence of the risk or mitigating the impact of its consequences. Other risk treatment options include transfer and sharing (e.g. insurance) of the risk, or avoidance of a risky activity.



		Internally Driven	**Externally Driven**
Key Risks	Strategic	Research and Development, Intellectual Capital	Competition, Customer Changes, Industry Changes, Consumer Demand
	Operational	Accounting Controls, Information Systems, Recruitment, Supply Chain	Regulations, Culture, Board Composition
	Financial	Interest rates, Foreign Exchange, Credit	Liquidity & Cash Flow
	Hazard	Public Access, Employees, Properties, Product & Services	Contracts, Natural Events, Suppliers, Environment

Figure 2
A possible categorization of risk factors [2]

Prior to a proper application of risk treatment, categorization of risks may be required. Risks may fall into such categories as strategic, financial, market, legal, operational, personnel, and environmental risks. However, risk categories are often interrelated, and separation is not always reasonable or feasible (e.g. loss of a high-skilled valuable employee). For this reason, risk categorization should rather be founded on a division into an external context (market, industry or region) and internal context (processes, resources, organization, investments). Normally, risks belonging to the former category occur on the strategic level, while those in the latter category on the operational level, respectively. Most importantly, any evaluation should cover all key risks (Figure 2).

4 Standards and Guidelines Underlying Risk Management

Responsible managers may be spoilt for choice; there are so many standards and guidelines dealing with measures to take for attaining a state of enterprise security [16]. These documents discuss risk management too.

The list below does not aim at completeness, and includes only standards and guidelines judged by the author of this paper as important. Related sources are available in the bibliography.

- COSO Enterprise Risk Management Framework [9]
- ISO/IEC 38500 → Governance – Risk Management – Compliance Model [42]
- ISO/IEC 27001 Information Security Management System [39]
- ISO 14001 Environmental Management System [27]
- CObIT Control Objectives for Information and related Technology [14]
- BS OHSAS 18001 & 18002 Occupational Health and Safety Management System [24,25]
- ISO/IEC 20000 IT Service Management [37,38]
- BS 25999 Business Continuity Management (see also ISO 22301) [22,23]
- Supply-Chain Operations Reference (SCOR) Model [18]
- Collaborative Planning, Forecasting and Replenishment (CPFR) Process Model [43]
- ISO 28000 Security Management System for the Supply Chain [29]

The three standards discussed below are not mentioned in the paper on a complex enterprise security model referenced above.

4.1 ISO 9001

ISO 9001 is a quality management standard with risk management sections and recommendations with some bearing on management, human resources, corporate infrastructure, product requirements, production, service provision, procurement, after-sale services, customer satisfaction, internal auditing of the governance system, and prevention [3].

4.2 ISO/IEC 27005

One of the important sections of this standard series on information security management systems offers recommendations relating to information security risk management [41]. The approach adopted here is very much similar to that in the ISO 31000 standard with general risk management guidelines. Focussing solely on information security risks as a matter of course, it is designed to help with identifying (elements of IT assets, threats, existing process controls, vulnerabilities, consequences), analysing (methodologies, determination of incident probabilities and risk levels), and evaluating such risks.

4.3 ISO/IEC 15504

According to the ISO/IEC 15504 standard series [33,34,35,36] , corporate processes can be grouped, evaluated, and improved along two dimensions. Firstly, what is the objective and expected outcome of a particular process? And secondly, what can be achieved by the process (process capability)? The following process capability levels are defined (in ISO/IEC 15504-2):

Level 1 Incomplete process (the process objective is not achieved for certain)

Level 2 Performed process (the process objective is achieved to some degree)

Level 3 Managed process (with adequately managed outcome of the process)

Level 4 Established process (it being designed and performed according to a pattern / standard)

Level 5 Predictable process (it being measurable and verifiable)

Level 6 Optimizing process (the process can be improved, and the set of objectives are achieved; some feedback also included)

In assessing processes, and rating their outcomes, one makes a step towards risk assessment. Performed and managed processes involve ‘medium’ and ‘high’ risks, while established and predictable processes on capability levels 4 and 5 are associated with ‘medium’ and ‘low’ levels of risk. An optimizing process may involve nothing but a low risk. Certainly, an established risk level is always dependent upon the measure an actual process may or does deviate from its pre-defined capability level [15].

5 Stakeholders, Sustainable Development, Corporate Social Responsibility

Unaware of existing corporate risks, their internal ratings, or risk controls in place, an onlooker may have difficulties in assessing the enterprise security of any particular company. Forming their opinion, business partners are often influenced, among other factors, by the very image, including security elements, which a company has formed of itself. In this case, business trust, which is an attitude difficult to quantify, is a further measure of enterprise security.

Edward R. Freeman introduced the so-called ‘stakeholder approach’ in the early 80’s. Every business organization is linked with a number of external and internal groups (such as the state government, competitors, trade associations and non-government organizations, employees, consumers, service deliverers, suppliers, creditors, etc) which are affected by the way the organization delivers its mission [11]. These groups often have some influence on corporate resources as well.

Interactions and the success of business transactions with these affected groups (or stakeholders) and allowance for their interests are of utmost importance to enterprise security. In identifying and assessing risks, a company should assess its relations with its stakeholders, their potential impact on corporate processes and outcomes, and their ‘fields of force’. In particular, the company should find out about the way these stakeholders wish to influence the operation of the company, or the manner they may threaten the implementation of corporate processes in case of bad relations. Stakeholders may as well be involved in such activities as strategic planning or defining a vision for the company. In a ‘friendly’ environment, with goals shared with stakeholders in common, it is easier to keep the company operational, or restore it to normal after disturbances.

Sustainability is of ever-increasing importance to the long-term operation of companies. The fact that a company does not exploit its resources to a degree beyond repair, may contribute to its general recognition, especially in its immediate surroundings or region. Long-term provision of resources is listed among the objectives of a company seeking to ensure enterprise security, a factor fundamentally affecting its relations with stakeholders in its region. They will be willing to come to an arrangement even with competitors if sustainability appears to be at risk. A division of enterprise security into an operational (or short-term) and strategic (or long-term) dimension may become a necessity. A compliant company will list in its enterprise security policy and strategic plans the requirement of regional sustainability (an environmental demand of the society) in addition to / instead of dependence on resources, with the result that security and regional sustainability considerations will be introduced in business decisions normally made solely on an expenditure basis (buy or manufacture; which supplier to select; how to ensure necessary labour; develop or buy know-how, etc). An atmosphere of trust is needed in which material dialog with potential stakeholders having resources in the region is possible [21]. Maybe, companies that keep regional sustainability in mind should be granted an opportunity to demonstrate their business processes and innovation efforts.

Practical business administration combined with corporate social responsibility (CSR) can be defined as a way the company nurses its relations with stakeholders. CSR is not simply an ethical category. A company is supposed to produce profits for its owners, satisfy its customers, comply with market rules, written or unwritten, and give equal consideration to potential short-term and long-term impacts of its business decisions on the environment, society, and individuals.

By the European Commission, CSR is defined as ‘a concept whereby companies integrate social and environmental concerns in their business operations and in their interactions with their stakeholders on a voluntary basis’ [10].

What does this have to do with enterprise security? A company with provable responsibility will arouse its stakeholders’ trust which may, in turn, lead to security-raising business deals.

A proven process may rely on self-estimation against some set of rules[1] or analysis for responsible behaviour by a third party. Investigations may use the following criteria:

- compliance with law and regulations (e.g. number of violations of law prosecuted),
- ethical conduct (e.g. is there any Code of Ethics in place at the company?),
- attitude towards the environment (e.g. is there an environment management system as per ISO 14001 in place?),
- stakeholder satisfaction (e.g. regular measurement and assessment of customer or employee satisfaction),
- political alignment (e.g. co-operation with the state government, local government, or non-governmental organizations),
- non profit-oriented activities with social benefits (e.g. patronage),
- responsiveness to social issues.

6 Setting Up Management and Control Systems for Enterprise Security

The abundance of standards and guidelines as shown in the Bibliography would embarrass any strategic decision-maker. As a matter of fact, it is extremely difficult to select a particular guideline to use, or a particular management system to adopt, from the large number of options available. On the other hand, it is infeasible to prepare for so many of them simultaneously. Excessive 'bureaucracy' or a many-sided approach to process control would exhaust the limited resources of any corporate management. In time, the control of operations would become more important than that of product / service delivery.

An ultimate solution may be the application of an integrated management and control system.

A common feature of ISO 9001 quality management standard [26], ISO 14001 environment management standard [27], and ISO 27001 information security standard [39] is a process-centred approach. Each of them is structured in the same way as ISO 9001. Following the succession of items in the table of contents, the

[1] For such self-estimation models, refer to the European Excellence Model by the European Foundation for Quality Management (EFQM; www.efqm.org), and General Reporting Initiative (GRI; www.globalreporting.org).

annexes to each standard demonstrate this congruence in detail. With an aim to avoid multiple controls, the standard designers have it among their goals to develop standards that allow integrated adoption. Furthermore, an integrated management system, once set up, will require no more than a 'single' auditing.

In 2012, the BPM-GOSPEL (Business Process Modelling for Governance SPICE and Internal Financial Control) group, including Hungarian experts among the contributors, developed a so-called 'Governance Model for Trusted Businesses' [5] which is based on COSO and CObIT guidelines and ISO/IEC 15504 standard series. Adopting the model, a company may become capable of designing sustainable, controlled, and verified business operations which will win the trust of its stakeholders, especially that of its business partners.

Recommendations formulated in accordance with the COSO corporate risk management framework can easily be integrated with a framework deigned on the basis of ISO 20000 and/or CObIT principles [20].

In 2009, Information Systems Audit and Control Association (ISACA) developed a Business Model for Information Security which integrated several standards and guidelines relating to multiple areas [12]. In 2008, organizations such as IT Governance Institute and Office of Government Commerce published in the ISACA website a guideline for a possible combined application of information systems management (ITIL and ISO/IEC 20000), information security governance (ISO/IEC 27002), and IT governance and control (CObIT) [13].

7 The Role of Security in Competitiveness

A company will be competitive if, while complying with socially accepted standards, it can convert its resources into the highest possible profits, and detect, and adapt itself to, such external and internal changes as may affect its operations, in order to remain steadily functional [8].

A fundamental, though non-exclusive, means of corporate competitiveness is a profitable economy. For steady functionality, a company should equally seek to attain enterprise security in terms of physical and human resources, corporate processes, innovation, market demand, and immediate environment of the company.

Corporate capital, demand for products and services delivered by a company, existence (or lack) of business trust, regional interests, and successful implementation of corporate development objectives (in terms of the market, products, technology, and organization) are all measures of competitiveness. If a business organization manages to maintain its competitiveness, this demonstrates, among others, its capability to achieve its strategic objectives under ever-changing economic, legal, market, and cultural conditions.

‘*The lower is the level of business trust measuring acceptance and undertaken of unavoidable uncertainties in business relationships, the higher is the cost of risk-taking due to mistrust (like in the form of higher interest rates, insurance and enforcement costs, etc.), which leads to lower efficiency and competitiveness by the unsubstantiated increase of operational costs.*’ [6, p.12]

Conclusions

Enterprise security management is an approach designed to control critical corporate processes and assets as a way to ensure that corporate objectives derived from strategic plans are attained. It consists of ongoing planning, organizating, governing, controlling, and co-coordinating activities that lead to a sustainable level of enterprise security acceptable to all external and internal stakeholders of the company. It focuses on organizational processes rather than technical issues. It allows measurement of security, and continuous improvement and optimization of security objectives [7, p.14] .

To sum up, enterprise security can be regarded as a state, though not a static one. The control efforts by a business organization can only be successful if they rely on risk analysis and risk treatment, and are made, improved, and verified on an ongoing basis. As well as on specific security needs of various corporate activities, these efforts should be concentrated on business processes and their workflow. This will require definition of new jobs and related job responsibilities. Since humans constitute the highest security risk in any organization, enterprise security cannot be attained unless through controlling the work of employees delivering processes, and preparing them for the management of unexpected risk events.

Enterprise security is not an ultimate goal. If it the truth of this statement is acceptable to both external and internal stakeholders, it will necessarily contribute to the competitiveness of the company, ultimately resulting in trust (between organizations affected), and an attitude equally difficult to measure and erode. In its turn, business trust will react upon competitiveness and, ultimately, enterprise security. Furthermore, trust is a qualifier of the business environment a company operates in. Trustful stakeholders may contribute to improved corporate performance.

References

[1] Allen, J., 2005: Governing for Enterprise Security. Networked Systems Survivability Program, Carnegie Mellon University, (CMU/SEI-2005-TN-023)

[2] Association of Insurance and Risk Managers (AIRMIC), ALARM – The National Forum for Risk Management in the Public Sector, The Institute of Risk Management (IRM), 2002: A Risk Management Standard. UK

[3] Avanesov, E, 2009: Risk Management in ISO 9000 Series Standards. International conference on Risk Assessment and Management, Switzerland, Geneva, 24-25 November 2009.

[4] http://www.fr.com/files/uploads/attachments/RISC/Report_Avanesov.pdf (accessed: 21/11/2013)

[5] Booker, R., 2006: Re-engineering enterprise security. Computers & Security, 25, pp. 13-17

[6] BPM-GOSPEL (Business Process Modelling for Governance SPICE and Internal Financial Control), 2011: Governance Model for Trusted Businesses.

[7] BPM-GOSPEL (Business Process Modelling for Governance SPICE and Internal Financial Control), 2012: Governance Capability Assessment Case Study Handbook Integrated Assurance Management Scenarios for Trusted Business Operation.

[8] Carelli, R. A. – Allen, J. H. – Stevens, J. F. – Willke, B. J. – Wilson, W. R., 2004: Managing for Enterprise Security. Networked Systems Survivability Program, Carnegie Mellon University, (CMU/SEI-2004-TN-046)

[9] Chikán, A. – Czakó, E. – Zoltay-Paprika, Z., 2002: National Competitiveness in Global Economy: The Case of Hungary. Akadémiai Kiadó, Budapest, Hungary

[10] Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2004: Enterprise Risk Management – Integrated Framework Executive Summary.

[11] European Commission, 2005: Opinion of the European Economic and Social Committee on Information and measurement instruments for corporate social responsibility (CSR) in a globalised economy.

[12] Freeman, R. E., 1984: Strategic Management. A Stakeholder Approach. Pitman Series in Business and Public Policy

[13] ISACA, 2009: An Introduction to the Business Model for Information Security.

[14] ISACA, 2008: Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit, A Management Briefing from IT Governance Institute & Office of Government Commerce.

[15] IT Governance Institute, USA. COBIT 4.1., 2007: Excerpt, Executive Summary, Framework.

[16] Iványos, J. – Roóz, J. – Messnarz, R., 2010: Governance Capability Assessment. Using ISO/IEC 15504 for Internal Financial Controls and IT management. Proceedings of the MONTIFIC Project at the Conference of "The Current Financial Crisis and Competences to Address Problems on the European Market". Budapest Business School together with European Qualification and Certification Association, Budapest, Hungary, 30 September – 1 October 2010, pp 17-47.

[17] Michelberger, P. – Lábodi, C, 2012: After Information Security – Before a Paradigm Change: A Complex Enterprise Security Model. Acta Polytechnica Hungarica Vol. 9, Issue 4, 2012, pp. 101-116

[18] Risk and Insurance Management Society Inc., 2011: RIMS Executive Report. The Risk Perspective (An Overview of Widely Used Risk Management Standards and Guidelines).

[19] Supply Chain Council, 2010: Supply-Chain Operations Reference-model (SCOR). Overview. Version 10.0.

[20] von Solms, B. – von Solms, R., 2005: From information security to… business security? Computers & Security, 24, pp. 271-274

[21] Wilder, D., 2008: The New Business Continuity Model. White paper, http://www.labrr.org/assets/docs/208.pdf (accessed 20/01/2014)

[22] Zsóka, Á. – Zilahy, G., 2010: Corporate participation in regional sustainability initiatives. ERSCP-EMSU Conference. Delft, Holland, 25-28 October 2010. http://repository.tudelft.nl/view/conferencepapers/uuid%3A64afbf74-fe45-4443-95c3-d68481806a0e/ (accessed 08/01/2014)

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

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

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

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

[27] ISO 9001:2008: Quality management systems – Requirements

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

[29] ISO 22301:2012: Societal security – Business continuity management systems – Requirements

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

[31] ISO 31000:2009: Risk management – Principles and guidelines

[32] ISO 31010:2009: Risk management – Risk assessment techniques

[33] ISO Guide 73:2009: Risk Management – Vocabulary

[34] ISO/IEC 15504-1:2004: Information technology – Process assessment – Part 1: Concepts and vocabulary

[35] ISO/IEC 15504-2:2003: Information technology – Process assessment – Part 2: Performing an assessment

[36] ISO/IEC 15504-3:2004: Information technology – Process assessment – Part 3: Guidance on performing an assessment

[37] ISO/IEC 15504-4:2004: Information technology – Process assessment – Part 4: Guidance on use for process improvement and process capability determination

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

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

[40] ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements

[41] ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security controls

[42] ISO/IEC 27005:2011: Information technology – Security techniques – Information security risk management

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

[44] Voluntary Inter-industry Commerce Standards (VICS), 2004:Collaborative Planning, Forecasting and Replenishment (CPFR). Overview.