Towards a Corporate IT Risk Management Model

MARIO SPREMIC, Ph.D., Associate Professor
Faculty of Economics and Business Zagreb, University of Zagreb
Kennedy's sq 6, 10000 Zagreb
CROATIA

MATIJA POPOVIC, M.Sc., CISA
Ernst & Young, Technology & Security Risk Services
Senior IT Auditor
Sachsova 1, 10000 Zagreb
CROATIA

Abstract: - New business era inaugurate the information infrastructure as a business backbone and a platform for conducting transactions and economic activities, what makes information technology (IT) a key prerequisite and the very basis for any competitive business model. Although IT is taking significant role in businesses with its innovating and supporting potential, it seems that it is least understood company asset. Successful organizations manage IT function in much the same way that they manage their other strategic functions and processes. This in particular means that they understand and manage risks associated with growing IT opportunities as well as critical dependence of many business processes on IT and vice-versa. IT risk management issues are not only any more marginal or 'technical' problems and become more and more a 'business problem'. Therefore, in this paper a Corporate IT Risk Management model is proposed and contemporary frameworks of IT Governance and IT Audit explained. Also the methodologies for their implementation (CobiT, ISO 27000 'family', ITIL) is shown and explained.

Key-Words: IT Governance, IT Audit, IT Risk Management, Corporate IT Risk Management Model, CobiT

1. Introduction – necessity for IT Governance Model

IT risks are risks associated with intensive use of IT to support and improve business processes and business as a whole. They are related to threats and dangers that the intensive use of IT may cause undesired or unexpected damages, misuses and losses in whole business model and its environment. Conscience about the systematic IT risk management should be present at the managerial level in organizations whose business is in any way related to the functioning of modern information systems (IS), no matter if they are used only for the purpose of business automation, or some vital business process are performed electronically. Since the efficiency, effectiveness and in a great deal the successfulness of all business activities depend on the functioning of the IT and IS, a sound risk management process should not only include technical or operational issues but also executive management' frameworks such as IT Governance and IT Audit.

IT Governance is the process for controlling an organization's IT resources, including information and communication systems and technology (Hunton, et al, 2004). According to the IT Governance Institute (ITGI 2003), *IT governance* is the responsibility of executives and board of directors, and consists of leadership, organizational structures and processes that ensure that enterprise's IT sustain and extends the organization's strategies and objectives. The primary focus of IT governance is on the responsibility of the board and executive management to control formulation and the implementation of IT strategy, to ensure the alignment of IT and business, to identify metrics for measuring business value of IT and to manage IT risks in an effective way. Nolan and McFarlan (2005) recently pointed out that 'a lack of board oversight for IT activities is dangerous; it puts the firm at risk in the same way that failing to audit its books would'.

A good, or rather, inevitable approach for managing IT risks include thorough audit of all aspects of IS and IT, including hardware, software, data, networks, organization and key business processes. The primary goal of the *information system audit (IT audit)* is to identify the key business processes that depend on IT, to systematically and carefully examine their IT controls efficiency, to identify key risk areas and constantly measure the risk level, to warn about possible failures, as well as to offer suggestions to the executive management how to improve current IT risk management practices (Spremic, 2005).

2. New perspectives on IT Risks Management

IT Risks represent the likelihood that in certain circumstances a given threat-source can exercise a particular potential vulnerability and negatively impacts the IT assets (data, software, hardware), IT services, key business processes or the whole organization. From IT Governance, IT Audit and IT Security perspective, IT risk management is the process of understanding and responding to factors that may lead to a failure in the authenticity, non-repudiation, confidentiality, integrity or availability of an information system. Information security program helps organization to measure the IT risk level and provides the management processes, technology and assurance to:

- allow businesses' management to ensure business transactions and information exchanges between enterprises, customers, suppliers, partners and regulators can be trusted (authenticity and non-repudiation),
- ensure IT services are available and usable and can appropriately resist and recover from failures due to errors, deliberate attacks or disaster (availability),
- ensure information is protected against unauthorized modification or error so that accuracy, completeness and validity is maintained (integrity),
- ensure critical confidential information is withheld from those who should not have access to it (confidentiality).

Although, IT risks characteristics dramatically change in recent decades, IT is still often mistakenly regarded as a separate organization of the business and thus a separate risk, control and security environment. While since 10 or 15 years ago an IT risk could cause minor 'technical' problems, today it may affect the corporation's competitive position and strategic goals. An attack on Amazon.com, for example, would cost the company $600.000 an hour in revenue and if Cisco's systems were down for a day, the company would loose $70 million in revenues (Nolan and McFarlan, 2005), not to mention indirect costs and reputation risk. It is estimated[1] that IS downtime put direct losses on brokerage operations at $4.5 million per hour, banking industry $2.1 million per hour, e-commerce operations $113.000, etc. Also, Fortune 500 companies would have average losses of about $96.000 per hour due to the IS downtime[2].

Therefore, Corporate IT Risk Management Model (CITRM) should be a holistic and structured approach that aligns governance policies, business strategy, management procedures, business processes and operational activities with the purpose of evaluating and managing risk and uncertainties the organization faces. The main objective of CITRM model is to align IT resources, IT infrastructure, key resources (data, people, assets, etc.) and business processes with governance policies and management procedures in order to effectively manage IT risk exposure. This in particular means that executive management and Board members become responsible for managing risk associated with using IT in conducting business operations and transactions. Such initiatives are well known 'heritage' of certain regulatory framework (for example, Sarbanes-Oxley act) and represent the core of IT Governance concept.

The fundamentals of the Corporate IT Risk Management Model are:

1. ***Corporate governance policies for managing IT risks*** – policies that are mandatory at all corporate levels and approved by the highest corporate bodies (Board, executive management). Typical examples are:
   - defining the 'risk appetite' which commonly represent the corporate rules and policies for IT risk response strategies (key metrics, Key Risk Indicators, KPIs)
   - corporate policies for analyzing the impact IT risks may have on the business (quantitative or qualitative measures for conducting a business impact analysis – BIA, metrics for IT risk validation, IT risk portfolio)
   - accountability for IT control activities and framework for the IT risk reports (the dynamics of IT risk reports, who and to whom IT risk reports should be presented),
   - establishing committees and other corporate 'bodies' responsible for managing IT risks (Audit Committee, IT Governance Committee)
2. ***Procedures for managing IT risks on business units level or functional level.*** They represent the standards, guidelines and activities which help in implementation of corporate IT Governance

[1] Hiles, A. (2004): Business Continuity: Best Practices - World-Class Business Continuity Management 2nd ed., Disaster Center Bookstore, USA.

[2] Ibidem.

policies (for example, IT Security Policy, Business Continuity Plan, etc). According to the regulatory requirements and specific area of interest, this usually means the adoption of world-wide standards or frameworks (CobiT, ISO 27001, Sarbanes-Oxley, Basel II, ITIL, SANS, SAS 70, …). Periodic internal or external IT audits are needed to detect the level of compliance with standards and regulatory frameworks. Performing IT audits are necessary in order to detect the priority risk areas, to identify specific IT controls needed, to constantly measure the level of their efficiency and to calculate IT risk level on regular basis.

3. ***Operational (technical) activities***, 'driven' by governance policies and management procedures represent the counter-measures, which aim to raise the level of 'immunity' on threats or attacks to IT assets. Typical examples of operational IT controls include access controls, application controls, system controls, change controls, data accuracy controls, integrity controls, business continuity controls, etc.

3. IT Risk Management Plan

In order to provide a successful protection against possible misuses, an organization should develop methods and techniques for the control of the IT incidents and for identification of possible risk evaluation methods. *An IT Risk Management plan* should have following important steps:

1. IT risk identification and classification,
2. IT risk assessment (Business Impact Analysis) and priority determination,
3. IT risk responses strategies – identification of IT controls,
4. implementation and documentation of selected counter-measures (IT controls),
5. portfolio approach to IT risks and alignment with business strategy,
6. constant monitoring of IT risks level and auditing.

3.1. IT risks identification and classification

Perhaps the most difficult aspect of process of managing risks is their identification and classification. IT risk identification process represent not only a listing of expected negative outcomes, but also their classification according to a proposed corporate framework and preparation for their assessment by evaluation of their possible impact on business, categorization of causes and triggers to the risk event, the probability of occurrence and the allocation of the responsibility for the risks. Generally, risks are identified in terms of their relevance to the specific business objectives or impact on business processes.

Some common frameworks or industry standards can help organizations to identify and classify IT risks. Apart from industry or country specific risk and regulatory frameworks (for example, Basel II, Sarbanes-Oxley), in understanding where IT risks exist within the organization, a classic *hierarchical risk approach* should help:

1. *Corporate or company-level IT risks* – these risks are vital part of corporation's overall risk management policies and associated with corporate and executive management activities. Typical corporate or company-level IT risks include various risks associated with setting up and implementing strategies, policies, procedures, governance models, etc. Examples may be: strategic risk (IT strategy planning risks), IT/business misalignment risks, risks associated with deficient IT policies and procedures, reputation risk, loss of business, financial risks (IT project failure[3], IT investments risk[4]), audit risks (risk that financial statements are incorrect, poor internal IT audit practices), acquisition risks, legal and regulatory risks (non-compliance), etc.
2. *Process-level IT risks (IT General Risks)* – in the contemporary environment business processes are highly automated and integrated with efficient IS and IT. Therefore, it is obvious that important IT risks are associated with execution of company's business processes[5]. Typical areas of process-level IT risks are: software development or acquisition risks, change management procedures and associated risks, access to program and data risks, physical and logical security risks, business continuity and disaster recovery risks, security administration risks, various security risks, system risks, information management risks.
3. *Specific IT risks (IT Applications and IT Services Risks)* – IT managers need to establish sound

[3] Standish Group in their 2004 The Chaos Report, claimed that only 29 percent of all IT projects succeeded while the remainder were either challenged or failed, source: (ITGI, 2006).

[4] A 2002 Gartner publication reported that 20 percent of all expenditure on IT is wasted, representing, on a global basis, annual value destruction of US $600 billion. Source (Gartner, 2002).

[5] For example, Nike reportedly lost more than US $200 million through difficulties experienced in implementing its supply chain software. Failures in IT-enabled logistics systems at MFI and Sainsbury in the UK led to multimillion-pound write-offs, profit warnings and erosion of share price. Source (ITGI, 2006).

policies and procedures for controlling key risks with running various IT operations. IT application risks are commonly associated with software applications that directly support specific business processes. IT services risks are mainly affected by their availability (BC and DR) and levels of functionality (SLAs). These IT risks mainly refer to business transaction's completeness, data accuracy, integrity, existence, authorization, segregation of duties and disclosure. IT service risks commonly include risks associated with following operations or activities: network management, database management, operating system management, storage management, facilities management, security administration, capacities, configuration management, etc.

3.2. IT risks assessment and priority determination

The objective of this step is to assess the important characteristics of IT risks such as 'gravity' and frequency. IT risks gravity is the measure of the damage or potential loss that certain undesired or unexpected activity may cause and commonly it can be expressed in financial terms. According the corporate governance polices, for all identified risks, *IT risk assessment plan* includes following activities:

- identification of the threats to IT resources and the exposure of IT infrastructure to various malicious or accidental acts,
- evaluation of the vulnerabilities to identified IT risks,
- determination of the IT risks probability of occurrence,
- evaluation of the business impact of IT risks occurrence,
- analysis of the IT risks frequency and IT risks ranking,
- calculation of the IT risks 'gravity' and expected value of IT risks, and
- preparation for the response strategies and for the control of IT risks level.

This in particular means that risk analysts have performed a business impact analysis (BIA). Business impact analysis is an essential component of an organization's business continuity (BC) plan. It is the management level process to prioritize business functions by assessing the potential quantitative (financial) and qualitative (non-financial) impact that might result if an organization was to experience a business continuity event[6]. BIA is a systematic process aimed to identify: key business processes performed by an organization, the resources required to support each process performed, the impact of failing of performing a process, the criticality of each process, a recovery time objective (RTO) for each process, recovery point objective (RPO) and availability rate for each process.

Table 1. Example of the IT risk assessment and priority determination activities

IT risk scenario	**Potential damage**	**Potential loss (BIA)**	**Risk ranking**
Authorized users perform illegal activities (confidentiality)	Users have unauthorized access to data, they can view and change them, they can manipulate with the system	100.000 €	Medium
System and services disruption (availability)	Disruption of key business processes and potential loss of important data	500.000 €	High
Incomplete transaction processing (integrity)	Financial reports may be incorrect, decision making process questionable	250.000 €	High
IT Project implementation failure (financial risk)	IT project not finished on time, costs to high, quality poor (Service Level, low functionality)	300.000 €	High

3.3. Strategies for IT risks responses – identifying IT controls

Once the organization has identified, classified and assessed IT risks, risk owners and 'affected' process owners are to be identified, appropriate responses should be developed and specific cost-effective controls over

[6] The Business Contiunity Institute (2002): Glossary of terms, www.thebci.org, accessed 07/2007.

those risks should be designed. Responses to IT risk may include following strategies:

- *acceptance* – the organization chooses to live with the risk and to constantly monitor its level (gravity and impact on the business and business processes),
- *reduction* – the organization takes steps to reduce the impact (gravity) or the probability of the risk occurrence,
- *avoidance* – the organization chooses to fully or partially avoid the risk,
- *sharing* – the organization transfers the risk by, for example, purchasing insurance, outsourcing risk management services, or engaging in partnership(s) regarding the risk management process to fully or partly cover risk exposure (especially in business continuity and disaster recovery plans).

Strategies for IT risks responses usually means that specific IT controls need to be implemented and their efficiency constantly monitored. *Control activities* are the policies, procedures and practices that are put into place so that business objectives are achieved and risk mitigation strategies are carried out. Control activities are developed to specifically address each control objective to mitigate the risks identified. An *IT control objective* is a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity (ITGI, 2003). IT Audit activities usually include the examination of the IT control efficiency. When doing so, IT Auditors commonly perform test of IT controls using specific metrics (for example, RTO, RPO for business continuity process), maturity models and audit tools (CAATs, ACL software, etc.). Common metrics for testing the efficiency of business continuity plan may be:

- MTBF (Mean Time Between Failures) represents an important system characteristic which help to quantify the suitability of a system for a potential application. MTBF is the measure of the systems' functionality and service level.
- Availability is the percentage of time when system is operational (for example, 99% availability means that the system downtime is 3,65 days per year, while 99,99% availability rate means that the downtime is 52 minutes per year).
- RTO (Recovery Time Objective) - the period of time within which systems, services, applications or functions must be recovered after an outage. It is maximum tolerable length of time that a IT infrastructure can be down after a failure or disaster occurs. The RTO is a function of the extent to which the interruption disrupts normal operations and the amount of revenue lost per unit time as a result of the disaster.
- RPO (Recovery Point Objective) – the maximum amount of data loss an organization can sustain during an event. It is also the point in time (prior to outage) in which systems and data must be restored to.

In recent years various groups have developed world-wide known IT control frameworks and guidelines to assist management and auditors in developing optimal controls systems. Contemporary IT governance and IT audit frameworks are:

- *CobiT* (Control Objectives of Information and related Technology),
- *ISO 27000 'family'* (ISO 27001:2005, ISO 27002:2005), and
- *ITIL* (IT Infrastructure Library).

The possible results of management efforts in managing IT risk are presented by table 2. IT Governance and IT Audit activities there give a clear guideline to executive management in managing IT risk.

Table 2. The results of Corporate IT Risk Management Model implementation

Key business process	Sales orders (e-orders)
IT risk	System disruption
IT risk level	High – critical, loss of data, corporate risk
Potential loss (BIA) (per day)	500.000 €
IT Risk Response Strategy	Immediate action, risk level reduction
IT Control	CobiT 4.1. (*DS4, DS5)* ITIL *BCM* ISO 27002 (10, 11, 4)
Key Metrics – IT Control Efficiency	Availability = 99,95% RTO < 3h RPO < 3h
Responsible person (business process owner)	XY

Implementing IT Governance and IT Audit frameworks may help organizations manage IT risk level. For example, CobiT is the widely accepted IT governance framework, organized by key IT control objectives, which are broken into detailed IT controls. Current version 4.1 of CobiT divides IT into four domains (Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate), which are broken into 34 IT processes covering all important processes within IT, and then further divided into more than 300 detailed IT control objectives. Therefore, CobiT provides a sound support especially for company-level and process-level IT risks management. For each IT control objective CobiT defines:

- performance goals and metrics (for example, RPO, RTO, availability time),
- KRI (Key Risk Indicator), KPI (Key Performance Indicator)
- maturity models (0-5 scale) to assist in benchmarking and decision-making for process improvements,
- a RACI chart identifying who is Responsible, Accountable, Consulted, and/or Informed for specific IT control objective.

4. Concluding remarks

Although, traditionally, only the IT departments were responsible for managing IT risks, their importance affects the fact that the number of companies starting to systematically deal with such problems is ever increasing. Thus the issue of managing the IT risks becomes less and less a technical problem, and more and more the problem of the whole organization i.e. a ‘business problem’, so that many companies formally nominate executive directors for such activities. Therefore, we find the proposed corporate IT risk management model incorporating contemporary IT governance and IT audit issues suitable and inevitable framework for managing IT risk in today’s business.

References:

[1]. Champlain, J.J. (2003): Auditing Information Systems, 2nd ed. John Wiley & Sons, SAD.

[2]. Gartner (2002): ‘The Elusive Business Value of IT’, August 2002.

[3]. Hiles, A. (2004): Business Continuity: Best Practices - World-Class Business Continuity Management 2nd ed., Disaster Center Bookstore, USA.

[4]. Hunton, J.E., Bryant, S.M., Bagranoff, N.A.: (2004): Core Concepts of Information Technology Auditing, John Wiley &Sons Inc., SAD.

[5]. International Organization for Standardization (ISO), *Code of Practice for Information Security Management*, ISO/IEC 17799, Switzerland, 2005

[6]. ITGI (2003): *Board Briefing on IT Governance*, 2nd ed., IT Governance Institute, Rolling Meadows, Illinois, SAD.

[7]. ITGI (2006): *Enterprise Value: Governance of IT Investments, The Val IT Framework*, IT Governance Institute, Rolling Meadows, Illinois, SAD.

[8]. Nolan, R. and McFarlan, F.W., (2005): Information Technology and Board of Directors, Harvard Business Review, October, 2005.

[9]. Spremic, M. (2005): Managing IT risks by implementing information system audit function, Proceedings of the 3rd International Workshop in Wireless Security Technologies, Westminster University, London, 04-05.04.2005, pp. 58-64.

[10]. Symons, C., (2005): IT Governance Framework: Structures, Processes and Framework, Forrester Research, Inc.

[11]. Weill, P., Ross, J.W., (2004): IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press, 2004.