ANDRO KULL

# A Method for Continuous Information Technology Supervision

## The Case of the Estonian Financial Sector

■

ACADEMIC DISSERTATION
To be presented, with the permission of
the board of the School of Information Sciences of the University of Tampere,
for public discussion in the Paavo Koli Auditorium, Kanslerinrinne 1,
Tampere, on January 20th, 2012, at 12 o'clock.

UNIVERSITY OF TAMPERE

UNIVERSITY
OF TAMPERE

ACADEMIC DISSERTATION
University of Tampere
School of Information Sciences
Finland

Distribution
Bookshop TAJU
P.O. Box 617
33014 University of Tampere
Finland

Tel. +358 40 190 9800
Fax +358 3 3551 7685
taju@uta.fi
www.uta.fi/taju
http://granum.uta.fi

Cover design by
Mikko Reinikka

Acta Universitatis Tamperensis 1694
ISBN 978-951-44-8688-3 (print)
ISSN-L 1455-1616
ISSN 1455-1616

Acta Electronica Universitatis Tamperensis 1160
ISBN 978-951-44-8689-0 (pdf)
ISSN 1456-954X
http://acta.uta.fi

Tampereen Yliopistopaino Oy – Juvenes Print
Tampere 2012

# Abstract

The year 2008 financial crisis showed that more control is necessary for the financial sector. Controls should be planned and realized at the international, country and bank levels because everyone who has to use financial services wants to be sure that data are secure. For example, the use of Internet banking in Estonia today accounts for over 95% of all transactions, meaning that almost everyone uses the electronic services of financial institutions. To increase security in computerized actions of financial institutions, a certain supervisory authorization must be established.

In order to cleverly realize such questions as “How much security is necessary?” and “How much security is sufficient?”, a systematic approach is necessary. In the current case, these questions should be answered by financial supervisors to provide assurances that people’s money is safe in banks and in other financial institutions. In this report we shall propose a new compliance assessment and monitoring method for these purposes.

We shall develop our method based on the following measures. Firstly, we shall perform a literature review. Secondly, we shall survey current arrangements in 29 European countries, and finally we shall explore the situation in our country. As a result of the research, the supervisory requirements for IT will be compiled and a method for information technology supervision will be developed. A method covers all the most important steps to assure information security, starting with risk assessment and requirements establishment and concludes with security scoring. Also, some initial preliminary use experiences will be reported.

**Keywords**

Information technology, risk assessment, information security, compliance, financial sector.

# Acknowledgements

I started my research years ago and the real impetus came when I started working at Estonian Financial Supervision Authority. I remember clearly that during an interview I noticed the potential to investigate the supervision approach connected with information technology more deeply. Competence is one of the authority's values and I am very grateful to my employer for this favor.

I dare to admit that the first doctoral seminars at the University of Tampere were terrifying to me. Article-by-article things went better and I began to understand how it works and it would be impossible without the constant guidance and help of my supervisor. Also he encouraged me to participate in relevant international conferences, which experience is hard to underestimate. I express the greatest appreciation for invaluable contribution to my supervisor Prof. Emer Pertti Järvinen.

My research has brought me into contact with the top ones in the field of information technology and information security science. My special thanks for the dedication of reviewing to Prof. Dr. Klaus Brunnstein, Cestmir Halbich, Dr. Richard Baskerville, Prof. Dr. Gurpreet Dhillon and for the dedication of acting as opponents to Prof. Dr. Peeter Normak and Prof. Mikko Siponen.

During my doctoral studies, I have once married and I have got two children. Without taking into account the minor fact that my wife Lilian and the children Marten and Simona take at home all of my attention, I probably would not have had enough motivation without them to go to school until the end. In times I should be away from home my wife’s parents were in support and my parents always believed that someday I will finish my studies.

Dedicated to my family

Andro Kull

# Glossary

**Business continuity** – a supervised entity's ability to conduct business without disruptions.

**Business continuity plan** – an integral written activity plan, which is a component of business continuity management, for recovering and continuing business in the event of an unforeseeable business disruption.

**Business impact analysis** – a process, which is a component of business continuity management, of systematically identifying and assessing (qualitatively and quantitatively) the impact of business disruptions on the supervised entity's business processes and other processes. Business impact analysis is used to identify recovery priorities and the resources required for recovery (including staff) and to develop business continuity plans.

**Credit institution** - a credit institution is a company whose principal and permanent economic activity is to receive cash deposits and other repayable funds from the public and to grant loans for its own account and in its own name and provide other financing. Receipt of deposits from public grant the right to companies to use the name of 'a bank'. (www.fi.ee, accessed 30.12.2010).

**Data** – re-interpretable presentation of information in formalized form that is suitable for transmission, interpretation or processing.

**Data element** – a data item that in certain contexts is regarded as indivisible.

**Data model** – description of the organization of data in a manner that reflects the information structure of a company.

**Financial supervision –** (objective) Financial supervision is conducted in order to enhance the stability, reliability, transparency and efficiency of the financial sector, to reduce systemic risks and to promote prevention of the abuse of the financial sector for criminal purposes, with a view of protecting the interests of clients and investors by safeguarding their financial resources, and thereby supporting the stability of the monetary system.

**Financial Supervision Authority** (FSA) - The Financial Supervision Authority is an agency by the Bank of Estonia, with autonomous competence and a separate budget and the management of which acts and submits reports pursuant to the procedure provided for in the Financial Supervision Authority Act. The Financial Supervision Authority conducts financial supervision in the name of the state and is independent in the conduct of financial supervision.

**Finantsinspektsiooni seadus (FIS)** – Financial Supervision Act.

**Information** – knowledge that concerns objects, e.g. facts, events, things, processes or ideas, including definitions, and that has a specific meaning in a certain context.

**Information system** – information processing system providing and distributing information together with accompanying legal solutions and organizational resources, including human, technical and financial resources.

**Information assets** – information, data and the applications necessary for their processing.

**Information security measures –** by enterprise knowingly taken actions to reduce information technology risks and to anticipate and to avoid information security incidents and minimize the impact of incidents if occurred.

**Information security policy** – enterprise's internal document, which explains information security content for the enterprise and describes the measures how information security will be assured.

**IT security** – protection of information in order to ensure:

- confidentiality – protection of information against unauthorized publication;
- integrity – protection of information against counterfeiting and unauthorized alteration;
- availability – timely availability of information and services for authorized persons.

**IT solution** – software and hardware, which supports certain business operation.

**Major business disruption** – a disruption of a supervised entity's business that exceeds the acceptability level established by the entity (the maximum failure time) and influences the functioning of the business processes that have been defined as critical by supervised entities.

**Owner of information assets** – an employee of a company who is liable for the security and maintenance of information assets and whose tasks, among others, include classification of data and determination of user's rights.

**Recovery plan** – a document, which is a part of the business continuity plan, that describes the roles, responsibilities and other activities for the recovery of business and other processes after an unforeseeable business disruption.

**Recovery Point Objective** (RPO) – maximum tolerable data loss in case of major business disruption.

**Recovery Time Objective** (RTO) – maximum tolerable time during which the business has to be recovered in case of major business disruption.

**Residual risk –** maximum tolerable risk which is accepted by enterprise and which persists after information security measures are implemented.

**Risk analysis –** a process, which is a component of business continuity management, of assessing potential risks and their impact on the supervised entity's processes and systems and identifying the major risks.

**Security incident** – an event the result of which is (or may be) violation of information security.

**Sensitive information** – information that, according to the decision of a competent authority, must be protected as its publication, alteration, destruction or loss would cause significant damage to somebody or something.

**Supervised entity** (SE) – an unit treated as a subject of financial supervision under financial supervision authority act FIS § 2 (1) (except for insurance brokers as referred to in § 130 (2) 1) of the Insurance Activities Act).

# Figures and tables

**Figures**

**Tables**

# Table of contents

# 1. Introduction

In connection with financial issues, the common examples about regulations are SOX (2002) for the United States, PCI-DSS (Payment Card Industry Data Security Standard) and Basel II (2004) for Europe. To be compliant with new regulations is a challenge for many enterprises. The question "How much security is necessary?" is important today for each organization, certainly it is more important for organizations in the financial sector. This study focuses on information security issues in the financial sector. Considering some facts about Estonia and financial sector - Estonia is a member of European Union, the bigger banks in Estonia are the subsidiaries, we have launched Euro lately - it is essential to be in accordance with European practices in developing our standards to regulate the financial sector and IT field.

I as an author have been working in Financial Supervision Authority in Estonia as an IT auditor about five years and the need for deeper investigation of the nature of IT supervision came from everyday activities. A lot of different frameworks, standards and best practices are used by financial market participants to ensure information security. As my own approach, the most important research issues were first to figure out the basic needs what IT supervisors have to expect from financial market participants in connection with information security and second to combine and analyze the possibilities of how to set up the requirements and what would be the criteria to assess whether the requirements are met or not.

The key concept presented in Figure 1.1 and used through the research is named as expression *technology assurance* (TA), it is all which gives the feel of security in using technology. This may be a synonym for the expression *information assurance* (IA). To ensure technology assurance, the lowest steps have to be passed to go higher level. Technology assurance presumes, that business processes are well organized, information assets and IT governance has to be well established etc. to build up higher level assurance like working business continuity process.

For each step, kind of best practice or international standard can be found, for example for IT governance a COBIT (Control Objectives for Information and related Technology) and for information security ISO/IEC 27001:2005 (Information technology, Security techniques, Information security management systems). The key idea considered throughout the study is to combine the sufficient best practices and international standards into asset, use the set for building appropriate method for IT supervision and apply it for Estonian financial sector.

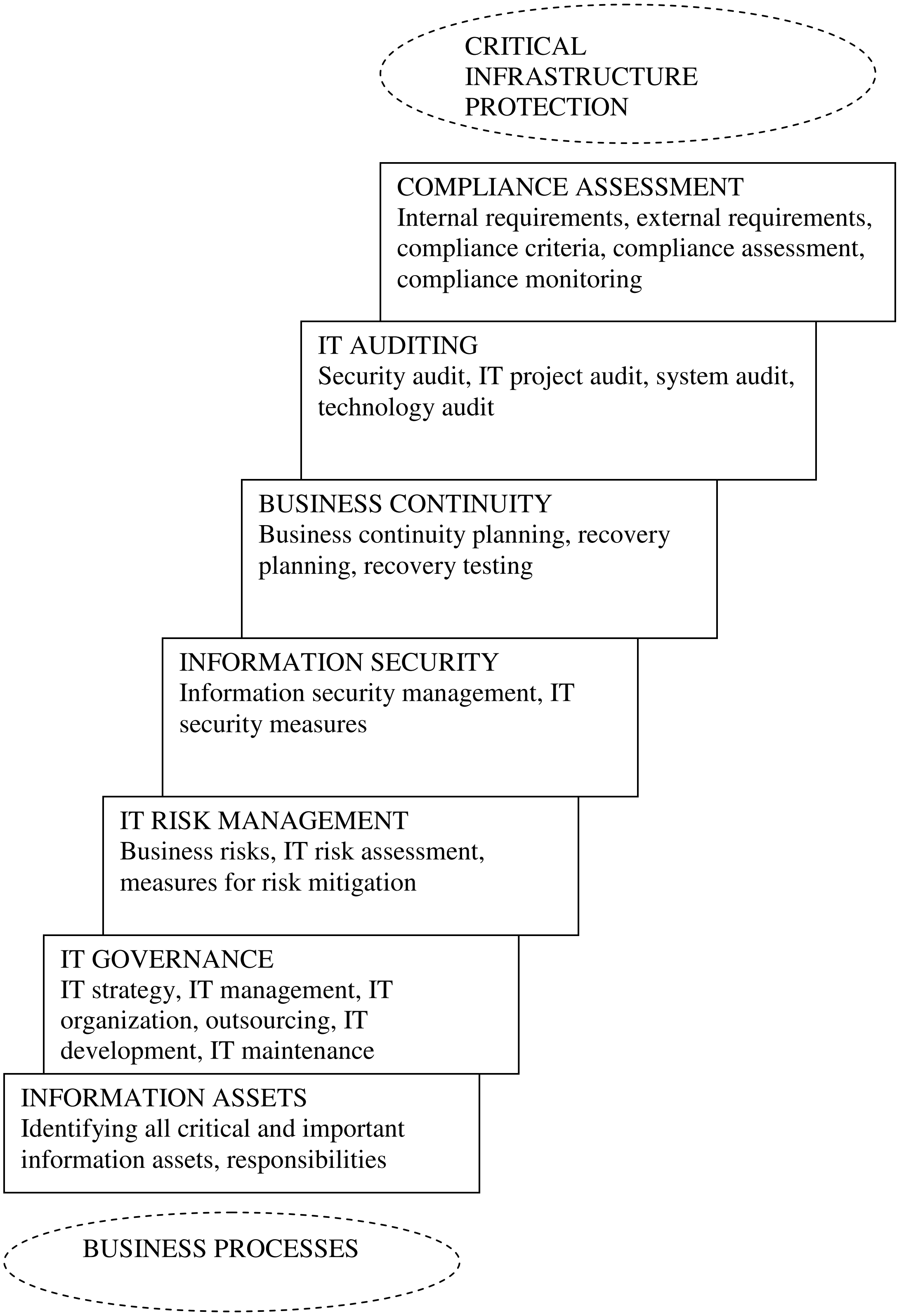
CRITICAL INFRASTRUCTURE PROTECTION
COMPLIANCE ASSESSMENT
Internal requirements, external requirements, compliance criteria, compliance assessment, compliance monitoring
IT AUDITING
Security audit, IT project audit, system audit, technology audit
BUSINESS CONTINUITY
Business continuity planning, recovery planning, recovery testing
INFORMATION SECURITY
Information security management, IT security measures
IT RISK MANAGEMENT
Business risks, IT risk assessment, measures for risk mitigation
IT GOVERNANCE
IT strategy, IT management, IT organization, outsourcing, IT development, IT maintenance
INFORMATION ASSETS
Identifying all critical and important information assets, responsibilities
BUSINESS PROCESSES

**Figure 1.1 Elements of IT assurance**

Most already developed information security assessment approaches are useful as such for enterprises. These approaches help to organize a risk assessment or give advice for choosing the measures for information security in common sense financial supervision deals with control of controls; therefore a different approach is needed for IT supervision. The current methods of IT supervision often have the following drawbacks:

1. Adaptability – the methods are developed for a specific market sector (mostly banking);
2. Universality – solutions and methods deal with off-site inspections or on-site inspections and there is no solution for both at the same time.

A new, better supervision method is needed and considering the needs for Estonia, it must have the following properties:

1. Usable for all sizes of financial institutions – adaptable for any kind of supervised institution;
2. Usable for conducting off-site and on-site issues – focus on both documentation and the actual IT situation.

In the literature, a little attention is paid to the IT compliance issues from regulator standpoint, i.e., what are motivations from regulatory side and what problems the regulators face today. It is obvious that regulators try to find the best solutions for determining requirements which on the one hand satisfies the needs for regulators to meet with their mission and on the other hand are essential for regulated organizations to keep market in a certain sector consistent.

The motivations from practice rise as usage of information technology in financial sector grows and from regulators perspective, the need to pay more attention to the operational risk rises. IT risk management becomes more clearly a part of operational risk management, for example, by Basel II regulations and it highlights quite new approach for regulators too. Its consequence is that there is a need for systematic IT auditing and IT supervision, especially in financial sector.

Literature review shows the number of theories, solutions, recommendations, best practices and standards in connection with information technology and information security. From scientific point of view author sees too little attention to:

- using existing knowledge for a certain task;
- combining different approaches to produce new ones.

The author uses and combines the best practices in way to develop a new method for IT supervision.

The most important and common research questions are – *how to continuously control organizations' IT domain compliance with requirements* and *does the level of compliance mean lower risks*? In this dissertation, the main questions will be answered through research and creation a solution.

Through the whole research work, the answers to the sub-questions will be found:

1. What are the reasonable security requirements for IT domain?
2. What are the reasonable criteria to measure?
3. How could the criteria be assessed to ensure the requirements are fulfilled?
4. How to ensure equal treatment of subjects independent on their size and business?

5. How to plan and organize IT auditing activities based on compliance assessments results?
6. How to ensure continuous compliance control?
7. What kind of solution can be used to perform continuous compliance and if there are deficiencies, how the IT risks come out and mate with other risks?

We shall derive a new supervision method based on our review of literature, our survey of Europe and some preliminary studies. The rest of this paper consists of the IT supervision approach, a review of literature, some empirical studies, and the development of a new supervision method and the evaluation of its merits.

As our own approach, the other supervision authorities and supervised entities are first studied to determine the best set of requirements for the IT field and to ensure information security. Next, a method is proposed on how to measure the level of compliance with these requirements. As further research and development, the method will be put into an info-technological solution, which will measure all the risks in the financial sector. In this report we shall show that from a supervisory standpoint, IT risks in the financial sector could be measured in a manner similar to the other financial sector risks.

During the research, three contributions are taken into account. All the contributions support to find answer to the research questions stated above.

Contribution 1 – acceptable way to work in financial sector considering safety, security and risks (FSA descriptions, rules and suggestions).

Contribution 2 – normal management and supervising unit (internal, external), supervision process.

Contribution 3 – how to measure the current state and comply with acceptance criteria?

There are some preliminary descriptive surveys presented leading to method development and a field study has been conducted.

Besides theoretical results of the study we suggest important implications for practice and doing so expand understanding about how to transfer theoretical findings into practice. Rosemann and Vessey (2008) discuss in their paper about the practice relevance of IS research. In their approach they analyze three dimensions of relevance: importance, accessibility and suitability (or applicability). The authors propose solution named applicability checks to make academic research applicable to practitioners. The results of the study are tested whether they are applicable for practical use in conducting IT supervision tasks.

The study starts with extensive literature review outlined in Chapter 2. Next, in Chapter 3 an IT supervision approach is introduced and in Chapter 4, IT risks by supervisory meaning are discussed.

As our own approach, the other supervision authorities and supervised entities are studied to determine the best set of requirements for the IT field and to ensure information security in Chapters 5-6. Next, a method is proposed on how to measure the level of compliance with these requirements in Chapters 7-8. As further research and development, the IT supervision method is described and it is put into an IT solution, which will measure all the risks in the financial sector in Chapters 9-10. In this report we shall show that from a supervisory standpoint, IT risks in the financial sector could be measured in a manner similar to the other financial sector risks.

Detailed descriptions are presented in Appendices 1 and 2.

# 2. Literature review

In this chapter we give an overview about research and literature in connection with information technology and governance, information security and business continuity as the areas the IT supervisors have to consider. After that, information security valuation follows and the methods and solutions for compliance and security assessment are outlined. For overview, a summary table is outlined and below description follows by subject areas.

I will organize literature review in such a way, that all the key concepts stated beforehand receive enough attention. Thus, a literature review is concept-centric (Watson and Webster 2002). The main concepts and relevant literature are summarized in single table as following.

Because of the need to concentrate to the very specific research topic – IT supervision and compliance assessment in a very concrete field, an expert review is used to find sufficient material, i.e., best practices in the broader meaning. Although Kitchenham et al. (2009) define evidence as a synthesis of best quality scientific studies on a specific topic or research question, an expert review using ad hoc literature selection is as contrast solution. Contrast solution will be used because of lack of sufficient literature in our very specific research and a systematic literature review (SLR) demonstrates it. In return, a lot of input for research is collected through different studies to find out solutions already implemented in practice.

| **Topic** | **Author(s)** | **Date** | **Title** | **Research focus** |
|---|---|---|---|---|
| Information technology governance, information security and business continuity requirements, risks and controls | Henderson and Venkatraman | 1999 | Strategic Alignment: Leveraging information technology for transforming organizations | Internal I/S domain |
| | Hirsch and Esingeard | 2008 | Perceptual and Cultural Aspects of Risk Management Alignment: a case study | Social aspects of information security and risk management |
| | SABSA | 2010 | SABSA - Sherwood Applied Business Security Architecture | Information security and risk areas |
| | ISACA | 2010 | COBIT - Control Objectives for Information and related Technology | IT governance |

| | | | | |
|---|---|---|---|---|
| | German BSI | 2005 | IT Grundschutz Kataloge | Standard approach of information security measures |
| | British BSI | 2010 | British Standards Institute | Appropriate standards |
| | Committee of Sponsoring Organizations | 2010 | COSO - Internal Control Framework | Preventive and detective controls |
| | Institute of Internal Auditors | 2010 | The GAIT methodology | A risk-based approach to assessing the scope of IT general controls |
| | Carnegie Mellon Software Engineering Institute (CMU/SEI) | 1999 | OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation | |
| | Forbes Gibb, Steven Buchanan | 2006 | A framework for business continuity management | |
| | Syed, Akthar, Afsar | 2004 | Business continuity planning methodology | Stages |
| | Andrew Hiles | 2004 | Business continuity: best practices, World-Class Business Continuity Management | Defining disaster |
| | ISO | 2008 | ISO/IEC 24762:2008 Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services | ICT Readiness for Business Continuity (IRBC) |
| | Macaulay Tyson | 2009 | Critical infrastructure: understanding its component parts, vulnerabilities, operating risks, and interdependencies | CI interdependency |
| | Estonian Ministry of the Interior | 2009 | Emergency Act | |
| | Bruce K. Behn, | 2006 | A Within Firm | Continuous |

| | | | | |
|---|---|---|---|---|
| | DeWayne L. Searcy, Jonathan B. Woodroof | | Analysis of Current and Expected Future Audit Lag Determinants | auditing |
| | IIA | 2006 | IT Audit Topics Research Symposium | The frameworks, measures and value |
| | IT governance Institute | 2006 | IT control objectives for Sarbanes Oxley | The role of IT in the design and implementation of internal control over financial reporting |
| | IT governance Institute | 2007 | IT control objectives for Basel II | The importance of governance and risk management for compliance |
| | Deloitte | 2007 | Global security survey | Top initiatives |
| | Marcia L. Weidenmier, Sridhar Ramamoorti | 2006 | Research Opportunities in Information Technology and Internal Auditing | |
| Security costs, security valuation | Ghose and Rajan | 2006 | The Economic Impact of Regulatory Information Disclosure on Information Security Investments, Competition, and Social Welfare | Investments for regulatory compliance and consequences |
| | Gary Hinson | 2008 | The financial implications of implementing ISO/IEC 27001 & 27002: a generic cost-benefit model | Costs and benefits for security |
| | Kirt, Kivimaa | 2010 | Optimizing IT security costs by evolutionary algorithms | IT security cost-effectiveness |
| | Virkkunen | 1951 | Teollisuuden kertakustannukset – niiden degressio sekä käsittely | universal problems in accounting |

| | | | | |
|---|---|---|---|---|
| | | | kustannuslaskennassa | |
| | Järvinen | 2004 | On research methods | division problem |
| | Thomas, Russell Cameron | 2007 | Total Cost of Cyber (In)security – Integrating operational security metrics into business decision-making | Total cost of security |
| | Wes Sonnenreich, Jason Albanese, and Bruce Stout | 2010 | Return On Security Investment (ROSI): A Practical Quantitative Model | Return on security investments |
| | Dhillon and Torkzadeh | 2006 | Value-focused assessment of information system security in organizations | Organizationally grounded principles and values |
| | Ramachandran and White | 2005 | Methodology to Assess the Impact of Investments in Security Tools and Products | Investments in Information Technology Security Tools and Products (ITSTP) |
| | Aberdeen Group | 2005 | Best Practices in Security Governance | Security level and losses |
| | Mukhopadhyay, Kekre, and Kalathur | 1995 | Business value of information technology: A study of electronic data interchange. | Business value of information technology |
| | ISACA | 2009 | An Introduction to the Business Model for Information Security | Link the security program to business goals |
| | Kevin Behr, Grant Castner, Gene Kim | 2010 | The value, effectiveness, efficiency, and security of IT controls: An empirical analysis | IT controls improve IT efficiency, IT effectiveness, IT security, and usiness value |
| Compliance measurement, security measurement, security metrics | Siponen and Iivari | 2006 | Six Design Theories for IS Security Policies and Guidelines | IS security policy compliance – voluntary or not? |
| | NetIQ | 2008 | Sustainable Compliance: How to reconnect | |

| | | | | |
|---|---|---|---|---|
| | | | compliance, security and business goals | |
| | Brotby | 2009 | Information security management metrics: a definite guide to effective security monitoring and measurement | Compliance metrics |
| | Brotby | 2009 | Information security management metrics: a definite guide to effective security monitoring and measurement | Percentage as a common measure; is 100 percent compliance realistic? |
| | MITRE Corporation | 2010 | A collection of Information Security Community Standardization Activities and Initiatives | Enumeration, languages, repositories |
| | Vaughn, Henning and Siraj | 2002 | Information Assurance Measures and Metrics - State of Practice and Proposed Taxonomy | Fundamental characteristics of metrics |
| | Johansson and Johnson | 2005 | Assessment of Enterprise Information Security - An Architecture Theory Diagram Definition | EIS |
| | IT Compliance Institute | 2006 | IT audit checklist: information security | Practical guidance on how to prepare for successful audits |
| | Software Engineering Institute | 1993 | CMM – Capability Maturity Model | |
| | John R. Hauser and Gerald M. Katz | 1998 | Metrics: You Are What You Measure! | Metrics, decisions and actions |
| | Hinson Gary | 2006 | Seven myths about information security metrics | |

**Table 2.1 Summary of literature review**

Following the key concept and research questions, the topics are divided into subtopics as follows:

- Information technology governance, information security and business continuity requirements, risks and controls;
- Security costs, security valuation;
- Compliance measurement, security measurement, security metrics.

By Alvesson and Sandberg (2011, page 247)

> "… "gap-spotting" means that the assumptions underlying existing literature for the most part remain unchallenged in the formulation of research questions. In other words, gap-spotting tends to *under-problematize* existing literature and, thus, reinforces rather than challenges already influential theories."

Considering the relevant literature, the gaps are connected with completeness of technology/information assurance based on different approaches and solutions. The challenge of current research is to improve the situation through proposing complete practical method.

The questions and topics are highlighted and relevant examples from different studies are presented, and afterwards, through the steps of research, our own approach is presented to deal with the problems and topics.

The questions raised from the literature review are addressed regarding IT supervision method through the use of studies, as follows.

# 3. IT supervision approach

In this chapter we describe and explain about IT supervision with the purpose to highlight the features in this area. First, supervisory activities at the principle level are described, which gives an answer to the question “What supervisors do and how they do it”. A wider picture about IT supervision follows and a small study about IT supervision in European level is demonstrated.

As a starting point, it can be mentioned that IT supervision differs from classical IT risk assessment, information security management and IT auditing. Next we will attempt to provide an overview explanation of these differences and disclose the practical need to perform IT supervision in a systematic manner.

## 3.1. Supervisory activities

In essence, IT supervision has to deal with a control of IT controls. Commonly, the activities from the supervision point of view could be divided into off-site inspections (controls) and on-site inspections (controls).

Off-site inspections could be taken as an IT risk assessment. For example, in case the supervised entities cannot prove good IT governance, there is a risk in the meaning of IT supervision. The best way to ascertain good intention is to carry out a compliance assessment, for example, to conduct compliance assessment with requirements stated in the supervisory guidelines.

The input for off-site inspection is all possible information regulators are able to collect regarding the IT field – subjects’ IT policies, IT procedures, IT reports, etc. The output of off-site inspections should be the clear understanding about the situation of subject’s IT and hence the entire financial sector’s IT and what could be the specific reasons (risks within the supervisory meaning) to plan on-site inspections.

During an off-site inspection, specific questions should be raised based on presented documented information, which needs to be controlled during the on-site inspection. For example, such questions are “what are the actions you take to perform a certain written procedure?”, “when and to whom you send the given information?” etc. In addition, there should be a clear idea after the off-site inspection as to which kind of observation is necessary during an on-site inspection, for example, “please, let us see, whether the location for software licenses and outsourcing agreements is safe!”, “please, let us see the current status of the incident reporting system!” or “please, try to create a user account using a password which does not correspond to the written roles!”. As a conclusion, ideally, the on-site inspection should provide an assurance to the findings discovered during an off-site inspection.

On-site inspections follow normal IT auditing procedure and during the audit the basic steps will be passed – planning, studying and evaluating controls, testing and evaluating controls, reporting and follow-up.

New IT supervision method is necessary to support the off-site inspections and corresponding information system should give possibilities to enter the results of on-site inspections.

## 3.2. Common picture of IT supervision

In this section we give an overview about how IT field regulation is organized in European Supervision Authorities to get rationale for setting up the regulative requirements in Estonia.

Today the banking operation depends, to a large extent, on all its aspects on information technology (IT), that development and maintenance of information systems are increasingly being outsourced, that computer centers are relocated to other countries, that IT risks have a significant impact on the operational risk level and on the level of capital requirements, in accordance with Basel II and Capital Requirements Directive - CRD, that organization of IT supervision within financial supervision represents a challenge for any supervisory institution and that, in most cases, co-operation between IT supervisors is based on a multilateral or bilateral relationships. Accordingly, there is a justified reason for additional cooperation and exchange of knowledge and experience among IT supervisors and a need for events gathering IT supervisors from various regulatory and supervisory institutions.

The format of the Conference consists of presentations and discussions.
For the purpose of greater efficiency of the Conference itself, we will send a questionnaire to all the invited regulatory and supervisory institutions, which will contain questions related to the organization and ways of conducting IT supervision in each country. The questionnaire results will be analyzed, processed and presented at the Conference and included in the Conference material.

To clarify the need for IT supervision a systematic approach, i.e., IT supervision method, participation in a certain questionnaire and its results are used amongst 25 central banks and supervision authorities in Europe. The questionnaire was a part of the International Conference on Information Systems Supervision in Croatia, in 2009. The aim of the questionnaire was to facilitate the exchange of information and ensure a better understanding of how the supervision of information systems of financial institutions is performed in various countries.

Based on the answers to the questions, the most important results in connection with research questions about IT and information security assessment are highlighted below.

One question concerning research problem was “How important are the following areas/elements for supervision of information systems and for determining the adequacy of a credit institution's management of the information system? If your answer is "Other", please provide additional information in the comment field."

Results are presented in Figure 3.1.

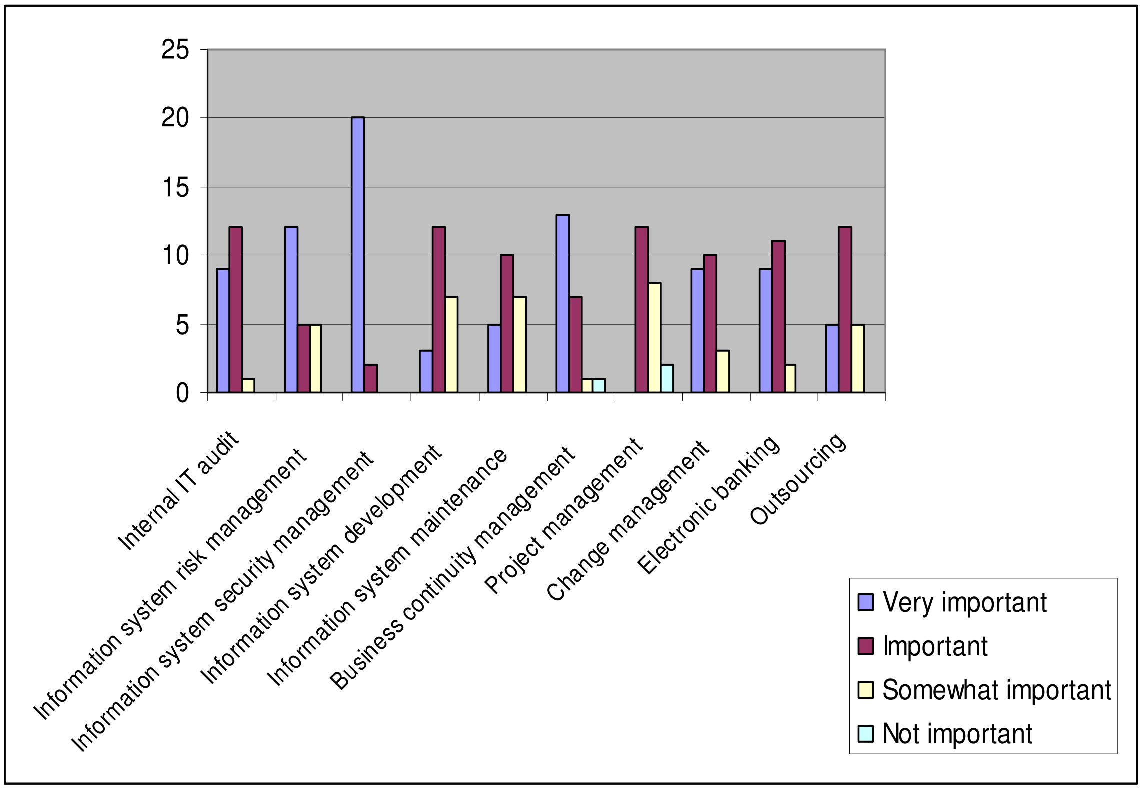

**Figure 3.1 Important areas for supervision of information systems**

As shown in Figure 3.1, the highest ratings have got information systems security, business continuity and information system risk management. The same basic pillars were pointed out in introduction of key concept of research, it is technology assurance, which gives the feel of security in using technology.

Second question concerning research problem was "Do you have a risk assessment methodology / scoring system for information systems in credit institutions? If so, and there are related resources that are publicly available, please provide a web link in the comment field. If your answer is "Other", please provide additional information in the comment field."

Results are presented in Figure 3.2.

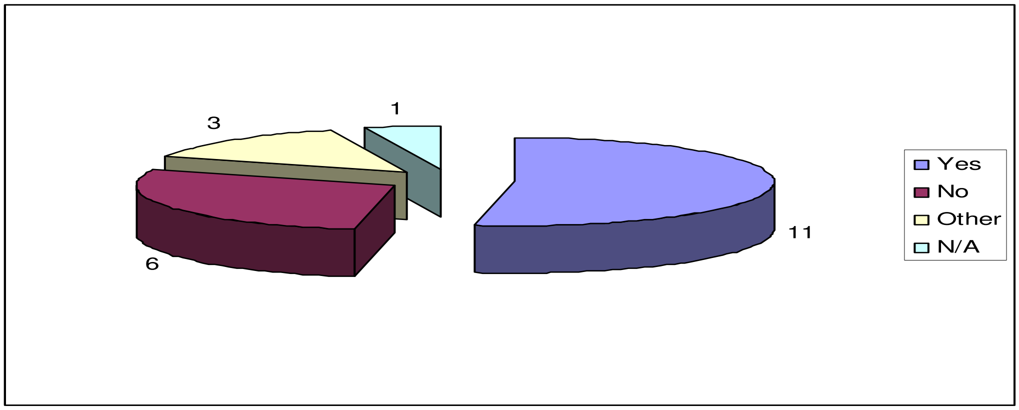

**Figure 3.2 Distribution of risk assessment methodology/scoring system**

More than a half of respondents have kind of solution to assess information systems in credit institutions. It shows the tendency to have systematic approach for information technology supervision and it can be explained by the fact that supervisor must use a lot of information from different sources, such as was seen in the previous answer.

Next question concerning research problem was “If there is a risk assessment methodology / scoring system for information systems in credit institutions, is it used for the planning of on-site examinations (supervisions)?
If your answer is “Other”, please provide additional information in the comment field."

Results are presented in Figure 3.3.

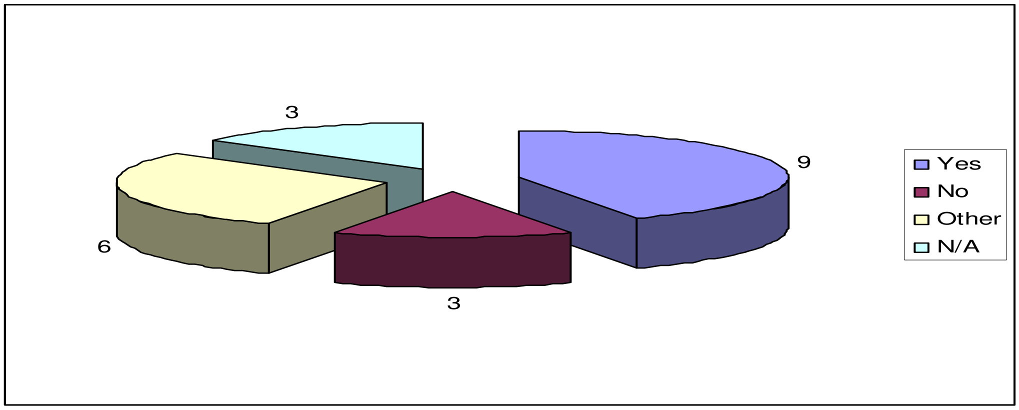

**Figure 3.3 Share of risk assessment methodology/scoring system**

The answers point to the fact that before on-site examinations an off-site assessment is needed.

If there is a risk assessment methodology/scoring system for information systems in credit institutions, please rate the importance of the following inputs:

1. Results (reports) of previous on-site examinations (supervisions) of the credit institution’s information system
2. Results (reports) of previous financial on-site examinations (supervisions)
3. Financial reports that credit institutions periodically send to the supervisory authority
4. Reports that are focused on information systems that credit institutions periodically send to the supervisory authority (e.g., based on questionnaires)
5. Ad-hoc reports focused on information systems that are requested by the supervisory authority
6. Reports from the external auditor of the credit institution
7. Reports from the internal IT auditor of the credit institution
8. Reports from other credit institution personnel (e.g., compliance officer, information security officer, etc.)
9. Information gathered at regular periodical meetings with the credit institution's top management
10. Information gathered at regular periodical meetings with the credit institution’s other personnel (e.g., information security officer, internal auditor, etc.)
11. Information gathered at ad-hoc meetings with the credit institution’s top management
12. Information gathered at ad-hoc meetings with the credit institution’s other personnel (e.g., information security officer, internal auditor, etc.)
13. Other (please provide additional information in the comment field)

Possible ratings were “Very important”, “Important“, „Somewhat important”, “N/A (not applicable)”, “Not taken into account”, “Does not exist/Is not performed” and “Other”.

Results are presented in Figure 3.4.

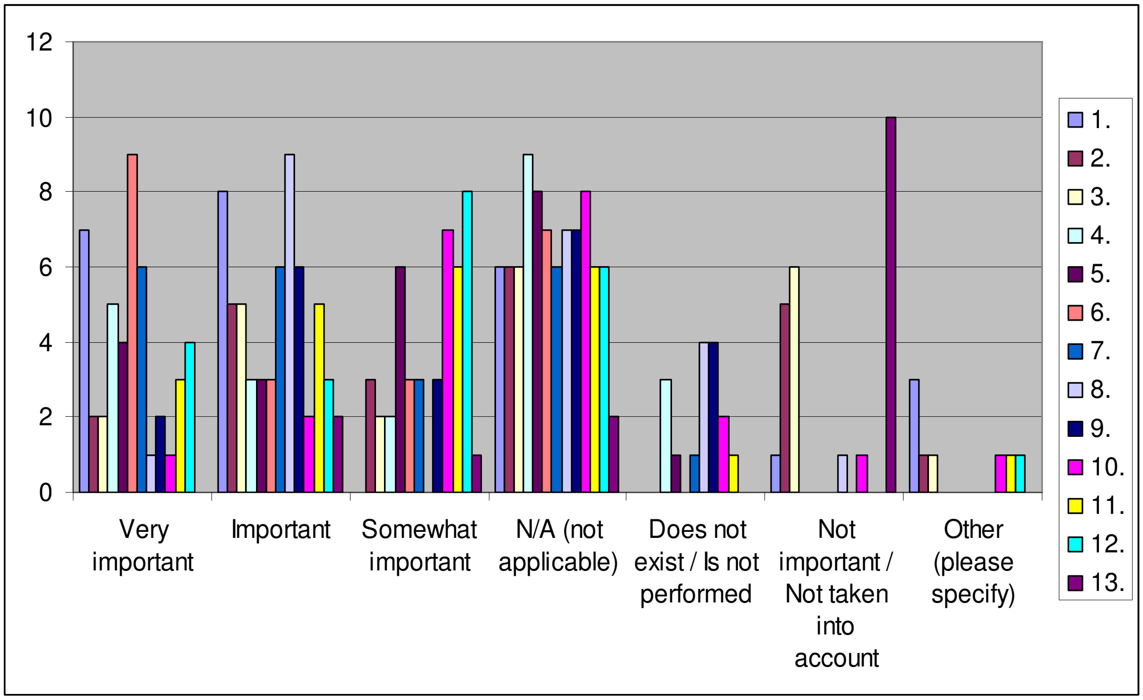

**Figure 3.4 The rate the importance of the inputs**

In common, the answers show that all the mentioned information collecting sources deserve attention. Considering the method for continuous information technology supervision and corresponding technical solution, all these sources have to be involved and some extra sources like, for example, questionnaires and self-assessments have to be included.

Discussion

The results of the study clearly show the tendency of IT assessment in the financial sector, although the approaches and needs for solutions are different.

The main criticism to the existing approaches for IT supervision is that the proposed list is not complete, for example, the concentration of IT and information security incidents seem to be more important in showing the actual condition of a supervised entity. IT supervision method notes to the need to collect all relevant information into one single solution.

As a result of this chapter an overview about IT supervision activities, it is off-site and on-site activities, were highlighted. Based on the results of sub-study a clear tendency shows that the systematic approach is needed for IT supervision. The study continues with integral part of our method – risk assessment.

# 4. IT risk from supervisory perspective

In this chapter, IT risks are exposed in more detail from supervisory perspective and considering previous chapter, there are some differences with traditional IT risk approach. First, the global and local dimensions for IT risk management are outlined and the use of SABSA - Sherwood Applied Business Security Architecture (2010) risk areas is proposed for mapping IT risks. Quite new necessity to consider in connection with IT risks is critical infrastructure protection and some basics to deal with these issues are described. Last sections are divided to two principle risk sites: risks before control and risk controls.

## 4.1. Global dimension

Deloitte 2007 Global Security Survey for financial institutions highlights top initiatives connected to information security:

- Access and identity management;
- Security regulatory compliance;
- Security training and awareness;
- Governance for security;
- Disaster recovery and business continuity.

It gives a signal that named areas are the most sensitive to information security risks in certain sector.

## 4.2. Local dimension

To start discussions about information security and connected risks in financial sector, which is one of the most important concerns for IT supervisors, first the concept of IT and information systems (I/S) identification should be determined.

Henderson and Venkatraman (1993, pages 474-475) address three components of internal I/S domain:

- I/S architecture – applications, hardware, software, communications, data architecture;
- I/S processes – systems development, maintenance, monitoring, control systems;
- I/S skills – knowledge and capabilities for management and operating the infrastructure.

Next, the main risk areas are highlighted which first are comprehensive and best fit with local situation.

### 4.2.1. Supervisory risks

Financial sector is sensitive because it keeps client's financial instruments and this fact sets great demands for supervised entities (hereafter subjects) like, for example, banks and insurance companies and their IT solutions. And it in turn sets the demands to the financial supervision authority (hereafter FSA).

> "The main objective of supervision is to ensure that financial institutions are able to meet their obligations to the customers in the future - pay out deposits, insurance losses or pension contributions, etc. An important task of the Financial Supervision Authority is also to help to increase the efficiency of the Estonian financial sector, avoid systemic risks, and prevent the abuse of the financial sector for criminal purposes. The work of the Authority also involves explanation of which are the risks for the customers and provide information and support to them in choosing financial services." (www.fi.ee).

Risks from regulatory standpoint seem to be different from the risks are taken by supervised entities.

To illustrate that statement, examples are next discussed. Risk assessment is not done by supervision authority but authority controls that supervised entities have processes and responsibilities in place to make risk assessments and in case some important areas are not included into risk assessment in comparison with whole financial sector, supervision authority has duty to pay attention to these risks.

Another example is about data security measures. These measures have to be chosen by supervised entity and supervision authority does not give evaluation about whether these measures are good, whether they are based on right technology etc. but gives an evaluation about whether these measures work to minimize risks and possible negative impact.

In general, supervision authority gives evaluation about the question: are the chosen measures adequate and sufficient and to give such an evaluation, there has to be some rationale for assessment framework in place.

### 4.2.2. Information technology risks

Information technology risk can be defined as a risk that could disturb use of IT solutions for supporting business functions in case if risk realizes.

IT risks from supervisory perspective are in more detail discussed hereafter, but in general, IT risks should not be isolated from other risks – it is credit risk, market risk, reputation risk etc. – and is strongly connected with operational risk. Such common view is also highlighted by other authors, for example, Hirsch and Ezingeard (2008, page 7).

> “Information security risk is only one category of risks organizations are exposed to and many organizations find it difficult to align their IT risk management efforts with those of the rest of the organization in other areas such as financial or business continuity risks. Often this is because risk management strategies, and more specifically information security strategies, are not grounded in organizational values (Dhillon and Torkzadeh, 2006). Yet, legislative and regulatory requirements for instance in the corporate governance arena, requiring organizations to think of information security within their overall risk management frameworks make this a requirement. This means that not only do risk management processes need to be aligned across functional areas in the organization, but also that attitudes towards risk need to be aligned.“

Although IT risks and information security are the main focus of our research, after all it will be connected with other risk areas.

No doubt risks in financial sector are something different from the other sectors, but the basics for IT risks called IT risk areas are pretty much the same. As the methodology by SABSA - Sherwood Applied Business Security Architecture (2010) is in nature generic, it can be used as a good starting point. In respective web-page www.sabsa.org it is stated:

> “SABSA is a model and a methodology for developing risk-driven enterprise information security architectures. SABSA methodology is by nature generic and can be the starting point for any organization and after deeper analysis, it becomes specific to the enterprise. It is suitable to start with finding the risk areas needed to cover in current case.”

To find out the risk areas in current case, interpretation of SABSA overall matrix will be used as illustrated in Table 4.1.

| | **Assets** | **Motivation** | **Process** | **People** | **Location** | **Time** |
|---|---|---|---|---|---|---|
| **Contextual** | Business requirements, information | Business risk, corporate policy | Management program | Security organization | Business field | Business timetable |
| **Conceptual** | Business continuity | Audit, compliance | Change control, disaster recovery | Awareness | Security domain | Operations schedule |
| **Logical** | Information security | Security policy, compliance monitoring | Security service management | Access control | Administration | Applications deadline |
| **Physical** | Database, software | Vulnerability, threat | Backup administration, log administration | Helpdesk | Network security management | Aging |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Component** | Product, tool | Vulnerability, threat research | Project management, operation management | User administration | Platform security management | Sequencing |

**Table 4.1 Interpretation of SABSA Framework for Security Service Management**

Why to use a SABSA framework in mapping risk areas? First, in assessing subjects' IT related risks and developing requirements for supervised entities to deal with these risks, the main attention comes to the security issues. Second, SABSA also uses the best practices and standards like ITIL, ISO 27001 and CobIT and in addition SABSA already accomplished relations between these practices and standards. The main purpose for method is to map risk areas so, that no single risk is forgotten.

## 4.3. Risk before control

Considering the key concepts used through this research, information technology risks are hidden into four main categories, first information technology governance, second information security governance, third business continuity and from supervisory perspective, compliance risks.

*IT governance* - risk, that IT field is not governed properly, IT field does not conform to wide-spread rules and standards and because of that IT field generates often problems to the business functions.

*IT security governance* - risk, that information security measures are not sufficient, information security governance does not conform to wide-spread rules and standards and because of that business experiences often security problems which affects negatively business functions.

*Business continuity* – risk, that business continuity is not ensured, business interruptions continue for a long time and because of that the consequences to business functions can be very serious or fatal.

*Compliance* - risk, that subject's IT governance, IT security governance or business continuity function do not comply with the laws, regulations or internal policies, processes and procedures and because of that public reputation can be suffered or direct penalties will be adjudged.

## 4.4. Risk control

In assessing the controls for reducing IT risks, all the criteria should not be fulfilled and decision about what criterion has to be fulfilled certainly, makes an examiner considering the current situation.

Common classification of controls:

- Risk identification;
- Risk policy;
- Administrative organization and internal control;
- Risk observation.

Risk identification – scope and manner, which are implemented for identification of concrete risk category, for example, risk assessment and analysis.

Risk policy – the quality of control methods, how subject determines significance of risk and risk appetite.

Administrative organization and internal control – scope and manner, how are concrete risk category, risk policy procedures, segregation of functions and other preventive methods implemented and put under control.

Risk observation – scope and manner, how is concrete risk observed and how are controls implemented, for example, report of performance, reports about incidents or exceptions, analysis etc.

As a result of this chapter, concrete risk scales are described and presented in Appendix 1. The research continues with requirements to reduce the level of risk.

# 5. Requirements

This chapter gives the basic principles and concrete requirements how the supervised entities should deal with IT risks. First the process of working out the advisory guidelines is described and the guidelines in connection with IT field – IT governance, information security and business continuity – are drawn up. The results of this phase are coordinated and approved documents freely available for everyone to consider when one wants to act in financial sector. To conclude with the requirements, also a common approach at European level is studied and the main results of this study are pointed last in this chapter.

## 5.1. Advisory guidelines process

The initiative for creating advisory guidelines comes from FSA to more precisely regulate the areas important for stability of market.

Considering, that the impact of any kind of requirements can the subjects account best, in setting up the requirements for IT and information security, position of the subject is considered.
FSA has also got signals from supervised entities that there is a need for more concrete regulation for market. First, it helps subjects to set up their own specific internal regulations and second, it helps to explain the importance of IT and information security measures and the need for investments for implementing the measures.

After the first version of guidelines they are under discussion inside of FSA. After that it comes to the market participants for comments. Considering the feedback, next versions will be developed and discussed. After common consensus with the version, the guidelines will be published.

Generally the next version which comes to establishment will be introduced to all interested parties in relevant seminar.

Between development and establishment of guidelines an adequate time buffer will be left, so the subjects can complete the actions to be in compliance with new regulations.

## 5.2. Guidelines in connection with IT

Guidelines cover the most important fields stated beforehand – IT governance, information security and business continuity.

### 5.2.1. IT governance

Well-known framework for IT governance is COBIT - Control Objectives for Information and related Technology which cannot be ignored in our case because it is widely approved and somehow used by financial sector institutions. As COBIT (version 4.1) is control-based, it gives possibility to set up requirements for IT governance initiatives.

> "COBIT is a framework and supporting tool set that allows managers to bridge the gap with respect to control requirements, technical issues and business risks, and communicate that level of control to stakeholders. COBIT enables the development of clear policies and good practice for IT control throughout enterprises. COBIT is continuously kept up to date and harmonized with other standards and guidance. Hence, COBIT has become the integrator for IT good practices and the umbrella framework for IT governance that helps in understanding and managing the risks and benefits associated with IT. The process structure of COBIT and its high-level, business-oriented approach provide an end-to-end view of IT and the decisions to be made about IT." (ISACA, 2010, page 11)."

However, COBIT approach has been accepted practice for many years in supervision and it cannot be violated without reasonable explanation. Objectives and application of advisory guidelines follow.

The activities of companies of the financial sector to a great extent depend on information technology (IT). The objective of these guidelines is to lay down minimum requirements for the organization of work in the field of information technology in the companies of the financial sector in order to increase the efficiency of the financial sector and to decrease systemic and operational risks.

These guidelines regulate the organization of work in the field of information technology in the subjects of financial supervision. The instructions provided in the guidelines are to be followed in compliance with the requirements provided in legislation.

The control objectives stated in COBIT (Control Objectives for Information and Related Technology) and its short version COBIT Quickstart served as the basis for compiling these guidelines. The control objectives of COBIT have been supplemented and specified with the requirements and definitions included in standards concerning information technology (BS:7799, EVS- ISO/IEC 2382).

The information technology control system or framework of a company of the financial sector must be created so that it would provide a suitable support for business processes. The information systems of a company must correspond to the requirements of availability, integrity and confidentiality derived from business activities. The implementation of these guidelines in a company first and foremost depends on the size of the company, complexity of processes, number of employees or the technology used.

### 5.2.2. Information security

Objectives and application of advisory guidelines follow.

Information security is a continuous process within enterprise. This process assesses the risks in connection with information technology, chooses the measures to reduce risks and controls that the measures are implemented and they work as needed.
The main purpose of information security is to reduce the risks in connection with information technology to the acceptable level.
The purpose of information security guidelines is to help govern information security process of supervised entity (SE) and to define the requirements which give an assurance for supervision authority if implemented by SE.
With the guidelines recommendations and common instructions are established how supervised entities are expected to govern information security process.

For setting up the recommendations and requirements the international standards ISO/IEC 27001 and ISO/IEC 27002 are used.

### 5.2.3. Business continuity

The biggest concern for IT supervision from three classical aspects of information security – availability, confidentiality and integrity – is undoubtedly availability, which brings us to the term business continuity. For example, it tries to avoid situations like some bank cannot operate further because of fatal errors in their banking information systems. More and more literature is available in this field, some findings are highlighted.

Gibb and Buchanan (2006) propose a framework for business continuity management (BCM), which could be a starting point to deal with continuity issues. They suggest for BCM – business continuity management reviews the following control questions:

- Is documentation effective and current?
- Is the project sponsor appropriate and involved?
- Does staff understand their roles and responsibilities?
- Are contract details for staff, vendors and service providers accurate and complete?
- Could nominated staff authorize and make purchases and allocate resources if required?
- Are vendor and service agreements still viable, credible and deliverable?
- Have back-up and testing procedures been followed?
- Are there staff with the authority to approve re-starts of, and access to, off-site facilities?
- Are alternative communication channels available?
- Has succession been addressed?
- Is the plan regularly reviewed and updated?
- Are all critical components of production and service been addressed?
- Are we protecting components which are no longer critical?

Business continuity planning methodology (Syed, 2004) divides topic into stages:

1. Stage 1 – Risk management
   Stage 1, risk management, assesses the threats of disaster, existing vulnerabilities, potential disaster impacts, and identifies and implements controls needed to prevent or reduce the risk of disaster.
2. Stage 2 – Business impact analysis (BIA)
   Stage 2, business impact analysis, identifies mission-critical processes, and analyzes impacts to business if these processes are interrupted as a result of a disaster.
3. Stage 3 – Business continuity strategy development
   Stage 3, business continuity strategy development, assesses the requirements and identifies the options for recovery of critical processes and resources in the event they are disrupted by a disaster.
4. Stage 4 – Business continuity plan development
   Stage 4, business continuity plan development, develops a plan for maintaining business continuity based on the results of previous stages, specifically, risk management, BIA, and business continuity strategy development.
5. Stage 5 – Business continuity plan testing
   Stage 5, business continuity plan testing, tests the business continuity plan document to ensure its currency, viability, and completeness.
6. Stage 6 – Business continuity plan maintenance
   Stage 6, business continuity plan maintenance, maintains the business continuity plan in a constant ready-state for execution.

In general, to work out the requirements for business continuity, all the stages should be covered.

Hiles (2004, page 3) underlines the need for defining disaster and gives some directions.

> "Defining "disaster" is fundamental to business continuity planning. Too loose a definition can cause a disaster – either by invoking an unproven and deficient plan unnecessarily, or by failing to recognize that a potential disaster condition exists until irreparable damage has been caused. The lesson is straightforward. Disasters are not always self-evident. There has to be a clear definition of disaster – and escalation procedure from customer compliance, help desk, quality defects, service level failures and production incidents so that decisions can be made about each incident against established disaster criteria.
>
> For a commercial entity, a typical definition of "disaster" would be: an event, which causes the loss of an essential service, or part of it, for a length of time which imperils the business.
>
> For a public sector organization, the following definition could apply: an event, which causes the loss of an essential service, or part of it, for a length of time which imperils mission achievement."

Beginning to address the business continuity practically for supervision activities, the need for defining “disaster” or “business continuity incident” as we call it emerged immediately. It is true that finding some common solution which suits for everyone is hard, if not impossible. Today we as supervisors accept that every supervised entity should define business continuity incidents itself and we as supervisors look if it is done and if it is reasonable. Two aspects must be identified as Hiles (2004) suggests: essential services considering the number of clients who suffer and severity of disaster considering whether loss of service is minor, essential or critical for business.

From IT supervision perspective, clear ICT component in connection with business continuity raises, which is noticed by standard organizations. For example, national standard ISO/IEC 24762:2008 Information technology - Security techniques - Guidelines for information and communications technology disaster recovery services cover that topic.

ISO/IEC 24762:2008 specifies:

- the requirements for implementing, operating, monitoring and maintaining information and communication technology (ICT) disaster recovery (DR) services and facilities;
- the capabilities which outsourced ICT DR service providers should possess, and the practices they should follow, so as to provide basic secure operating environments and facilitate organizations' recovery efforts;
- the guidance for selection of recovery site; and
- the guidance for ICT DR service providers to continuously improve their ICT DR services.

One step forward for business continuity could be national critical infrastructure (CI) protection, which concerns also financial sector and hence supervisors. Macaulay (2009) highlights the interdependency between different CI services.

> “The proxy indicators we propose in this chapter are econometrics and data-dependency metrics. These are good starting points for discussions of CI sector interdependency for two specific reasons: all sectors possess, produce, spend, and manage money; and all sectors possess, produce, send and receive information and data. Money and data are the lowest common denominators of modern economies and CI sectors. These are things that all business and sectors have and must use on a constant basis to remain operational.“

In addition, in Estonia the banks are included into list of critical service providers in national level. By the Emergency Act (Estonian Ministry of the Interior, 2009) making a risk assessment, next steps will be covered:

- Taking the objects as following:
    - Human factor, personnel

  - Facilities, buildings
  - Equipment, intermediate agents
  - Software and data
  - Data in physical form
  - Electronic communication
- Assessment of vulnerability based on criteria:
  - Dependence on risk elements
  - Dependence on external services like, for example, electricity and transportation
  - Current security measures
  - Alternatives
  - Resources needed for recovery
- Taking into account likelihood, a risk will be calculated for each object and also in summary.

Purpose and scope of guidelines are as follows.

The financial system operates as a network of closely interrelated markets, infrastructures and market participants. The functioning of each link of the network can influence others and is capable of interrupting the entire financial system, thus impacting on the whole economy.

Business continuity planning is a process through which supervised entities ensure the administration or recovery of their business, including services for customers, upon the occurrence of extraordinary disruptions. A functioning business continuity process shows that an undertaking is prepared for business disruptions that may occur for reasons beyond the control, and has plans in place for continuing its operations and reducing potential losses. Business disruptions may be caused by e.g., loss of staff, problems with the physical location or infrastructure of the business, malfunctioning of the information systems, various environment-related disasters (e.g., a fire).

The goals of business continuity plans are to save human lives and reduce potential injuries, to minimize the financial losses of supervised entities, to continue servicing customers and financial market participants, to reduce the negative impact of disruptions on the entity's strategic plans, reputation, principal business, liquidity, credit quality, market position, and the ability to comply with the requirements of law.

The purpose of these guidelines is to:

• contribute to the supervised entities' process of preparation and administration of business continuity plans;

• facilitate a uniform understanding of the process of preparation and administration of business continuity plans and the requirements for those plans among supervised entities.

These guidelines establish advisory and general code of conduct, and guidelines for supervised entities for organizing their business continuity processes and plans, taking international practice in the area and the recommendations of international organizations into account.

The "High-level principles for business continuity" issued by the Joint Forum1 in August 2006 were used for developing the recommendations presented herein. These guidelines present what the Financial Supervision Authority believes to be the minimum requirements for ensuring business continuity. The scope of application of the guidelines depends on organizational structure, scope and risk level of business, the quantity and complicacy of the financial services and products offered, and the entity's overall impact on the financial system.

Application of these guidelines should take the requirements of law into account, as well as the other advisory guidelines of the Financial Supervision Authority and the characteristics of the particular supervised entity, as well as the internal organization of business continuity of the entity. Where the legislation provides for special requirements, these must be followed.

The "comply or explain" principle should be taken into account in the application of these guidelines: if necessary, a supervised entity shall be able to explain why it is not applying or is only partly applying any of the paragraphs of these guidelines.

The guidelines should be applied, and any interpretation problems should be solved, following the principle of reasonability, taking the purpose of these guidelines into account, and acting in good faith with the diligence expected of a supervised entity.

## 5.3. Alternative approaches

Before starting with information technology and information security governance measures compilation, some principal questions should be answered. Rule based approach vs. principle based approach? According to the IT supervisory method, the regulator issues general requirements to the subjects. For example, Bundesamt für Sicherheit in der Informationstechnik (BSI) uses a different approach in their IT Grundschutzhandbuch (in Estonia ISKE) – public sector institutions shall by themselves determine what kind of requirements need to be implemented based on information about data applied inside of the institution. With the IT supervisory method, supervisors need to decide on the relevance of measures taken, but with ISKE, in principle, these measures are already developed and institutions should just implement them. So, which could be better for public sector institutions and which for private institutions like financial institutions?

BSI standard approach (BSI, 2005) was studied and the main advantages and disadvantages are outlined as following:

+ BSI system is complete, documented in detail and is under annual regular improvement
+ Standard approach of information security is economical because the standard measures are re-usable for organizations acting similar conditions and therefore the security needs are in principle the same
+ Time needed for security analysis and measures selection is short
– In case standard level is set too high, the expenditures for security can be too high
– In case standard level is set too low, the security measures cannot be sufficient

– For mission critical systems and for other very important information assets it is not possible to find economically optimal solution

Pros-arguments: the supervising unit cannot decide about business decisions and therefore the direct rules are not suitable. The most important thing is that subjects operate securely, and what is secure should be decided by the subjects. Also, IT and information security are changing rapidly and there should not be a permanent solution.

Cons-arguments: subjects may not have the necessary knowledge about IT risks and the necessary solutions to deal with these risks. Adaptable method creates a situation where all the subjects develop a different type of approach to deal with information security.

Committee of Sponsoring Organizations, the COSO (2010) Internal control framework focuses on the internal control, and not directly to IT.

Framework consists of three objectives:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

and five components:

- Control environment
- Risk assessment
- Control activities
- Information/Communication
- Monitoring

COSO requires an entity level focus and an activity level focus.

All objectives and components are important for supervision to demonstrate good governance.

Besides, COSO clearly sets out the different types of control, they are preventive controls like standard policies and procedures, proper segregation of duties, authorization levels and approvals and detective controls like exception reports, reconciliations and periodic audits. For IT supervision method, both types should be considered.

Institute of Internal Auditors released Guide to the Assessment of IT Risk, the GAIT methodology for management of organizations and their independent auditors, whose challenge is to define an effective and efficient scope for the annual assessments of internal control over financial reporting required by Sarbanes-Oxley Act (SOX).

To apply the GAIT methodology:

- Phase 1: Review the key manual and automated controls and key functionality in the business process to determine the critical functionality that is relied on.
- Phase 2: Extend the understanding of the in-scope financially significant applications and their infrastructure.
- Phase 3: Identify and assess the risk of IT process failures at each layer of the stack and identify related control objectives. This is the core of the GAIT methodology.
- Phase 4: Identify the key IT general controls to achieve the objectives

- Phase 5: Perform a reasonable person review

As we can see, the GAIT methodology is worked out for very specific reason, it is for internal control.

OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation Framework version 1.0 is completed by Software Engineering Institute, Carnegie Mellon University. The main purpose of this framework is to identify and manage information security risks.

Framework covers three phases:

Phase 1, Build Enterprise-Wide Security Requirements
During Phase 1, information assets and their values, threats to those assets, and security requirements are identified using knowledge of the staff from multiple levels within the organization, along with standard catalogs of information. For example, known threat profiles and good organizational and technical practices are used to probe staff members for their knowledge of the organization's assets, threats, and current protection strategies. This information can then be used to establish the security requirements of the enterprise, which is the goal of the first phase of OCTAVE.

Phase 2, Identify Infrastructure Vulnerabilities
Phase 2 of OCTAVE builds on the information captured during Phase 1 by mapping the information assets of the organization to the information infrastructure components (both the physical environment and networked IT environment) to identify the high-priority infrastructure components. Once this is done, an infrastructure vulnerability evaluation is performed to identify vulnerabilities. As in Phase 1, standard catalogs of information are used; for example, standard intrusion scenarios and vulnerability information are used as a basis for the infrastructure vulnerability evaluation. At the conclusion of Phase 2, the organization has identified the high-priority information infrastructure components, missing policies and practices, and vulnerabilities.

Phase 3, Determine Security Risk Management Strategy
Phase 3 of OCTAVE builds on the information captured during Phases 1 and 2. Risks are identified by analyzing the assets, threats, and vulnerabilities identified in OCTAVE's earlier phases in the context of standard intrusion scenarios. The impact and probability of the risks (also called the risk attributes) are estimated and subsequently used to help to prioritize the risks. The prioritized list of risks is used in conjunction with information from the previous phases to develop a protection strategy for the enterprise and to establish a comprehensive plan for managing security risks, which are among the goals of Phase 3.

OCTAVE deals with infrastructure vulnerabilities in Phase 2, and standard catalogues are used. It could not be a good solution for supervision, and for critical infrastructure components protection, a business continuity approach is lacking.

## 5.4. European supervision

“Requirements for IT in European supervision authorities” study helps to answer the question of what requirements are reasonable to ensure security and which of them are obligatory.

Next, description of the study of requirements in the IT area in European countries’ supervision authorities follows.

A study on how European supervision authorities regulate the IT area was conducted in August 2008. 27 European Union countries, Norway and Croatia were surveyed.

The information and materials about the requirements were collected from relevant web-pages and a simple keyword search gave results for only one third of the countries. In setting up the keywords, the IT field was divided into three parts – IT governance, information security and business continuity and lower-lever topics.

Considering the poor results with the keyword search, an e-mail was compiled with the generic e-mail addresses of the supervision authorities. The e-mail contained the following request:

“I am writing to you on behalf of the Estonian Financial Supervision Authority, where I am responsible for IT field supervision. Since we are conducting a small survey regarding what kind of requirements are in place for the IT field in the financial sector throughout European Union Member States, we have already examined your web-sites, but we have been unable to locate clear documents or links to the relevant information. We are interested in the whole financial sector (banking, insurance, etc.) and we are covering the main components of IT (IT governance, information security, business continuity). The results of this survey will be used for the improvement of our regulations in the IT field of supervised entities.

Considering the information above, please give a short answer to the following questions:

1. What kinds of regulations contain requirements for the IT field of supervised entities in your country?

2. Are these regulations freely available via the Internet?

2.1. If so, is it possible to provide the exact link to the adequate information?

2.2. If not, is it possible to send the relevant files via e-mail?

3. In case the relevant information is only for internal use, could you please describe what are the common demands for the IT field of supervised entities?”

Responses were received to about one half of the sent e-mails, accounting for another one third of the participating countries. The other third of the countries did not answer the e-mail and keyword-searches also failed to provide a result, so there is no information whether they have established IT requirements or not and what kind of requirements they may be. The results of the study are composed based on two thirds of the participating countries and the author considers it adequate enough to make reasonable conclusions.

Categories and statistics about different areas are illustrated with next three figures following the main themes.

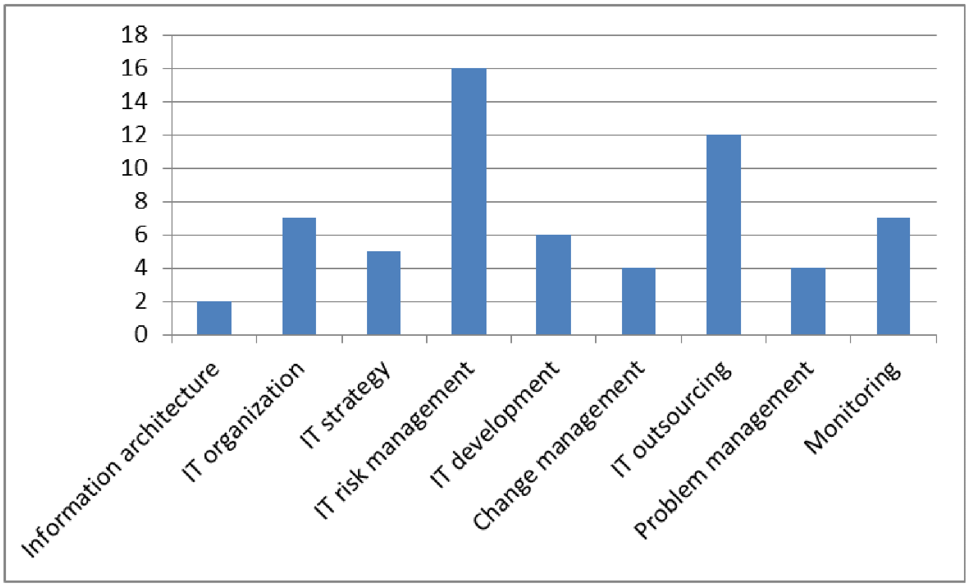

**Figure 5.1 Summary of study of European supervision – IT governance**

Explanation for presented columns follows:

Information architecture
Only two countries are mentioned – Estonia thoroughly and the Netherlands slightly

IT organization
7 countries thoroughly, 6 countries slightly and 10 countries do not mention

IT strategy
5 countries thoroughly, 2 countries slightly and 16 countries do not mention

IT risk management
16 countries thoroughly, 4 countries slightly and 3 countries do not mention

IT development
6 countries thoroughly, 5 countries slightly and 12 countries do not mention

Change management
4 countries thoroughly, 5 countries slightly and 14 countries do not mention

IT outsourcing
12 countries thoroughly, 3 countries slightly and 8 countries do not mention

Problem management
4 countries thoroughly, 3 countries slightly and 16 countries do not mention

Monitoring

7 countries thoroughly, 4 countries slightly and 12 countries do not mention

For IT governance topics, a lot of attention is paid to the IT risk management, outsourcing and monitoring. Less attention is paid to the information architecture and this indicates that the architecture is left to decide by supervised entities.

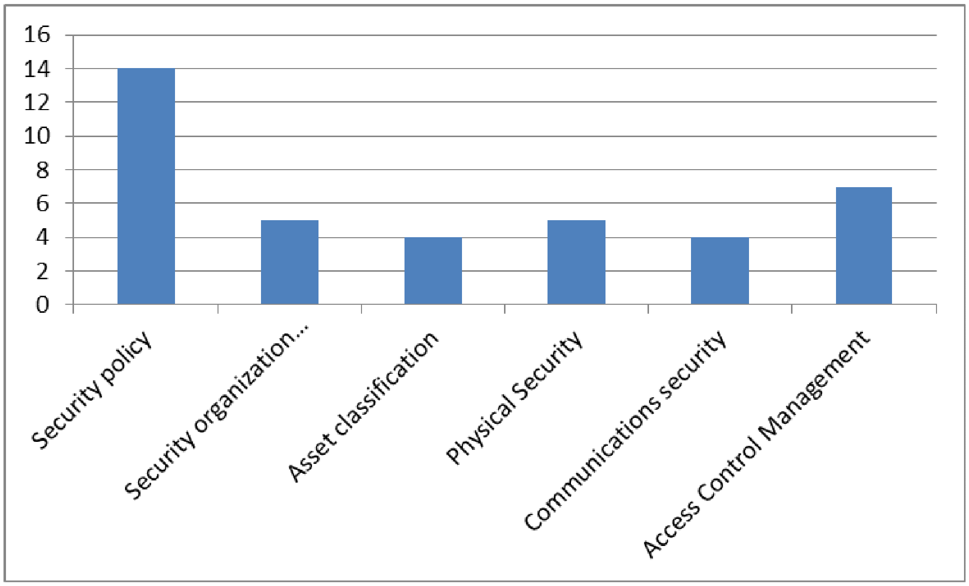

**Figure 5.2 Summary of study of European supervision – information security**

Explanation for presented columns follows:

Security policy
14 countries thoroughly, 2 countries slightly and 7 countries do not mention

Security organization structure
5 countries thoroughly and 18 countries do not mention

Asset classification
4 countries thoroughly, 2 countries slightly and 17 countries do not mention

Physical Security
5 countries thoroughly, 5 countries slightly and 13 countries do not mention

Communications security
4 countries thoroughly, 5 countries slightly and 14 countries do not mention

Access Control Management
7 countries thoroughly, 8 countries slightly and 8 countries do not mention

For information security governance, a lot of attention is paid to the information security policy and access control management. Less attention is paid to information security organization and information assets classification.

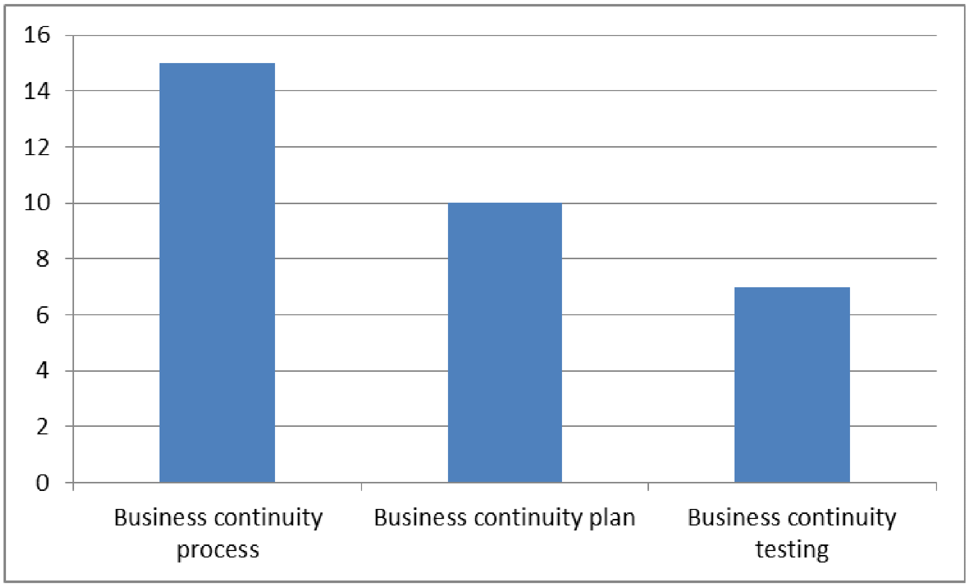

**Figure 5.3 Summary of study of European supervision – business continuity**

Explanation for presented columns follows:

Business continuity process
15 countries thoroughly, 3 countries slightly and 5 countries do not mention

Business continuity plan
10 countries thoroughly, 3 countries slightly and 10 countries do not mention

Business continuity testing
7 countries thoroughly, 4 countries slightly and 12 countries do not mention

Conclusion and discussion

As a first conclusion, eight countries have a rather high level of regulation, five countries have mid-level regulation and nine countries have a low-level of information technology regulation. There is no information about six of the countries, and one of respondents announced that they do not have specific regulations for information technology.

As next conclusion, there is remarkable difference between countries in connection with IT field regulations.

The results of the study, about how the IT field is regulated in European countries, could be used as follows:

- In setting up the requirements for information security in Estonia, consider mainly excellent examples such as Greece, Finland, Slovakia, the Netherlands and Latvia.
- Later, when analyzing all of the requirements and pointing out the criteria for assessment, use descriptions of those requirements which are handled thoroughly as a comparison.

## 5.5 Requirements in guidelines

In light of existing guidelines, it can be stated that between already covered topics, i.e. IT governance and business continuity, the topic of information security stands. In setting up the requirements for information security it is presumed that information security begins when by IT governance a risk assessment is conducted and begins choosing the measures to deal with risks. Information security area ends when the presumptions for business continuity and disaster recovery are performed, for example, backups and monitoring. Considering that, it should be stated that next the main attention goes to information security and for IT governance and business continuity requirements are only explained.

The outcome of study is used for further analysis. The results were used to guide or develop Estonia's Advisory Guidelines of the Supervision Authority and these are freely available:

- Advisory Guidelines of the Financial Supervision Authority http://www.fi.ee/failid/IT_governance.pdf
- Requirements for the organization of the field of information security http://www.fi.ee/failid/information_security.pdf
- Requirements for Organizing the Business Continuity Process of Supervised Entities http://www.fi.ee/failid/Business_continuity.pdf

As one new guideline paper is published, it seems to the right time to make necessary changes in existing guidelines. In practice, supervisors have not experienced significant problems with guidelines, but some little changes are necessary. The main point is that the similar chapters about information security and business continuity were included into existing guidelines and now, when there is an idea to work out special guidelines for named topics, the existing chapters will be removed to avoid disorder.

As a result of this chapter, the practices for setting up the requirements and common European supervision practices were surveyed and Estonian supervisory guidelines process and documents were presented. The research continues with analysis how the stated requirements may influence on the supervised entities and determining the criteria for requirements to start with compliance assessment issues.

# 6. Compliance with the requirements

In this chapter, first the compliance issues are discussed and next “what does conformity to the requirements mean for subjects?” is studied and last “which kinds of criteria indicate the conformity?” is studied. To deal with possible costs for initiatives to conform to supervisory requirements, the supervised entities were studied about how they today conform to requirements and is there a large gap between existing and required ones.

## 6.1. Compliance issues

Bruce et al. (2006) highlight future trends about the need for continuous auditing. In their paper (page 83) they state that:

> „There are indications from leading audit practitioners that the market is expecting the best performing companies to report their operating results more rapidly, and some believe this will be a requirement in the not-too-distant future. The marketplace may soon demand a shift away from the traditional year-end audit to a more continuous audit (CA) model. A continuous audit model is:
> a methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditors’ reports issued simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter.“ (CICA/AICPA 1999, 5)

Continuous auditing gives some impetus for continuous IT supervision and IT supervision method already takes the trend coming soon into account.

What do IT auditors concern about follows, for example, the topics discussed in IT Audit Topics Research Symposium. Symposium attendees discussed:

- The need to reach a consensus on the value of IT in an audit environment.
- The problems faced by internal auditors when monitoring IT controls.
- The use of metrics to measure audit performance.
- The related standards, frameworks, legislation, and the best practices for improving IT controls, namely
- ISACA's Control Objectives for Information and related Technology framework and the IT Infrastructure Library.
- The benefits of conducting research in the area of IT controls, such as the use of better metrics, the collection of needed empirical evidence, more guidance and knowledge on the best practices, and tools to help inexperienced auditors perform their work.
- The expected results and deliverables from such research, including better guidance.

To demonstrate how IT control has been observed in the specific field, more specifically in connection with financial sector, next IT Governance Institute (ITGI) books are highlighted.
IT control objectives for Sarbanes Oxley (ITGI, 2006, page 9):

> "There is no such thing as a risk-free environment, and compliance with the Sarbanes-Oxley Act does not create such an environment. However, the process that most organizations will follow to enhance their system of internal control to conform to the Sarbanes-Oxley Act is likely to provide lasting benefits. Good IT governance over planning and life cycle control objectives should result in more accurate and timely financial reporting.
>
> …
>
> The work required to meet the requirements of the Sarbanes-Oxley Act should not be regarded as a compliance process, but rather as an opportunity to establish strong governance models designed to result in accountability and responsiveness to business requirements."

IT control objectives for Basel II (ITGI, 2007, page 12):

> "Compliance has evolved from a tick-box, reactive approach to a forward-looking, proactive discipline that supports good governance. Compliance is now far broader than simply working through a list of all-or-nothing requirements, although rules-based compliance is still an important subset of overall compliance. In most cases, the compliance requirements set down in regulations or standards are maturity-driven and designed for continuous improvement over time. Market practice, benchmarks and new developments in business must be factored into the notion of compliance, given the constant changes and challenges of global business."

Deloitte conducted 2007 Global security survey: The shifting security paradigm, which purpose was to explore how is the state of information security changing within organizations and are these changes aligned with those of the rest of the industry. The top five initiatives were:

- Access and identity management (50%);
- Security regulatory compliance (49%);
- Security training and awareness (48%);
- Governance for security (37%);
- Disaster recovery and business continuity (37%).

The survey was conducted for financial institutions and the results are remarkable. It shows that so called softer side – key words like compliance, awareness, governance etc. are the must-initiatives.

Still there are under-researched areas in information technology auditing fields. Weidenmier and Ramamoorti (2006, p. 213) highlight some most important areas, which will be addressed by IT supervision method.

> "Internal controls also help ensure compliance with applicable laws and regulations (COSO 2004a, 109), an activity that becomes even more important in heavily regulated industries such as healthcare and financial services. Accordingly, yet another significant governance activity performed by internal auditors is compliance assessment."

## 6.2. Benefits and costs

When setting up regulatory requirements for handling IT in financial sector institutions, the most important aspect to consider is the economic impact. Ghose and Rajan (2006) have studied these issues taking Sarbanes-Oxley legislation and IT security for examination. While Sarbanes-Oxley or SOX is applicable for the United States, the similar approaches for the European financial sector are established by Basel II regulations.

In conclusion, Ghose and Rajan (2006, p. 17) mention that:

> "Our analysis reveals that mandatory investments in regulatory compliance may have several unintended consequences such as reduction in optimal production quantities, a decrease in the extent of market competition and an overall reduction in social welfare. In particular, our results highlight that smaller sized firms are more drastically affected than larger firms and this process if unchecked, may lead to a severe long term impact on the operations of both capital as well as product markets. Because small cap firms are an important engine of economic growth and technological innovation, the ripple effects of regulations like the service oriented architecture (SOA) will be felt throughout the economy. One major implication of this is that some changes in regulations need to be enforced sooner rather than later by the federal government.
>
> In our ongoing research, we will extend this theoretical model to look at the optimal levels of information about material weaknesses that should be disclosed by firms in the presence of legislation through entities like the Securities and Exchange Commission (SEC) and verification through intermediaries such as auditing firms."

As a security level is raised, the expenses increase essentially. Otherwise, this tendency assumes from regulators the paying of more attention to economic issues caused by tight regulations.

ISO27k generic business case highlights some benefits and costs regarding information security (Hinson, 2008).

Benefits:

- Reduces information security risks, reduces probability and impacts of info-security incidents;
- Certification to an international standard, marketing advantages, etc.;
- Structured, coherent approach, comprehensive risk assessment;
- Focuses info-security spending to the greatest advantage;
- Demonstrable governance.

Costs:

* Project management, project resources;
* Organizational change requires organizational resources;
* Design, development, testing, implementation;
* Certification and surveillance visits;
* Ongoing operation and maintenance.

The most important aspects of ISO27k are benefits because it reduces probability and the impact of information security incidents, and in connection with costs, first design, development, testing, implementation and after that, ongoing operation and maintenance.

The solutions are sought to optimize IT security costs. One example comes from Estonia, where evolutionary algorithms are used for optimizing IT security costs (Kirt, Kivimaa, 2010). As a result it was pointed that the evolutionary approach is applicable to the security of the cost/confidence optimization task and it allows generating equivalent security profiles for every cost level.

The supervised entities must also consider universal problems in accounting (Virkkunen 1951):

1. The range problem – which costs and benefits are included?
2. The measurement problem – how to measure costs and benefits?
3. The valuation problem – how to assign value to costs and benefits?
4. The division problem – how to divide costs and benefits between products and services?

and division problem (Järvinen 2004), which is divided into two sub-problems:

4 a. The allocation problem – how overhead costs are allocated between products and services?

4 b. The periodization problem – how is a lot cost divided into periods?

In IT-world, the terms like *Total cost of ownership (TCO)* and *Return on investments (ROI)* are accepted, today are the relevant terms for information security presented – Total Cost of Security (Cameron, 2007):

> "… an approach to integrate operational security metrics with business decision-making, especially budget decisions, investment decisions, priority decisions, strategy decisions, and tactical decisions in day-to-day implementation or execution. Drawing an analogy to the Total Quality Management movement, the approach is called "the Total Cost of Security

> (or Insecurity)". By dividing costs into three categories: "Budgeted", "Self-insured", and "Catastrophic", it shows how operational security metrics can be used in each of these cost estimates. This approach makes the most of existing information, aligns with decision-making processes, and avoids the problem of conflating reliable and unreliable estimates. In addition to helping with security cost and performance management, this approach highlights the importance of organization learning and discovery."

and Return on Security Investment (Sonnenreich et al. 2010, p. 1):

> "Before spending money on a product or service, decision-makers want to know that the investment is financially justified. Security is no different -- it has to make business sense. What decision-makers need are security metrics that show how security expenditures impact the bottom line. There's no point in implementing a solution if its true cost is greater than the risk exposure. This paper will present a model for calculating the financial value of security expenditures, and will look at techniques for obtaining the data necessary to complete the model."

Supervisors, in establishing security requirements, have to consider that supervised entities may calculate Total Cost of Security and Return on Security Investment.

## 6.3. Information security valuation

Also, the need for focus on value is an important consideration. Dhillon and Torkzadeh (2006, p. 1) studied the value-focused assessment of information system security in organizations:

> "A large part of IS security research is technical in nature with limited consideration of people and organizational issues. The study presented in this paper adopts a broader perspective and presents an understanding of IS security in terms of the values of people from an organizational perspective. It uses the value-focused thinking approach to identify 'fundamental' objectives for IS security and 'means' of achieving them in an organization.
> …
> The findings suggest that for maintaining IS security in organizations, it is necessary to go beyond technical considerations and adopt organizationally grounded principles and values."

Investments in security could yield a positive impact on the enterprise and how to assess such impact, Ramachandran and White (2005, p. 1) suggest approach:

> “Existing estimators such as Annual Loss Expectancy (ALE) and Cost Benefit Analysis (CBA) have been widely used to quantitatively perform risk analysis and to identify tangible benefits from investments in IT-STPs. Intangible benefits from IT-STPs, which are as critical as tangible benefits, are harder to measure. The lack of metrics for assessing these intangibles provides a challenge for comprehensively assessing the value of investment in IT-STPs. This paper explores past IT payoff literature to develop a comprehensive methodology for assessing the impact of IT-STPs, which can better assess both the tangible and intangible benefits. In this light, we present a Complementarity Based First-Order Effects (CoBFOE) approach to assess the impact of investments in IT-STPs based on Business Value Complementarity (BVC) model. An illustration of how the CoBFOE approach could be used in an organizational setting is also discussed.”

Deciding about security level, main purpose of the supervision is to avoid financial losses. Aberdeen Group (2005) has released Best Practices in Security Governance, and besides it is mentioned that:

> “Firms operating at best-in-class levels are lowering financial losses to less than one percent of revenue whereas other organizations are experiencing loss rates that exceed five percent.”

The financial sector, especially the banking sector, plays the leading role in information security in Estonia, and financial supervision must support such a situation in order to avoid losses. Hence, the business value of information technology gets essential.

> “Unfortunately, the results of recent studies of IT business value are at best inconclusive. While some authors have reported positive impacts, others have found negative or no impacts. At least two limitations are posed in those recent works. First, IT is often treated as a single factor. Given the complexity of the technology and the difficulty of implementing it in organizations, some systems may be effective, while others may bring negative returns. Therefore, by aggregating over all systems, the favorable impact of effective systems may be nullified by poorly designed systems. Second, many of the earlier studies use cross-sectional or short-time series data. If there is a lag in achieving IT business value, data covering a limited time period may not reveal the impact.” (Mukhopadhyay et al., 1995, p. 137)

Information security cannot be a thing in itself. ISACA (2009), one of the most accepted representative body of these issues introduces a business model.

> “Enterprises too often view information security in isolation: the perception is that security is someone else’s responsibility and there is no collaborative

> effort to link the security program to business goals. It is easy for this compartmentalized approach to lead to weaknesses in security management, possibly resulting in serious exposure. From a financial perspective, it is possible for this lack of comprehension to result in unnecessary expenditure on security and control. From an operational perspective, information security efforts may not achieve the intended business benefit, resulting in information at risk."

In setting up the regulatory requirements, the best practices and standards should not be ignored. What could be the value of IT controls come from these standards and best practices, Behr et al. (2010) set some hypotheses.

> "Information technology managers are confronted with a myriad of best-practice frameworks for information technology service management. These frameworks include the Information Technology Infrastructure Library (ITIL) and the Control Objectives for Information and related Technology (COBIT). Advocates of these frameworks promote the value of these guidelines in achieving cost reductions and improving business processes. The problem is that implementing these frameworks involves substantial upfront costs. Many practitioners view them as simply another level of bureaucracy. The purpose of this paper is to empirically determine whether IT controls affect the value, effectiveness, efficiency, and security of information-technology operations. We hypothesize that implementation of IT controls improves IT efficiency, IT effectiveness, IT security, and indirectly, business value."

## 6.4. Study about current situation

To conform to the new requirements may cause subjects additional costs for IT-related operations, i.e., more controls, improved physical security measures etc. What is the real situation is studied as following.

The study about how do supervised entities conform to the requirements – helps to answer to the question about whether the economic aspects of being in compliance with the requirements are reasonable.

The purpose of the next study is to find out how the subjects fulfill the requirements for the information technology field today. It helps to provide an appreciation for how adequate the criteria are and what kind of changes for increasing or decreasing the number of requirements are needed.

Not all of the supervised entities from Estonia are involved in this survey, but the part of the financial sector for making a general conclusion regarding the market situation is involved. Interviews were performed within all the banks in the market, because the banking sector is a leader there and market requirements have to cover its highest level. The next step of the survey will cover a portion of the insurance firms, including both life and non-life insurance companies, but also some investment firms and fund management companies. It provides some insight on how to set up an index system for subjects and build up a weighting system for requirements.

The information was collected from 7 banks, 3 insurance companies, 2 fund management companies and 2 investment firms. Considering the current market situation, a lot of bigger subjects are connected with other subjects meaning that their IT infrastructure is the same, for example, banks and investment firms. Also, in the market there are life insurance and non-life insurance firms using the same IT infrastructure.

The data gathering technique was interview with responsible persons following the indicative collection of questions and analysis of documents.

Control of relevant documentation and discussion points for clarifying the content was selected following the main topics of best practices and standards – for IT governance the COBIT methodology was used, for information security an international standard ISO/IEC 27001 was used and for business continuity, the Basel guidelines were used.

- IT strategy
    - How is IT strategy alignment to business objectives ensured?
    - How is IT strategy document development implemented?
    - What kinds of IT development plans IT strategy initiates?
    - What is the time period for updating IT strategy?

- Information assets
    - How are information assets classified?
    - How are the owners to the information assets appointed?
    - Do information asset classes have security levels and how it will be found out?
    - According to the security levels, are there predefined security measures determined?

- IT organization
    - How is necessary and suitable IT organization stated?
    - How is segregation of duties guaranteed?
    - For what services is outsourcing used?

- IT risk management
    - How are IT risks valued and how is continuous risk assessment organized?
    - Is acceptable residual risk established?

- Information security policy
    - Which kinds of information security principles are included in information security policy document?
    - What is the procedure of composing information security policy document?

  - On which basis is access granting process organized and how is this process controlled?
  - How is logging of operations and transactions inside of information systems organized?

- Business continuity plan
  - Is there current business continuity plan in place?
  - What is the procedure of composing the business continuity plan?
  - Which kinds of main components does business continuity plan include?
  - What is the time period for updating a business continuity plan?

- Business continuity testing
  - How is business continuity testing (including recovery testing) organized?
  - How are business continuity testing results analyzed and does it and how it affects the changes in business continuity plan?

- Significant business disruptions
  - Is significant business disruption conception defined?
  - Did significant business disruptions happen during current year and what was the reason?
  - Which kinds of proactive measures were taken to avoid significant business disruptions in the future?

General questions

- Has supervised entity experienced problems with implementing requirements of financial supervision guidelines?
- What is subject's view about: Is it necessary to clear up regulatory requirements more thoroughly?
- Is the implementation of regulatory requirements helpful for simplifying IT governance and auditing the IT field?
- Is it necessary to work out additional guidelines for certain topic and which ones?

The purpose of interviewing was to get an overview of how supervised entities met the requirements described in the guidelines. As a result, it will be presented whether or not the supervised entities follow the guidelines and how, and what are the main problems and deficiencies. Special attention is focused on information security issues.

All apparent requirements, which could in one way or another be aggregated under a common denominator, are considered in making the analysis. In practice, in adding the criteria under requirement, all the applicable objects are outlined.

A summary is presented in Tables 6.1, 6.2 and 6.3. Summary tables show what kind of internal regulation supervised entity has in connection with stated requirement. Summary tables include information about 7 subjects and replays for organizations using the same IT infrastructure and processes are removed.

| | **IT governance requirements** | | | |
|---|---|---|---|---|
| ***Subject*** | *IT description* | *IT organization* | *IT strategy* | *IT risk* |
| Subject 1 | IT functions | | IT strategy | |
| Subject 2 | List of IT services | IT structure | | Business impact analysis |
| Subject 3 | | IT organization | IT strategy | IT risk management |
| Subject 4 | IT description | IT description | | Risk consciousness |
| Subject 5 | IT overview | IT overview | IT overview | IT risk assessment |
| Subject 6 | Information assets, infrastructure system | IT department, IT committee | IT strategy | Critical information assets |
| Subject 7 | | IT division structure | IT development directions | |

**Table 6.1 Subjects' conformity to the IT governance requirements**

| | **Information security requirements** | | | | |
|---|---|---|---|---|---|
| ***Subject*** | *Information security policy* | *Monitoring* | *Access manageme nt* | *Backups* | *Logging* |
| Subject 1 | Information security measures | Information security measures | Access rights administrat ion | Information security measures | Information security measures |

| | | | | | |
|---|---|---|---|---|---|
| Subject 2 | IT security policy | | | | |
| Subject 3 | Information security policy | | Access rights procedure | The procedure of making and keeping backups | IT logging |
| Subject 4 | Risk consciousness | Risk consciousness | | | |
| Subject 5 | | | | | |
| Subject 6 | Information security policy, information security rules | System administration procedure | Password administration rules, administration of user accounts | Business continuity and recovery | |
| Subject 7 | Information security policy | | Regulation of access | | Control traces |

**Table 6.2 Subjects' conformity to the information security requirements**

| | **Business continuity requirements** | | |
|---|---|---|---|
| ***Subject*** | *Business continuity plan* | *Recovery plan* | *Business continuity testing* |
| Subject 1 | Business continuity plan | Business continuity plan | Schedule |
| Subject 2 | | IT recovery plan | Schedule |
| Subject 3 | IT continuity | Recovery plan | Schedule |
| Subject 4 | Business continuity plan | Business continuity plan | Schedule |

|  |  |  |  |
|---|---|---|---|
| Subject 5 | Common business continuity plan |  | Schedule |
| Subject 6 | Business continuity and recovery | Business continuity and recovery | Schedule |
| Subject 7 |  |  | Schedule |

**Table 6.3 Subjects' conformity to the business continuity requirements**

Conclusions

In making conclusions, a decision was made to import all of the analyzed and highlighted criteria into the next phase. Conclusions also give some directions about how the criteria will be dealt with further.

For performing an analysis, the guide of ISO 27k implementers was also used. (ISO27001 security forum, 2007).
Firstly, this sub-study provides the answers to what could be the criteria for complying with requirements, and secondly what measures have been taken by supervised entities thus far. The main purpose is to avoid a situation where measures become too overcharged for supervised entities.

This chapter gave some confidence that the requirements stated in Chapter 5 are not too burdensome for supervised entities and in general, the main activities are carried out to meet the requirements. The study may proceed with finding out the criteria to meet the requirements.

# 7. Compliance criteria

In this chapter we deal with compliance assessment in principle and give the main outcome of entire research. During current research, the first version of relevant handbook is compiled and this handbook have to be a subject of continuous improvements considering the real assessments, the financial sector changes and developments in this are wider. Compliance criteria and weighting help to answer the question of what kinds of criteria should be used to ensure compliance with requirements and how to assure equal treatment of market participants. Criteria handbook as it is called will be presented in Appendix 2 due to the extensive content.

## 7.1. Compliance assessment issues

The question rises about how mandatory the requirements should be to show compliance. Six Design Theories for IS Security Policies and Guidelines (Siponen and Iivari 2006, pp. 453-454) give some implications.

> "According to the conservative-deontological theory, the IS security policy cannot be violated. The liberal-intuitive theory desires the same response, since according to the security rules of the organization, every exception must be approved by the senior security specialist. According to the prima-facie theory, IS security policy can be violated provided that:
>
> (i) business objectives and security requirements are in conflict, and
>
> (ii) the benefits of compromising those guidelines outweigh the benefits of complying with them.
>
> The virtue theory regards IS security policy compliance as voluntary… If the software house had a utilitarian theory in place, they would need to follow the IS security guidelines in normal circumstances. In exceptional situations, or situations suspected to be exceptional, a resolution is arrived at by means of utilitarian happiness calculus. In the case of the universalizability theory, the IS security policy can be violated in exceptional situations, provided that the action in question satisfies one of the two universalizability rules."

Certainly, within the meaning of supervision, compliance with requirements cannot be voluntary. Otherwise, I think that a supervisor would be unable to decide about business. For that reason, IT supervision requirements are built as "comply or explain".

NetIQ (2008) highlights the challenges the organizations face in dealing with business continuity (BC) issues and seeking the answer to the question "How to reconnect compliance, security and business goals."

> "Many organizations are facing a growing crisis in their compliance and security management programs. Compliance programs that deliver little in the way of measurable security improvements, yet place ever-greater resource demands on administrators, have left businesses urgently searching for a more sustainable and scalable approach.
>
> The pressure on organizations to meet increasing numbers of regulatory compliance goals is steadily rising, driven in no small part by a growing public awareness of corporate malpractice and the risks of data theft. Regulatory and industry bodies have responded to public concern by mandating increasingly broad controls with more stringent penalties for non-compliance. Further, as organizations seek to enforce policy-based compliance standards across their business, they may impose additional or even contradictory goals on administrators and compliance officers."

Besides, some principle questions can get some direction, for example, to decide about compliance metrics, next should be considered (Brotby 2009):

1. The criticality and sensitivity of assets involved
2. The level of risk the assets are exposed to
3. The state of compliance with the relevant procedure
4. The degree of procedural competence of personnel
5. The adequacy of resources
6. The reliability and accuracy of the metrics themselves
7. The functionality, efficiency, and appropriateness of the procedure

And what unit of measurement is useful for compliance (Brotby 2009)?

> "Percentage is a common measure and would seem obvious, but upon consideration it proves to be inadequate. In some cases, only 90 per cent level of compliance with the steps required in a critical procedure can be fatal. So, for important or critical procedures we need 100 per cent level of compliance with all the steps, 100 per cent of the time. Accordingly, the metric doesn't need to scalar, just binary – either the procedures are consistently followed or they are not.
>
> It can be argued that a 100 per cent level of compliance is unrealistic and high percentages might be adequate. For non-critical procedures, that might be sufficient, but in the case of heart surgery or flying jumbo jets, the argument is not persuasive, and procedural failures have resulted in fatalities and huge negligence awards. Given potentially catastrophic consequences, few knowledgeable managers would accept only high percentages of critical procedural compliance as acceptable."

## 7.2. Compliance assessment principles

The main idea of compliance control, considering the IT supervision method, is to examine organizations' IT domain to ensure that it conforms to the established requirements. Conformance to specifications influences, amongst other, on the quality. The strengths of this approach include characteristics like precisely measurable, leads to efficiency, necessity for global strategy, specifications can be derived from customer needs and most appropriate for industrial customers. The weaknesses of this approach include characteristics like specifications vs. subjective perception of quality, inappropriate for services, may reduce adaptability and needs may expire. (Reeves and Bednar, 1994).

Setting up the requirements beforehand, three categories were presented for compliance criteria, IT field should also be presented as sum of three components:

1. IT governance – criteria should show good governance;
2. Information security – criteria should assure security;
3. Business continuity – criteria should ensure continuity.

For each component, three categories of criteria can be used in assessment as it is emerged from supervision practice:

1. Quantity - documented evidence that necessary security measures are described and approved, i.e., we can count the documents;
2. Quality - substantive analysis that security measures are accurate and complete;
3. Control – control or auditing issues to confirm that security measures are utilized.

All the categories will be considered for assessing each requirement.

The purpose for a weighting system is to ensure equal treatment. Taking into account the features of the financial market, a certain classification should be performed in assessing compliance with requirements and equal treatment should be the focus of such classification. The main idea is simple, which states that bigger entities with bigger market share have stronger requirements and smaller firms with smaller market share have weaker requirements. It seems reasonable to establish common requirements for all market participants, but to measure the compliance differently. Considering the current practice of supervision, and considering the financial market structure, the following classifications should be reasonable:

- I level (BB) - bigger banks
- II level (SB) - smaller banks
- III level (BI) - bigger insurance companies
- IV level (SI) - smaller insurance companies
- V level (IF) - investment firms
- VI (FM) - fund management companies

The weighting process will be used in making sense of requirements, and in reality the criteria vary depending on the level of the supervised entity. It means that in general the requirements for supervised entities are the same, for example, information security has to be an issue and information security has to be handled, the mechanisms have to be set up for ensuring business continuity, etc. But depending on the size and complexity of the subject, the criteria to meet the requirements can be different and the next such kind of differentiation is highlighted.

## 7.3. Criteria handbook

This part of the research describes how the organizations will be measured against the requirements stated before. The general approach is to develop an assessment handbook which includes forms for each requirement. In this form, three main sectors are described: firstly the freely available information about the requirements, secondly the content of the requirements is described in terms of how it works for supervised entities and lastly, how the requirements will be assessed based on a different group of supervised entities.

This handbook describes requirements for IT governance, IT security and business continuity in Estonian financial sector.

During development of the criteria handbook and the first real assessment (use case), the requirements for IT security governance can be changed.

Conclusion

The results of Study 3 are presented in Appendix 2.

The criteria handbook created during study described in this chapter is the most important outcome of the whole research. The handbook summarizes the results and ideas from previous sub-studies and gives a tool for exercising compliance assessment. It provides the criteria for assessment through deep analysis and also the question of equal treatment is addressed. The research proceeds with scoring issues based on the requirements and criteria stated beforehand.

# 8. Compliance scoring

In this chapter some widely known security assessment approaches are described and possible measures and metrics are studied. Using this knowledge, the scoring scale for IT supervision is proposed and a real use case will be conducted. This is the first attempt to check applicability of criteria handbook in practice.

## 8.1. Security assessment approaches

BSI (ISKE)

Terms used in the ISKE methodology are treated as follows:

- availability – availability of timely information and services for authorized persons;
- integrity – protection of information against counterfeiting and unauthorized alteration;
- confidentiality – protection of information against unauthorized publication.

In principle, the idea from the ISKE methodology (BSI, ISKE, 2010) about information assets security could be used by supervisors to determine the security need. IT supervision practice points out that some supervised entities use such ISKE predetermined scales as following.

For data availability, in ISKE the next scale is used:
0 – reliability – not important; performance – not important;
1 – reliability – 90% (maximum tolerable interruption for one week ~ twenty-four hours); response time - hours;
2 – reliability – 99% (maximum tolerable interruption for one week ~ 2 hours); response time - minutes;
3 – reliability – 99,9% (maximum tolerable interruption for one week ~ 10 minutes); response time - seconds.

For data integrity, in ISKE the next scale is used:
0 – establishing data source, data change and deleting of data is not important; control of data completeness and appropriateness is not necessary;
1 – possibility to establish data source, data change and deleting of data; control of data completeness and appropriateness is necessary in special cases and as appropriate
2 – possibility to establish data source, data change and deleting of data; periodic control of data completeness and appropriateness;
3 – establishing data source, data change and deleting of data should be provable; real time control of data completeness and appropriateness.

For data confidentiality, in ISKE the next scale is used:
0 – public information: access is not restricted;

1 – information for internal use: access is restricted, there should be legitimate interest to access the information;
2 – secret information: access only for particular user groups, there should be legitimate interest to access the information;
3 – top secret information: access only for particular users, there should be legitimate interest to access the information

COBIT, CMM (ISACA, 2010)

A maturity model is a set of structured levels that describe how well the practices and processes of an organization can produce required outcomes. According to COBIT perspective, these practices and processes are linked with IT governance and information security issues.

0 Non-existent. Complete lack of any recognizable processes. The enterprise has not even recognized that there is an issue to be addressed.
1 Initial. There is evidence that the enterprise has recognized that the issues exist and need to be addressed. There are, however, no standardized processes; instead there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.
2 Repeatable. Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.
3 Defined. Procedures have been standardized and documented, and communicated through training. It is, however, left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices.
4 Managed. It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
5 Optimized. Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modeling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

While previous approaches give assessments for establishing security level (BSI) or help to address security level (COBIT, CMM), there is not much about assessment of security measures adequacy which is important for IT supervision.

## 8.2. Security assessment issues

As a need for information security measurement increases, this area gets more and more attention. For example, MITRE Corporation (2010) launched a specialized web site to help discuss security measures.

> "MITRE, in collaboration with government, industry, and academic stakeholders, is improving the measurability of security through enumerating baseline security data, providing standardized languages as means for accurately communicating the information, and encouraging the sharing of the information with users by developing repositories."

Information assurance (IA) measures and metrics are proposed by Vaughn, Henning and Siraj (2002). They highlight 10 (it is 5+5) fundamental characteristics of metrics:

1. Objective/subjective – objective metrics are more desirable but subjective metrics are more readily available;
2. Quantitative/qualitative – quantitative metrics are more preferable because they are discrete, objective values;
3. Static/dynamic – dynamic metrics evolve with time and they are more useful because the best practices change over time with technology;
4. Absolute/relative – absolute metrics do not depend on other measures, relative metrics are only meaningful in context;
5. Direct/indirect – direct metrics are generated from observing the property that they measure. Indirect metrics are derived by evaluation and assessment. It is preferred to measure behavior directly, but it is not always feasible.

All described characteristics should be counted afterwards in choosing the measures and metrics.

There have been other attempts to work out solutions for security assessment. For example, EIS by Johansson and Johnson (2005, p. 136) is proposed.

> "The purpose of the overall research project is to develop a method for the assessment of Enterprise Information Security (herein denoted as the EIS method). This EIS method presents an indicative single value on a scale, i.e., and EIS score. Secondly, it presents sound estimates of the credibility of the assessment score. Thirdly, the EIS procedure is designed to be as cost-effective as possible."

The method for enterprises cannot be used for the whole sector, and the main reasons are highlighted. For example, enterprises need an approach for developing risk management; supervision has to control how the risk management works; enterprises have to calculate the level of resources necessary to ensure business continuity; supervision has to control that business continuity is ensured; etc.

IT Audit Checklist Series for information security can be useful tool for IT supervision too.

> „IT Audit Checklists are a series of topical papers that provide practical guidance for IT, compliance, and business managers on preparing for successful internal audits of various aspects of their operations. In addition to helping managers understand what auditors look for and why, the IT Audit Checklists can help managers proactively complete self-assessments of their operations, thereby identifying opportunities for system and process improvements that can be performed in advance of an actual audit.“ (IT Compliance Institute, 2006, p. 2)

As a conclusion about security measurement, all leads to that we do not have an universal solution for information security or compliance assessment and kind of CMM – capability maturity model (Software Engineering Institute, 1993) approach will be used. It helps to decide what the situation of information security governance is:

0 Non-existent.
1 Initial.
2 Repeatable.
3 Defined.
4 Managed.
5 Optimized.

By supervisor's side, we have to consider that any kind of assessment or score will initiate some action. Hauser and Katz (1998, p. 2) point out the idea.

> "Our thesis is that every metric, whether it is used explicitly to influence behavior, to evaluate future strategies, or simply to take stock, will affect actions and decisions. If a brand manager knows that, in his or her company's culture, a "good brand is a high share brand," he or she will make decisions to maximize market share – even if those decisions inadvertently sacrifice long-term profit or adversely affect other brands in the company's portfolio."

In conclusion, some myths about metrics should be highlighted using Hinson's words (2006, pp. 2-5).

1. Metrics must be "objective" and "tangible"
2. Metrics must have discrete values
3. We need absolute measures
4. Metrics are costly
5. You can't manage what you can't measure and you can't improve what you can't manage
6. It is essential to measure process outcomes
7. We need the numbers

For each myth, an argumentation is presented.

## 8.3. Security measures

Percentage is good for making an assessment:

1. It gives a flexibility – assessment scale does not have any kind of limits for making an assessment;
2. It gives a possibility to transfer the scores into another scale as discussed in next section – whatever the final appreciation is, percentage scale gives possibility for transformation;

These numbers are not directly usable, but can be used for creating the appropriate scales.

Also, the need for assessing IT risks with the same scale as, for example, operational risks and credit risks, should be considered. The scale in financial supervision in Estonia is implemented and IT supervision risk factor could be presented as follows:

- High risk – for example compliance 0%-25%
- Measured risk - for example compliance 26%-50%
- Acceptable risk - for example compliance 51%-75%
- Low risk - for example compliance 76%-100%

In composing IT supervision method, besides compliance information security operational risk metrics should be considered. According to the Basel Committee on Banking Supervision, this includes the following areas:

- Internal fraud – losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party;
- External fraud – losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party;
- Employment practices and workplace safety – losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events;
- Clients, products, and business practice – losses arising from an unintentional failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product;
- Damage to physical assets – losses arising from loss or damage to physical assets from natural disaster or other events;
- Business disruption and system failures – losses arising from disruption of business or system failures;
- Execution, delivery, and process management – losses from failed transaction processing or process management, from relations with trade counterparties and vendors.

(BIS, 2010)

## 8.4. Security metrics

For risk areas, the SABSA (2010) framework was used and now, in setting up the metrics for information security, risk management attributes which describe the business requirements for mitigating operational risk can be used.

| Business attribute | Attribute explanation | Metric type | Suggested measurement approach |
|---|---|---|---|
| Access-controlled | Access to information and functions within the system should be controlled in accordance with the authorized privileges of the party requesting the access. Unauthorized access should be prevented. | Hard | Reporting of all unauthorized access attempts, including number of incidents per period, severity and result (did the access attempt succeed?) |
| Accountable | All parties having authorized access to the system should be held accountable for their actions | Soft | Independent audit and review against Security Architecture Capability Maturity Model with respect to the ability to hold accountable all authorized parties. |
| Assurable | There should be a means to provide assurance that the system is operating as expected and that all of the various controls are correctly implemented and operated. | Hard | Documented standards exist against which to audit |
| | | Soft | Independent audit and review against Security Architecture Capability Maturity Model |
| Assuring honesty | Protecting employees against false accusations of dishonesty or malpractice. | Soft | Independent audit and review against Security Architecture Capability Maturity Model with respect to the ability to prevent false accusations that are difficult to repudiate. |
| Auditable | The actions of all parties having authorized access to the system, and the complete chain of events and outcomes resulting from these actions, should be recorded so that this history can be reviewed. The audit records should provide an appropriate level of detail, in accordance with business needs. | Soft | Independent audit and review against Security Architecture Capability Maturity Model |
| | The actual configuration of the | Hard | Documented target |

| | | | |
|---|---|---|---|
| | system should also be capable of being audited so as to compare it with a target configuration that represents the implementation of the security policy that governs the system. | | configuration exists under change control with a capability to check current configuration against this target. |
| | | Soft | Independent audit and review against Security Architecture Capability Maturity Model |
| Authenticated | Every party claiming a unique identity (i.e., a claimant) should be subject to a procedure that verifies that the party is indeed the authentic owner of the claimed identity. | Soft | Independent audit and review against Security Architecture Capability Maturity Model with respect to the ability to successfully authenticate every claim of identity. |
| Authorized | The system should allow only those actions that have been explicitly authorized. | Hard | Reporting of all unauthorized actions, including number of incidents, per period, severity, and result (did the action succeed?) |
| | | Soft | Independent audit and review against Security Architecture Capability Maturity Model with respect to the ability to detect unauthorized actions. |
| Capturing new risks. | New risks emerge over time. The system management and operational environment should provide a means to identify and assess new risks (new threats, new impacts, or new vulnerabilities). | Hard | Percentage of vendor-published patches and upgrades actually installed. |
| | | Soft | Independent audit and review against Security Architecture Capability Maturity Model of a documented risk assessment process and a risk assessment history. |
| Confidential | The confidentiality of (corporate) information should be protected in accordance with security policy. Unauthorized disclosure should be prevented. | Hard | Reporting of all disclosure incidents, including number of incidents per period, severity, and type of disclosure. |
| Crime-free | Cyber-crime of all types should be prevented. | Hard | Reporting of all incidents of crime, including number of incidents per period, severity, and type of crime. |
| Flexibly secure | Security can be provided at various levels, according to business needs. The system should provide the means to | Soft | Independent audit and review against Security Architecture Capability Maturity Model |

| | | | |
|---|---|---|---|
| | secure information according to these needs, and may need to offer different levels of security for different types of information (according to security classification). | | |
| Identified | Each unit that will be granted access to system resources and each object that is itself a system resource should be uniquely identified (named) such that there can never be confusion as to which entity or object is being referenced. | Hard | Proof of uniqueness of naming schemes. |
| Independently secure | The security of the system should not rely upon the security of any other system that is not within the direct span of control of this system. | Soft | Independent audit and review against Security Architecture Capability Maturity Model of technical security architecture at conceptual, logical, and physical layers. |
| In our sole possession | Information that has value to the business should be in the possession of the business, stored and protected by the system against loss (as in no longer being available) or theft (as in being disclosed to an unauthorized party). This will include information that is regarded as "intellectual property". | Soft | Independent audit and review against Security Architecture Capability Maturity Model |
| Integrity-assured | The integrity of information should be protected to provide assurance that it has not suffered unauthorized modification, duplication, or deletion. | Hard | Reporting of all incidents of compromise, including number of incidents per period, severity, and type of compromise. |
| | | Soft | Independent audit and review against Security Architecture Capability Maturity Model with respect to the ability to detect integrity compromise incidents. |
| Nonrepudiable | When one party uses the system to send a message to another party, it should not be possible for the first party to falsely deny having sent the message or to falsely deny its | Hard | Reporting of all incidents of unresolved repudiations, including number of incidents per period, severity, and type of repudiation. |
| | | Soft | Independent audit and review |

| | | | |
|---|---|---|---|
| | contents. | | against Security Architecture Capability Maturity Model with respect to the ability to prevent repudiations that cannot be easily resolved. |
| Owned | There should be an entity designated as “owner” of every system. This owner is the policy maker of all aspects of risk management with respect to the system and exerts the ultimate authority for controlling the system. | Soft | Independent audit and review against Security Architecture Capability Maturity Model of the ownership arrangements and of the management processes by which owners should fulfill their responsibilities, and of their diligence in so doing. |
| Private | The privacy of (personal) information should be protected in accordance with relevant privacy or “data protection” legislation, and so as to meet the reasonable expectation of citizens for privacy. Unauthorized disclosure should be prevented. | Hard | Reporting of all disclosure incidents, including number of incidents per period, severity, and type of disclosure. |
| Trustworthy | The system should be able to be trusted to behave in the ways specified in its functional specification and should protect against a wide range of potential abuses. | Soft | Focus groups or satisfaction surveys researching around the question “Do you trust the service?” |

**Table 8.1 SABSA risk management attributes**

The business attributes and especially the last column “Suggested measurement approach” gives significant and practical value for our compliance assessment method comparing with general standards in information technology and information security field.

## 8.5. Use case

In the next study, the exercise of assessing the compliance of requirements and criteria is presented. It is the first intention to use the criteria handbook in practice.

In this stage the real compliance control will be made by deciding how well the evidence presented by supervised entity complies with the requirements. Assessment starts with data collection and a survey will be conducted to describe the current situation of

supervised entities using summaries of interviews, questionnaires through the financial sector, external reviews etc.
The outcome of this exercise implies whether the control results are reasonable and practicable to continue with solution for making assessments.

Quantity

| **Subject/requirement** | **Requirement 1** | **Requirement 2** | **Requirement 3** | **…** |
|---|---|---|---|---|
| **Subject 1** | Material/No material | Material/No material | Material/No material | |
| **Subject 2** | Material/No material | Material/No material | Material/No material | |
| **Subject 3** | Material/No material | Material/No material | Material/No material | |
| **…** | | | | |

**Table 8.2 Basic table in use case for quantity measures**

Quality

| **Indicator/requirement** | **Requirement 1** | **Requirement 2** | **Requirement 3** | **…** |
|---|---|---|---|---|
| **Quality indicator 1** | Yes/No | Yes/No | Yes/No | |
| **Quality indicator 2** | Yes/No | Yes/No | Yes/No | |
| **Quality indicator 3** | Yes/No | Yes/No | Yes/No | |
| **…** | | | | |

**Table 8.3 Basic table in use case for quality measures**

Control

| **Requirement/control** | **Control 1** | **Control 2** | **Control 3** | **…** |
|---|---|---|---|---|
| **Requirement 1** | Increase/Decrease | Increase/Decrease | Increase/Decrease | |
| **Requirement 2** | Increase/Decrease | Increase/Decrease | Increase/Decrease | |
| **Requirement 3** | Increase/Decrease | Increase/Decrease | Increase/Decrease | |
| **…** | | | | |

**Table 8.4 Basic table in use case for control measures**

In the use case, scoring the quantitative, qualitative and control criteria, the percentage scale was used. Although in example Table 8.5 randomly generated numbers were used, conducted case with real numbers illustrate the study with the fact that in principle percentage scale is usable.

|  |  |  |  |  | IT governance* |  |  |  |
|---|---|---|---|---|---|---|---|---|
|  | Map |  |  | Org |  |  | Strat |  |
| Q | Q | C | Q | Q | C | Q | Q | C |
| 100 | 100 | 50 | 0 | 0 | 50 | 100 | 50 | 50 |
| 100 | 22 | 12 | 13 | 40 | 82 | 11 | 59 | 81 |
| 100 | 96 | 90 | 11 | 30 | 35 | 58 | 16 | 32 |
| 75 | 36 | 82 | 79 | 67 | 38 | 43 | 68 | 28 |
| 60 | 20 | 74 | 69 | 87 | 67 | 87 | 82 | 45 |
| 90 | 50 | 94 | 63 | 7 | 29 | 77 | 53 | 53 |
| 100 | 97 | 64 | 15 | 92 | 76 | 50 | 61 | 31 |

* Map – IT description, Org – IT organization, Strat – IT strategy, etc. “Q”, “Q” and “C” mean accordingly quality, quantity and control.

**Table 8.5 Illustrative table in use case with summarized figures**

Based on percentage scale and numerical information, it is quite easy to draw illustrative summary diagrams as seen for example in Figure 8.1.

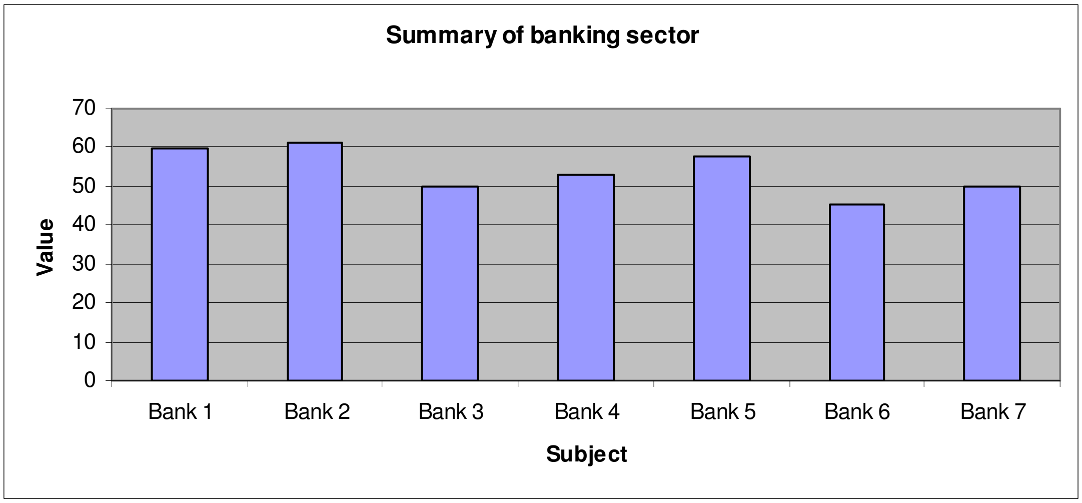

**Figure 8.1 Illustrative columns in use case with aggregated figures**

Diagrams are to use for decision makers and it is quite easy to convert to a different scale. For example, it may be stated that subjects with lower rate than 50 are important risk, between 50 and 60 are the average level of risk and subjects with higher rate than 60 are low risk for supervisors.

As a result of this chapter, the compliance scoring issues were analyzed and practical use case was conducted to score the compliance with requirements and criteria stated before. Studies continue to determine the best solution for assessment and it is made in connection with the development of scales for other risks.

# 9. Solution for compliance control

In this chapter we give an overview about the attempt to realize the results developed during previous chapters. First the need for IT solution to systematically deal with compliance assessment is explained and next, a pre-analysis of expected solution is proposed following the context description and functional and non-functional requirements analysis.

## 9.1. The need for IT solution

The practitioners, it means IT auditors in supervision authorities in financial field are studied IT supervision. For example, initiated by Bank of Greece, a query on information systems audits in supervised financial institutions was conducted. Connected with IT supervision/IT auditing methods, the most relevant conclusion is as following:

"There isn't any off-site procedure for collecting, on a regular basis, data related to information systems and their audit from supervised institutions. In most of the cases the supervisory authorities use as data resources the submitted by the institutions annual reports on the evaluation of internal control systems and the external auditors' reports. In some other cases ad-hoc off-site questionnaires, thematic reviews and reporting of incidents that lead to failures are used."

## 9.2. IT solution analysis

Once the idea for continuous compliance control is built, the questions for use and further development arise. A method as handbook is necessary but not enough. To put a method to work and considering that a lot of information will be collected, classified, analyzed and assessed, a kind of info-technological solution must be developed. The main reason for this is that a huge amount of information for assessing the current situation, as well as the amount of information, is growing rapidly. Another reason for this is a systematic approach, it means that one change causes other changes. The third reason is the market situation in the financial sector, which also changes continually.

In Financial Supervision Authority an analysis team was assembled and based on preliminary proposed structure of pre-analysis, RASS's (Risk Assessment System Solution) desired solution follows. Pre-analysis should describe the context of the system and the functional and non-functional requirements.

### 9.2.1. Context

Main functions:

- RASS data collection - a single solution must allow to gather all possible information of all subjects and all of the different risk indicators for risk assessment.
- Systematization of information - system must allow information connected subjects and risk indicators to be placed in such a way that it supports appropriate risk assessments
- Description of events - system must provide a single solution for all kinds of events, either associated with the subjects or the risks.
- Analysis and results - system must enable risk analysis and presentation of risk analysis results.
- Assessments - system must allow the user to develop a risk assessment based on available information and assist the user through the process.
- Estimates design - system must allow summarizing the risk assessments made for the subjects.

### 9.2.2. Functional requirements

The following factors are agreed with IT solution project team in Supervision Authority.

Users

The system must allow categorizing users at least four different levels considering how they use the functions: administrator – administrator or root-user; chief auditor - responsible for subjects; risk analyst - responsible for risk and user - normal user.

Inputs

Inputs entering in new subject or new information (for example a document) into system are predefined and will agree with the analysis of the system. Subjects' description should give an overview about the subject – its structure, business activities etc.

Requirements

Next assessment requirements and criteria should be developed in system:
Qualitative – yes/no, sufficient/not sufficient, reliable/not reliable, presented/not presented;
Quantitative – statutory indicators, analyst's ratios, internally set limits and ratios.

Risk

Assessment in system must comply with the prescribed classification of risks:

- Low risk
- Medium risk
- Considerable risk
- High risk

Shortcomings which cause the risks are in essence the observations require action of supervision and measures of supervision, and deficiencies in the system must be presented separately.
Formally, the system should display the parallel information fields, in which observation of the deficit, decided measure (both proposals as well as confirmation), the deadline agreed for implementation and the status (whether the measure is implemented or needs implementation).

Requests

The system must allow for all sorts of queries with respect to criteria drawn up. There should be both the predefined queries (described above) as well as opportunity to make queries and disclose via query preparation module. For example, the query on the general information of subject allows seeing the whole information connected to the subject in one window.

### 9.2.3. Non-functional requirements

The following aspects are agreed with IT solution project team in Supervision Authority.

Security

The system must identify and authenticate users, who must be resolved as a username and password combination, as well as ID card to use.
System controls are necessary to ensure data integrity and must be built into the system. System controls should be implemented for input, operations and output.
Database design should allow to continuously copy the changes (incremental backup) and periodic full backup copy (full backup). Backup system has to ensure that the maximum allowable data loss does not exceed one week (recovery point objective).
Sending data out of the system or putting the data into the system by means other than through the user interface, data must be encrypted. Encryption is necessary to ensure data confidentiality and integrity.
The created system has to enable the remote access to the system in accordance with previously agreed and certain number of specified computers.
Specific security requirements will be developed during the system analysis and design.

Performance

Capacity must allow serving at least 50 concurrent users while maintaining the system to normal operating speed, including the opening of the functions, data input and query responses displayed.
With increasing number of data it may be necessary to optimize the database in order to maintain performance characteristics.

Records

The system must allow logs of operations or audit trails. Log files can be managed by the administrator.
Log files should provide information about who, what and when changed, added or deleted a certain information in system.

Usability

The system must be developed to draw attention to usability. For example, the usability requirements such as the thousands of empty spaces rather than commas, currency conversion, etc. must be carried out automatically.
Usability requirements are divided as following:

- Clarity - simple and usable functions, structure;
- Perceptibility - the system complies with a given business process;
- Simplicity - less steps to reach the desired results;
- System support - guidance by the system;
- Data input - to add documents must be comfortable, also there has to be a possibility to add multiple files at once.

Flexibility

The system must allow easy and quick improvements to the system, including the administrator or super user to change some parameters or classifications, make them obligatory/not obligatory etc.
The system must allow easy and fast system development, such as the addition of new inquiries, new functions, new connections with other databases, new check-lists, include ORSA (Operational Risk Self-Assessment) and the like.

Infrastructure

The system must be built on a client-server solution. Relational database must be used by the system.
Possible file types used in data input:

- Office - doc, xls, ddoc, ppt, odf, docx
- txt
- pdf
- jpg, png
- XML
- HTML

Interfaces

System must allow connections at least with following systems:

- Web-page
- Analysis software

- Document management system
- E-mail system

Views

The system has the ability to display different views, such as:

- Home - all subjects and all predefined queries, standards (the laws with the main figures) as a link etc.;
- Subject chosen - index bookmarks (generic, etc.), standard numbers, in addition the given estimates, links to the main operations etc.

Development

The system developer must be willing to add the specialists in their field into development process. The main focus should be directed to develop a system suitable for users and smaller proportion of the whole system may be directed to analysis and documentation. A significant amount of prototyping development method should be used.

Testing

Testing tasks should be prepared and approved prior to the tests conducted. Both, the technical tests by developer and functions tests by the end user should be conducted. Testing scenarios must be composed.

Pilot use

One of the system development phases must be the pilot phase, allowing complete risk assessment.
Further evaluation of system will be carried out outside the system to verify compliance with the results - if there is a significant differences about the results, an analysis must be carried out. The analysis must explain why the differences occur and how the system must be improved.

System administration

Using administration interface, the functions like insert, change and delete of users; insert, change and close the subjects in system; manage classificatory, look through the logs of the system, initiate the backup copy of system data etc. must be available. Also there must be tools in the system for administrators and master users for making minor changes in functionality.

System documentation

After development, next documentation will be delivered:

- Analysis and design of the system;
- Source code;

- Administration manual;
- User manual;
- Development project documentation.

Documentation should allow external users (end-users, developers, administrators) to understand how the system is developed and how it works.

## 9.3. Outcomes

Some basics of IT solution outcomes are drawn up. In common, outcomes by risks and outcomes by subjects can be possible shown in the figures as following.

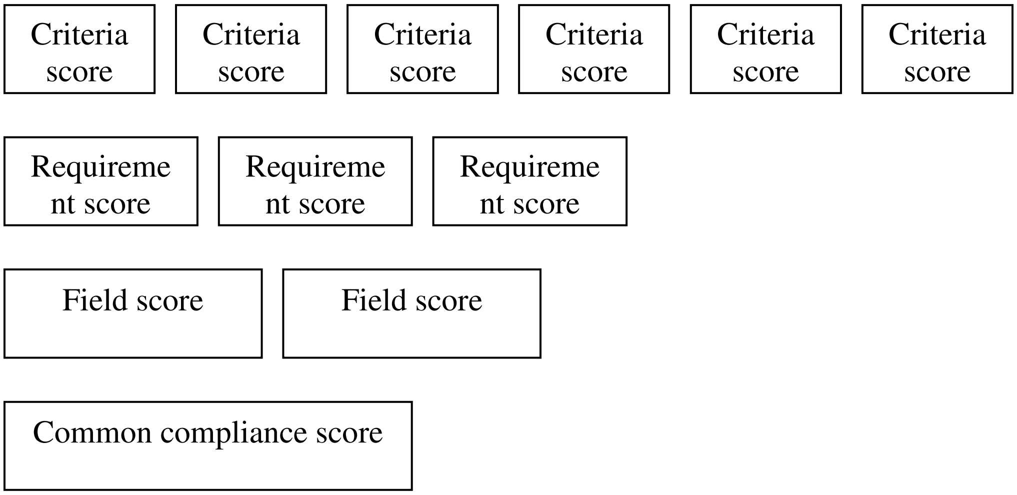

**Figure 9.1 Compliance risk aggregation**

Figure 9.1 presents the possibility in IT solution to aggregate risk scores from detailed level (specialist level) to the common level (decision makers level).

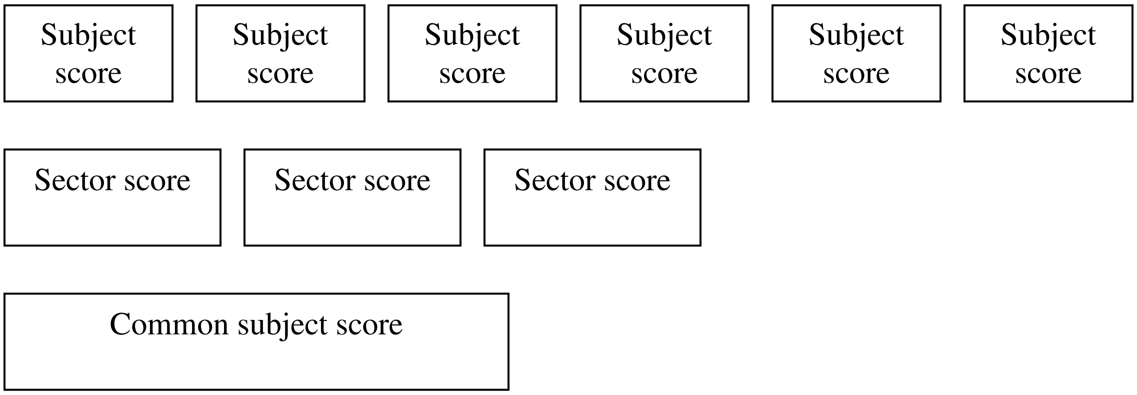

**Figure 9.2 Subject risk aggregation**

Figure 9.2 presents the possibility in IT solution to aggregate subject scores from single subject level to the sector (for example banking sector) level.

The figures point the possibility to get aggregated information from the system by subject or by the risk based on the level of aggregation. The outcomes should be used to create any kind of reports in connection with risks in financial sector.

As a result of this chapter, the basics for creation IT solution for compliance scoring is outlined. Using this specification, it is possible to start negotiations with possible service providers, i.e., system developers.

The requirements and criteria to meet with the requirements for information technology field and connected risks will be taken from criteria handbook, as stated in Chapter 7 and presented in Appendix 2.

The research proceeds with summation of previous results and putting together method for continuous information technology supervision.

# 10. IT supervision method

In this chapter we mainly describe the desired state of how IT supervision will be conducted in using the solution developed previously. First, the changing direction for IT supervision is under discussion, and next, as a desired state continuous IT supervision and audit planning is hypothetically proposed. As a conclusion, an evaluation of method with universal criteria is carried out.

## 10.1. IT supervision direction

Starting with the IT supervision method, the situation in IT supervision was as follows. We have preliminary guidelines for supervised entities and some internal explanation for the requirements to be used in on-site inspections. A systematic approach for IT supervision was not used and continuous assessment of IT was not performed.

The first main step was to finish with guidelines that regulate firms' information technology area covering all the main areas we supervise. One new guidelines paper for information security issues and existing guidelines papers – IT governance and business continuity - was modified. The guidelines give a signal to the supervised entities about the expectations for governing the IT field.

In developing the method, it is necessary to assign a meaning to these requirements. Otherwise, we can simply require from subjects that they must operate securely – if we do not clarify what it means, it will not work. To illustrate that, real life situations could serve as examples. Once, it appeared that one bank did not understand the regulative statement "the information exchanged through a public network should be protected". Following discussions establishing what a public network is, what information exchange is and what protection is, it became clear that a suitable solution is the encryption of information or encryption of a channel. From supervision point of view, such types of questions should be discussed and decided upon before the actual measures. To clarify the content of requirements, representative tables will be composed. Inside these tables each requirement will be described, the criteria will be determined, and compliance indicators will be highlighted. The tentative version of these tables is presented in Appendix 2.

When developing a method, equal treatment should be ensured. In practical supervision, supervisors already make a difference between bigger subjects and smaller subjects. For example, the supervisory statement is: "The larger the scope of business and risk level of the supervised entity and the entity's impact on the financial system as a whole, the greater the amount of attention the supervised entity needs to pay to a potential alternative location". Through the method it is planned to make such differentiation for each requirement and thereby approve the criteria. The main purpose of such differentiation is to ensure equal treatment of subjects, it means that in principle the requirements are the same for the whole sector, but to meet the requirements the criteria are different depending on the size of the subject. To illustrate the last issue, for example, the supervisor could require a separate position of chief information security officer (CISO) from bigger banks, but it is not reasonable to require CISO position from a smaller investment firm. In both cases the requirement is “There should be a responsible person for information security inside the company“.

## 10.2. Continuous IT supervision and auditing

In this section we point to the need for continuous information gathering for making assessments and based on these assessments, help to make supervision decisions.
IT supervision method attempts to collect all connected information into one base – changes in IT field (for example, business processes affected by information systems, IT infrastructure, IT organization, internal and external regulations, risk assessments), changes in data security field (for example, organizational, regulative, technological, physical), changes in business continuity planning (for example, BC plan update, BC testing information, organization), data security and business continuity incidents and all audit information (for example, FSA audits, internal audits, external audits).

In this section we describe how continuous compliance assessment will be achieved by following IT supervision method. Continuous compliance assessment assumes continuous information gathering. Continuous compliance assessment indicates that all important information and all significant changes will be recorded and considered for assessment to make a decision if updated information gives a basis to change a score in certain area.

In this section we describe how the assessment results give an objective signal for IT auditing assignments.
First, the assessment results present the most critical areas and subjects where IT audits are necessary. For example, in case the method gives low rates in business continuity by certain subject, this area needs to be under deeper investigation for further period.
Next, there is a need for very exact IT audit assignments to increase the effectiveness of IT auditing. For example, if a certain subject has low rate in disaster recovery planning in comparison with other subjects, assessment scores point out the real reasons why rate is low, for example, recovery planning organization is not determined.
Next, based the IT auditing assignment, the suitable IT auditing techniques can be selected like, for example, document analysis, interviews, surveys, system usage and real data analysis, penetration testing etc.

The use of IT supervision method assumes at least an annual re-assessment of financial sector IT compliance risk and IT security profiles. During this re-assessment the serious not-compliant areas are highlighted, which gives the input for planning auditing activities by critical institutions. For FSA, it connects with the annual general risk assessments.

Benefits as self-evaluation results of the method could be first monitoring the whole sector, they are banks, insurance, fund management companies and investment firms. Next, based on method we can use quantitative measures, because as a result of assessment, we get the numbers (compliance percentage) and we can use these numbers henceforth. Next, using the method we can cover the most important IT issues we need to supervise, it is IT governance, IT security governance and business continuity. Using the method we can prove equal treatment as we use weighting in such a way that equal treatment is assured. Finally, based on the results of the method, we can establish real IT auditing tasks using the assessment matrix and aggregated results.

## 10.3. Evaluation of method

The method is evaluated by using March and Smith's (1995) universal criteria and once the method is realized in an information technology solution, it meets the evaluation criteria:

- Operationality - the ability to perform the intended task is realized first by integration into everyday supervision work. Secondly, realization of the method supports almost every activity needed by supervisor, i.e., collecting input information, ordering and analyzing input information, making assessments, making risk assessment and executing any kind of queries. Method is partially implemented into everyday IT supervision work and it will be a part of overall risk assessment solution in Financial Supervision Authority.
- Efficiency – using the method, assessment of the IT situation is quick and productive, it means that results are usable for taking supervision activities. This criterion also refers to the adaptability of method, i.e., all the requirements for the IT field are considered and once the new criteria appear (for example, initiated by new legislation) they can be added to the method. The efficiency appears after some period real usage.
- Generality – this criterion refers to the universality of the method, having the possibility to deal with little investment firms as well as with bigger banks. Also, this criterion refers to the fact that using the method, IT supervision is done similarly to other risks (for example, credit risk, market risk and operational risk).
- Ease of use – this criterion needs to be one of the most important in starting the realization of the method in the information technology solution. Ease of use means that all the specialists starting to use the system give assistance in performing analysis and assessments of supervised entities. The most important criteria in developing respective IT solution are usability and flexibility.

Comparing with common methods for some certain task (for example COBIT methodology for IT governance or ISO 27001 for information security), it can be stated that developed IT supervision method is able to manage all the necessary tasks taking account also the specifics of financial sector. The main advantage of IT supervision method in comparison with other solutions comes from its scope, which includes the basic components as IT risks, information security, business continuity (stated in key concept) and combines the actual events in connection with IT for risk assessment.

The author finds that the criteria highlighted above are mainly met in the IT supervision method and its further realization and in comparison with known methods in literature, it can be stated that while other methods support the proposed method, they cannot entirely replace it.

The depth and coverage of our method refers to the best possibility to support the daily activities of IT supervision and its implementation in practice will complement the method as needed.

# 11. Discussion and conclusions

In the last chapter some discussion points and conclusions about research results are initiated, the use of results and limitations are outlined and some further research directions are proposed.

## 11.1. Results and limitations

In this section, some implications involving the science and the practices will be highlighted, also the limitations of research are discussed.

The main purpose of the current research was to examine by means of step-by-step sub-studies the core content of IT supervision and propose a method for continuous information technology supervision.
As a result of the research, a method for IT supervision in the financial sector is developed. Research was initiated by a practical need to use a systematic approach for IT field supervision. The trends show that kind of assessment solutions for IT supervision risks are already in use, but using systematic literature review it became clear that no universal method for IT supervision for financial sector exists.

From a scientific point of view, we performed some sub-studies and combined the methods for IT and information security assessment and analyzed their strengths and weaknesses and implementation opportunities for the financial sector in Estonia.
An overview about research and literature in connection with information technology and governance, information security and business continuity as the areas the IT supervisors was highlighted.

From a practical point of view, research results will be used in everyday supervision processes and the IT supervision method will be implemented into the common risk assessment system. The compliance scoring issues were analyzed and practical use case was conducted to score the compliance with requirements and criteria stated before.

The research process was divided into sub-studies.
The results of the sub-study, about how the IT field is regulated in European countries, were considered in setting up our requirements. The sub-study about how do supervised entities conform to the requirements helped to answer to the question about whether the economic aspects of being in compliance with the requirements are reasonable. The purpose of the next sub-study was to find out how the subjects fulfill the requirements for the information technology field today. It helped to provide an appreciation for how adequate the criteria are and what kind of changes for increasing or decreasing the number of requirements are needed. The criteria handbook created during sub-study is the most important outcome of the whole research. The handbook summarizes the results and ideas from previous sub-studies and gives a tool for exercising compliance

assessment. It provides the criteria for assessment through deep analysis and also the question of equal treatment is addressed.
The results are novel in the sense that through similar sub-studies IT supervision approach is never studied.

Research has also some limitations. First, research is done in Estonia where security requirements and standards may vary from other countries. Focusing especially for financial sector is not a limitation, because in principle the results may be useful for other sectors too, while making some changes in requirements or in criteria.
Second, the practical usage of IT supervision method needs to be done to ensure its reliability and it will be done further in realizing the method in IT solution and using it in everyday supervision in Estonia. The practical use also gives a basis for making improvements, for example in proposed handbook.

## 11.2. Further research

Further research focuses on the results of using the method inside of common risk assessment systems (RAS) – are the problems discussed above addressed prudentially, what are the scores and do these scores show the real situation of market and risks, etc.
Presence of a sufficient number of evaluations over time will provide an opportunity to assess the long progress of subjects IT- and information security risks. In addition, given the previous estimates and the current situation, how is situation changed? Ideally it can be examined if higher rating ensures fewer major incidents, i.e., less realized risks.

As Estonia and financial sector institutions have suffered from serious cyber-attacks in 2007. April, the common overview of how the IT risks are managed in financial institutions allows us to give a greater contribution to the problem solving. Suggested "continuous supervision of IT" may also help, directly or indirectly in future cases, to detect attacks early and to possibly reduce the impacts.

Research continues with an examination of how the market participants comply today with requirements. The results show that the proposed requirements are not overcharged. It is true, that expenses for IT and information security associated with business continuity are high and expenses should be argued for each specific case to ensure a reasonable level of security.
Research was done using questionnaires and interviews with relevant persons. Applicability of new requirements is under research.

Research continues with an exhaustive analysis of the proposed requirements and the main question is “what does a certain requirement mean?” As a result, the criteria handbook is composed. It may be noted that the handbook itself cannot be a static document, but has to be updated continually.
Substantive analysis was used for working out the first version of handbook and continuous update based on practical use follows.

Next, based on previous results, the assessment of compliance is discussed and execution of practical use case is started. Further steps to implement IT supervision method in practice are started and pre-analysis of IT solution has begun.
Practical analysis was done using groupware form and brainstorming.

Once the method is implemented, further examination begins to determine those entities with good compliance with IT requirements experiencing lower level losses in the case of IT incidents. Based on that examination the reasons will be explored, if it is not true, and next, the method will be improved.
The main purpose of research – examination the core content of IT supervision – is achieved and the main result – an IT supervision method – will be implemented into everyday supervision work.

# 12. References

Aberdeen Group. 2005. Best Practices in Security Governance. http://www.aberdeen.com/Aberdeen-Library/1951/RA_GOVERNANCE_JH.aspx. Accessed at 24.08.2010.

Alvesson. M., Sandberg, J. Generating Research Questions Through Problematization. Academy of Management Review. 2011. Vol. 36, No. 2, 247-271.

Behr, K., Castner, G., and Kim, G. 2010. The value, effectiveness, efficiency, and security of IT controls: An empirical analysis. http://www.itpi.org/docs/veesc.pdf. Accessed at 24.08.2010.

BIS – Bank of International Settlements. 2010. Operational risk metrics. http://www.bis.org. Accessed at 26.08.2010.

Brotby, W. K. 2009. Information security management metrics: a definite guide to effective security monitoring and measurement, CRC Press, ISBN 978-1-4200-5285-5.

Bruce, K. B, DeWayne, L. S., Jonathan, B. W. 2006. A Within Firm Analysis of Current and Expected Future Audit Lag Determinants. Journal of Information Systems. Vol. 20, No. 1, pp. 65–86.

BSI. 2005. IT-Grundschutz Catalogues. http://www.bsi.bund.de. Estonian version ISKE. www.ria.ee. Accessed 14. May 2010.

Cameron, T. R. 2007. Total Cost of Cyber (In)security – Integrating operational security metrics into business decision-making. (Presentation) Mini-Metricon, February 5, 2007, San Francisco, CA.

Carnegie Mellon Software Engineering Institute (CMU/SEI). 1999. OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation Framework. Technical report, CMU/SEI-99-TR-017, ESC-TR-99-017.

Committee of Sponsoring Organizations (COSO). 2010. http://www.coso.org. Accessed 10. August 2010.

Deloitte. 2007. Global security survey: The shifting security paradigm. www.deloitte.com. Accessed at 23.08.2010.

Dhillon, G., and Torkzadeh, G. 2006. Value-focused assessment of information system security in organizations, Information Systems Journal 16, 293–314.

Estonian Financial Supervision Authority. 2010. Objective of Financial Supervision. http://www.fi.ee. Accessed at 25.08.2010.

Estonian Ministry of the Interior. 2009. Emergency Act. Available at http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXXX26&keel=en&pg=1&ptyyp=RT&tyyp=X&query=h%E4daolukorra. Accessed 19. August 2010.

Ghose, A., Rajan, U. 2006. The Economic Impact of Regulatory Information Disclosure on Information Security Investments, Competition, and Social Welfare, Submitted to Workshop on Economics of Information Security 2006.

Gibb, F., and Buchanan, S. 2006. A framework for business continuity management. International Journal of Information Management. No. 26, 128-141.

Hauser, R. J., and Katz. M. G. 1998. Metrics: You Are What You Measure! Available at http://www.mit.edu/~hauser/Papers/Hauser-Katz%20Measure%2004-98.pdf. Accessed at 26.08.2010.

Henderson, J. C., and Venkatraman, N. 1993. Strategic Alignment: Leveraging information technology for transforming organizations, IBM Systems Journal, Vol 32, No.1, 472-484.

Hiles, A. 2004. Business continuity: best practices, World-Class Business Continuity Management, 2nd edition, ISBN 1-931332-22-3.

Hinson, G. 2006. Seven myths about information security metrics. Published in ISSA Journal. IsecT Ltd. www.isect.com. Accessed at 26.08.2010.

Hinson, G. 2008. The financial implications of implementing ISO/IEC 27001 & 27002: a generic cost-benefit model. Case study has been updated and republished at ISO27001security.com, along with a complementary paper: a generic cost-benefit analysis (business case) for ISO27k.

Hirsch, C., and Ezingeard, J. N. 2008. Perceptual and Cultural Aspects of Risk Management Alignment: a case study. *Journal of Information System Security*. 4(1), 3-20.

IIA Research Foundation. 2006. IT Audit Topics Research Symposium. http://www.theiia.org/research/. Accessed at 23.08.2010.

Information Security Forum, 2011. https://www.securityforum.org/. Accessed 26. March 2011.

Institute of Internal Auditors. 2010. GAIT - A risk-based approach to assessing the scope of IT General Controls. http://www.theiia.org/guidance/standards-and-guidance/ippf/practice-guides/gait/. Accessed 21. June 2010.

ISACA. 2009. An Introduction to the Business Model for Information Security. https://ww.isaca.org.

ISACA. 2010. COBIT - Control Objectives for Information and related Technology. https://www.isaca.org/. Accessed 29. March 2010.

ISO. ISO/IEC 24762. 2008. Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services. Available at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41532. Accessed 19. August 2010.

ISO27001 security forum. 2007. ISO/IEC 27001 & 27002 implementation guidance and metrics. Prepared by the international community of ISO27k implementers. Version 1.1. Available at ISO27001security.com.

IT Compliance Institute. 2006. IT audit checklist: information security. Practical guidance on how to prepare for successful audits. www.itcinstitute.com.

IT governance Institute. 2007. IT control objectives for Basel II: The Importance of Governance and Risk Management for Compliance. ISBN 978-1-893209-38-1.

IT governance Institute. 2006. IT control objectives for Sarbanes Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition. ISBN 1-933284-76-5.

Järvinen, P. 2004. On research methods, Opinpajan kirja, Tampere.

Johansson, E., and Johnson, P. 2005. Assessment of Enterprise Information Security - An Architecture Theory Diagram Definition. PROCEEDINGS CSER 2005, March 23-25, Hoboken, NJ, USA, ISBN 0-615-12843-2.

Kirt, T., Kivimaa, J. 2010. Optimizing IT security costs by evolutionary algorithms. Conference on Cyber Conflict, Proceedings 2010. CCD COE Publications, 2010, Tallinn, Estonia. 145-160.

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., Linkman, S. 2009. Systematic literature reviews in software engineering – A systematic literature review. *Information and Software Technology*. No. 51, 7–15.

Macaulay, T. 2009. Critical infrastructure: understanding its component parts, vulnerabilities, operating risks, and interdependencies, ISBN 978-1-4200-6835-1.

March, S. T., and Smith, G. F. 1995. Design and natural science research on information technology, Decision Support Systems, 15 (4), 251-266.

MITRE Corporation. 2010. Web-page. A collection of Information Security Community Standardization Activities and Initiatives. www.makingsecuritymeasurable.mitre.org.

Mukhopadhyay, T., Kekre, S., and Kalathur, S. 1995. Business value of information technology: A study of electronic data interchange. MIS Quarterly, 19(2): pp. 137-156.

NetIQ. 2008. Sustainable Compliance: How to reconnect compliance, security and business goals. http://www.netiq.com. Accessed at 25.08.2010.

Ramachandran, S., and White, G. B. 2005. Methodology to Assess the Impact of Investments in Security Tools and Products, Journal of Information System Security, 1(2), 3-25.

Reeves, C. A., and Bednar, D. A. 1994. Defining quality: Alternatives and implications, Academy of Management Review 19, No 3, 419-445.

Rosemann, M., and Vessey, I. 2008. Toward Improving the Relevance of Information Systems Research to Practice: The Role of Applicability Checks. MIS Quarterly Vol. 32 No. 1, 1-22.

SABSA Limited. 2010. SABSA - Sherwood Applied Business Security Architecture. http://www.sabsa.org/. Accessed 17. August 2010.

Siponen, M., Iivari, J. 2006. Six Design Theories for IS Security Policies and Guidelines, Journal of the Association for Information Systems Vol. 7 No. 7, pp. 445-472.

Software Engineering Institute. 1993. CMM – Capability Maturity Model. http://www.sei.cmu.edu/index.cfm. Accessed at 25.08.2010.

Sonnenreich, W., Albanese, J., and Stout, B. 2010. Return On Security Investment (ROSI): A Practical Quantitative Model. A summary of Research and Development conducted at SageSecure. www.sagesecure.com. Accessed at 24.08.2010.

Syed, A. 2004. Business continuity planning methodology. ISBN 0-9733725-0-8.

Vaughn. R. B. Jr, Henning, R., Siraj, A. 2002. Information Assurance Measures and Metrics - State of Practice and Proposed Taxonomy. Proceedings of the 36th Hawaii International Conference on System Sciences, 0-7695-1874-5/03.

Virkkunen, H. 1951. Initial costs for product types and lots in manufacturing as a cause for decreasing unit costs and their treatment in cost accounting, Summary, (Teollisuuden kertakustannukset - niiden degressio sekä käsittely kustannuslaskennassa,) Helsinki research institute for business economics No 13, (Liiketaloustieteellisen Tutkimuslaitoksen julkaisuja 13,) Helsinki.

Watson, R. T., and Webster, J. 2002. Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly.* Vol. 26 No. 2, 13-23.

Weidenmier, L. M., Ramamoorti, S.  2006.   Research Opportunities in Information Technology and Internal Auditing. Journal of Information Systems, Vol. 20, No. 1, pp. 205–219.

# APPENDIX 1

Appendix 1 is divided into 2 parts, i.e., risk before control and control assessment. Risk before controls contains three domains: IT governance, information security governance and business continuity.
IT governance concerns nine aspects: information architecture, IT organization, IT strategy, IT risk management, IT development, IT change management, outsourcing IT services, problem management and monitoring. Nine scales (one scale per each aspect) with four degrees are defined: low risk before control, minor risk before control, major risk before control and high risk before control.

**Risk before control - IT governance**

Low risk before control

Information architecture

Information assets are classified and information assets have owners. According to the information asset security class, the information asset owner determines a minimum set of information security measures to protect certain asset, including access permissions.

IT organization

IT organization is established, structure is confirmed and proper IT posts are created. Procedures for recruiting IT personnel ensure that proper and suitable persons with competence will be selected. In performing IT functions, segregation of duties is guaranteed.

IT strategy

There is an IT strategy in place, which is aligned with business strategy and is approved by management. IT strategy is a basis for IT development plans, including for setting up priorities of plans. IT strategy will be updated regularly and if needed, changes will be made to ensure IT strategy conformity with changing business priorities.

IT risk management

There is a procedure for assessment and management IT risks to determine IT security measures and decide the amount of residual risk. IT risk assessment is obligatory before each bigger change in IT environment and impact for IT security will be assessed.

IT development

Before system development, research about user requirements and analysis of realization occurs. During system development, the requirements for further system administration and requirements for system security will be established. With appropriate procedures it will be assured that system development, testing and production environments are separated.

IT change management

There is a relevant change management procedure established. Before changes are implemented, the impact of change will be analyzed, including impact to the security and testing of the change is obligatory. Through the change process, it is beforehand agreed the co-ordination levels and each change has to be logged.

Outsourcing IT services

The procedures for choosing external service providers are established, the criteria and requirements for contracting and observation of service level agreements are determined. It is ensured that external service provider does not get access to the information systems before it is ascertained that service provider conforms to the accepted information security requirements.

Problem management

Procedure for IT incident and IT problem management is established. IT incident and IT problem management procedure guarantees that employees, service providers and clients are aware of how IT incident resolving is organized and how to report about incidents.

Monitoring

The requirements are established of how monitoring should be organized to ensure IT functioning, it is confirmed what and how IT should be monitored and how monitoring results are used to plan improvements.

<u>Minor risk before control</u>

Information architecture

Information assets are classified and information assets have owners. According to the information asset security class, only the access permissions are determined.

IT organization

IT organization structure is confirmed and proper IT posts are created. Procedures for recruiting IT personnel ensure that proper and suitable persons with proper competence will be selected. In performing IT functions, segregation of duties is not guaranteed.

IT strategy

There is an IT strategy in place, which is in accordance with business strategy and is approved by management. IT strategy is a basis for IT development plans, including for setting up priorities of plans. IT strategy will not be updated regularly.

IT risk management

There is a procedure for assessment and management IT risks to determine IT security measures and decide the volume of residual risk. IT risk assessment is not obligatory before each bigger change in IT environment and impact for IT security will not be assessed.

IT development

Before system development, research about user requirements and analysis of realization occurs. During system development, the requirements for further system administration and requirements for system security will be established. It is not assured that system development, testing and production environments are separated.

IT change management

There is a relevant change management procedure established. Before changes are implemented, the impact of change will be analyzed, including impact to the security and testing of the change is obligatory. Through the change process, it is not agreed the co-ordination levels and each change does not have to be logged.

Outsourcing IT services

The procedures for choosing external service providers are established, the criteria and requirements for contracting of service level agreements are determined, but agreement observation is not an issue. It is ensured that external service provider does not get access to the information systems before it is ascertained that service provider conforms to the accepted information security requirements.

Problem management

Procedure for IT incident and IT problem management is established. IT incident and IT problem management procedure does not guarantee that employees, service providers and clients are aware of how IT incident resolving is organized and how to report about incidents.

Monitoring

The requirements are established of how monitoring should be organized to ensure IT functioning and it is confirmed what and how IT should be monitored, but monitoring results are not used to plan improvements.

Major risk before control

Information architecture

Information assets are not classified and information assets do not have owners. For information security, common security measures are implemented.

IT organization

Common IT organization structure is confirmed and IT posts are described. Procedures for recruiting IT personnel do not ensure that proper and suitable persons with competence will be selected. In performing IT functions, segregation of duties is not guaranteed.

IT strategy

There is an IT strategy in place, but it is not a basis for IT development plans. IT strategy will not be updated regularly.

IT risk management

There is a procedure for assessment IT risks, but IT security measures and the volume of residual risk will not be determined. IT risk assessment is not obligatory before each bigger change in IT environment and impact for IT security will not be assessed.

IT development

Before system development, research about user requirements and analysis of realization occur. During system development, the requirements for further system administration and requirements for system security will not be established. It is not assured that system development, testing and production environments are separated.

IT change management

There is a change management procedure established. Before changes are implemented, the impact of change will not be analyzed, including impact to the security and testing of the change is not obligatory. Through the change process, it is not agreed the co-ordination levels and each change does not have to be logged.

Outsourcing IT services

The procedures for choosing external service providers are established, the criteria and requirements for contracting of service level agreements are determined, but agreement observation is not an issue. It is not ensured that external service provider does not get access to the information systems before it is ascertained that service provider conforms to the accepted information security requirements.

Problem management

Procedure for IT incident management is established, but IT problem management is not an issue. IT incident management procedure does not guarantee that employees, service providers and clients are aware of how IT incident resolving is organized and how to report about incidents.

Monitoring

Common requirements are established of how monitoring should be organized to ensure IT functioning. It is not confirmed what and how IT should be monitored and monitoring results are not used to plan improvements.

High risk before control

Information architecture

Information assets are not classified and information assets do not have owners. For information security, there is no particular security measures neither planned nor implemented.

IT organization

IT organization structure is not confirmed and IT posts are not described. Procedures for recruiting IT personnel do not exist. In performing IT functions, segregation of duties is not an issue.

IT strategy

There is no IT strategy in place.

IT risk management

There is no procedure for assessment and management IT risks.

IT development

Before system development, research about user requirements and analysis of realization do not occur. During system development, the requirements for further system administration and requirements for system security will not be established. It is not assured that system development, testing and production environments are separated.

IT change management

There is no change management procedure established. Through the change process, it is not agreed the co-ordination levels and each change does not have to be logged.

Outsourcing IT services

The procedures for choosing external service providers do not exist. It is not ensured that external service provider does not get access to the information systems before it is ascertained that service provider conforms to the accepted information security requirements.

Problem management

Procedure for IT incident and IT problem management do not exist.

Monitoring

The requirements are not established of how monitoring should be organised to ensure IT functioning.

**Risk before control - information security governance**

Information security governance concerns five aspects: information security policy, information security organization, logical security, physical security and information technology security. Five scales (one scale per each aspect) with four degrees are defined: low risk before control, minor risk before control, major risk before control and high risk before control.

<u>Low risk before control</u>

Information security policy

There exists current and by management established information security policy, which defines the main principles about information security assurance, including information security measures and procedures and employees' roles and responsibilities.

Information security organization

One of the members of board is responsible for information security, information security organization with roles and responsibilities is established.

Logical security

There exist procedures for information systems access management and presumption for granting access rights in information systems is security training for users. Access management procedures deal with access granting only to the users, who need access rights for everyday work (need to know). Access management procedures contain processes for granting, changing and closing access rights to the users.

Physical security

Critical or sensitive information assets will be kept in security areas with limited access and for securing these areas, physical security measures are implemented to protect assets against any kind of damage.

Information technology security

Necessary and sufficient set of information security measures are implemented. For delivering sensitive information through public networks, it is necessary to take measures to ensure information availability, integrity and confidentiality and there has to be procedures in place to make backups about critical information.

<u>Minor risk before control</u>

Information security policy

There exists current and by management established information security policy, which defines the main principles about information security assurance, but information security measures and procedures and employees' roles and responsibilities are not defined.

Information security organization

Information security organization with roles and responsibilities is established.

Logical security

There exist procedures for information systems access management, but presumptions for granting access rights in information systems are not determined. Need to know principle is not followed in access management procedures. Access management procedures contain processes for granting, changing and closing access rights to the users.

Physical security

Critical or sensitive information assets will be kept in security areas with limited access and for securing these areas, some physical security measures are implemented, but not to protect assets against any kind of damage.

Information technology security

Information security measures are implemented, but analysis about sufficiency did not proceed. For delivering sensitive information through public networks, it is necessary to take measures to ensure information availability, integrity and confidentiality and there has to be procedures in place to make backups about critical information.

Major risk before control

Information security policy

There exists current information security policy, but it is not established by management. Information security policy defines the main principles about information security assurance in general terms, information security measures and procedures and employees' roles and responsibilities are not defined.

Information security organization

Information security organization is established without roles and responsibilities.

Logical security

There exist procedures for information systems access management, but presumptions for granting access rights in information systems are not determined. Need to know principle is not followed in access management procedures.  Access management procedures contain processes for granting access rights to the users, but do not contain processes for changing and closing accesses.

Physical security

Critical or sensitive information assets will be kept in security areas with open access and for securing these areas, some physical security measures are implemented, but not to protect assets against any kind of damage.

Information technology security

Information security measures are implemented, but analysis about sufficiency did not proceed. For delivering sensitive information through public networks, there are no extra measures to ensure information availability, integrity and confidentiality and there are no procedures in place to make backups about critical information.

High risk before control

Information security policy

There is no current information security policy.

Information security organization

Information security organization is not established.

Logical security

There are no procedures for information systems access management.

Physical security

Critical or sensitive information assets are not kept in security areas.

Information technology security

Information security measures are implemented according to the fact that security incidents are occurred.

**Risk before control - business continuity**

Business continuity concerns three aspects: business continuity process, the content of business continuity planning and business continuity testing. Three scales (one scale per each aspect) with four degrees are defined: low risk before control, minor risk before control, major risk before control and high risk before control.

<u>Low risk before control</u>

Business continuity process

Ensuring business continuity is an inherent part of enterprises risk management and management is ultimately responsible for ensuring business continuity. Management formulates relevant framework for business continuity with adequate policies and procedures, ensures business continuity planning, plan examinations, upgrades and testing. Also the management is responsible for allocating necessary resources for business continuity activities and ensures, that employees are aware of business continuity arrangements and their roles in process.

The content of business continuity planning

Business continuity plans include information about emergency procedures, communication, alternative resources and locations, logistics, critical business functions and recovery scenarios.

Business continuity testing

Regular testing of business continuity plans are established and based on the results, necessary changes will be made in plans. Internal procedures exist to plan business continuity testing activities and communicate supervision authorities about the results.

<u>Minor risk before control</u>

Business continuity process

Ensuring business continuity is not an inherent part of enterprises risk management and nominated person is responsible for ensuring business continuity. Responsible person formulates relevant framework for business continuity with adequate policies and procedures, ensures business continuity planning, plan examinations, upgrades and testing. Also that person is responsible for allocating necessary resources for business continuity activities and ensures that employees are aware of business continuity arrangements and their roles in process.

The content of business continuity planning

Business continuity plans include information about emergency procedures, communication, alternative resources and locations, but do not include information about critical business functions and recovery scenarios.

Business continuity testing

Regular testing of business continuity plans are established, but based on the results necessary changes will not be made in plans. Internal procedures exist to plan business continuity testing activities and communicate supervision authorities about the results.

Major risk before control

Business continuity process

Ensuring business continuity is not an inherent part of enterprises risk management and responsibility is not appointed. Relevant framework for business continuity exists, but adequate policies and procedures do not ensure business continuity planning, plans examinations, upgrades and testing. Also allocating necessary resources for business continuity activities and employees' awareness of business continuity arrangements and their roles in process are not ensured.

The content of business continuity planning

Business continuity plans are general and include information about emergency procedures and alternative resources, but do not include information about communication, logistics, critical business functions and recovery scenarios.

Business continuity testing

Business continuity plans are established but will not be tested regularly and based on the results, the necessary changes are not implemented. There are no procedures to plan business continuity testing activities and communicate about the results.

High risk before control

Business continuity process

Ensuring business continuity is not an inherent part of enterprises risk management and responsibility is not appointed. Relevant framework for business continuity with adequate policies and procedures does not exist.

The content of business continuity planning

There are no business continuity plans.

Business continuity testing

Business continuity testing is not established.

## Controls assessment – risk identification

Control assessment contains four domains: risk identification, risk policy, administrative organization and internal control and risk observation. Four scales (one scale for each domain) with four degrees are defined: strong control, adequate control, weak control and inadequate control.

Strong control

Ongoing IT risk assessment in cooperation with IT and business side.
Before bigger IT developments, risk assessment is obligatory.
There exists systematic approach to identify risks and decide the measures and the results are documented.
As a result, risk appreciations are ordered by priorities.

Adequate control

Ongoing IT risk assessment by IT side.
Before critical IT developments, risk assessment is obligatory.
There exists systematic approach to identify risks and decide the measures, but the results are not documented.
As a result, only the risks with higher priority are ascertained.

Weak control

Ongoing IT risk assessment by IT side on occasion.
Before some critical IT developments, risk assessment occurs on occasion.
Risk identification and measures selection occurs on occasion, the results are not documented.
As a result, risks are commonly divided into „High“ and „Low“.

Inadequate control

No risk assessments.
Before none IT development risk assessment occurs.
There exists no approach for risk identification and measures selection.
There are no risk appreciations.

**Controls assessment – risk policy**

Strong control

IT strategy will be aligned with business strategy.
Management establishes IT strategy, IT security policy and business continuity plan as documents with proved high quality.
IT strategy, IT security policy and business continuity plan are made in accordance with recognized principles and standards.
IT strategy, IT security policy and business continuity plan are realized through standards, procedures and guidelines and realization is supervised.
IT risk assessments are basis for creating and updating IT strategy, IT security policy and business continuity plan.

Adequate control

IT strategy is in accordance with business strategy by several points.
Management establishes IT strategy, IT security policy and business continuity plan.
IT strategy, IT security policy and business continuity plan are partially made in accordance with recognized principles and standards.
IT strategy, IT security policy and business continuity plan are realized through standards, procedures and guidelines.
IT risk assessments are basis for creating IT strategy, IT security policy and business continuity plan.

Weak control

IT strategy is composed independently by IT department.
IT strategy, IT security policy and business continuity plan are not established by management.
IT strategy, IT security policy and business continuity plan do not consider with recognized principles and standards.
There are lower level documents to realize IT strategy, IT security policy and business continuity plan.
IT risk assessments are not a basis for creating and updating IT strategy, IT security policy and business continuity plan.

Inadequate control

There is no IT strategic planning.
There are no IT strategy, IT security policy and business continuity plan.
There are no IT strategy, IT security policy and business continuity plan.
There are no IT strategy, IT security policy and business continuity plan.
There are no IT strategy, IT security policy and business continuity plan.

**Control assessment - administrative organization and internal control**

Strong control

Management is ensured with the best practices of IT and information security government.
Inside of IT organization, duties and responsibilities of information security are clearly defined
All the information assets have owners.
Physical, technological and logical information security measures are implemented according to business needs.
Control procedures are implemented to ensure that all the information security measures function.

Adequate control

Management uses IT and information security government best practices.
Inside of IT organization, duties and responsibilities of information security are partially defined
Only the most important information assets have owners.
Physical, technological and logical information security measures are implemented.
Control procedures are implemented to ensure that several information security measures function.

Weak control

Management uses IT and information security government best practices in several domains.
Inside of IT organization, duties and responsibilities of information security are inadequately defined.
Few information assets have owners.
Physical, technological and logical information security measures are partially implemented.
Control procedures are implemented to ensure that few information security measures function.

Inadequate control

IT and information security government best practices are not used.
Inside of IT organization, duties and responsibilities of information security are not defined.
Information assets do not have owners.
Physical, technological and logical information security measures are not implemented.
Control procedures are not implemented to ensure that information security measures function.

**Control assessment – risk observation**

Strong control

IT risks are followed by reporting to the management and reports include information about IT risks and proper measures.
For monitoring IT risks, proper prevention, detection and intervention systems are implemented, including backup systems.
In IT area, continual process is implemented to control the compliance with internal and external IT- and information security requirements.

Adequate control

IT risks are followed by reporting to the management and reports include information about IT risks.
For monitoring IT risks, proper prevention and detection systems are implemented.
In IT area, control of compliance with internal and external IT- and information security requirements is in place.

Weak control

IT risks are followed, but reporting to the management is not an issue.
For monitoring IT risks, extra systems are not implemented.
In IT area, sometimes control activities occur to ensure compliance with internal and external IT- and information security requirements.

Inadequate control

IT risks are not followed.
There is no monitoring of IT risks.
No control for compliance with internal and external IT- and information security requirements occurs.

# APPENDIX 2

Appendix 2 is divided into four parts: planning and organization, acquisition and implementation, information security and business continuity. The planning and organization part consists of four sub-parts: IT strategy, information architecture, IT organization and IT risk management. Each sub-part contains definition, description, content and criteria and format for assessment.

Planning and organization

**IT strategy** – each firm wants to be active in financial sector have to direct a way of business and plan high level initiatives for supporting IT and information systems solutions.

**Description**

The basis of information technology activities of a company must be the strategy derived from business objectives and strategy of the company approved by the management of the company (IT strategy). In developing IT strategy it must be assessed which information technology support is necessary for achieving the business objectives of the company and whether the existing IT solutions enable to achieve the desired business result. Development plans must be compiled and the priorities and investments of IT projects must be determined on the basis of the IT strategy.

The IT strategy must be regularly updated and supplemented regularly according to the changes in the business strategy of a company or the development trends of information technology. The IT strategic planning process must include the directors of both business as well as IT authorities of a company.

For the optimal management of information technology expenses that would correspond to business objectives, the management of IT investments must be carried out through a periodical budgeting process.

Management must analyze the IT situation of the company at least once a year. It is recommended to regularly review the prudent use of IT resources for the support of business strategies and to approve the budget for the following period.
The management of a company must ensure the regular assessment of the compliance of IT organization of a company with external requirements (laws, regulations, etc.) and consideration of their effects. Measures must be taken for bringing IT organization into compliance with external requirements, if necessary.

**Content and criteria**

There has to be an IT strategy document in place. This document has to be approved by company's management board and have to be current. In proof of validity, strategy document has to have approved date and relevant signatures. IT strategy can be proved also by relevant decision of board meeting.

To assess the criteria, next documentation should be reviewed:

- Business strategy;
- IT strategy;
- Protocols and other documents in connection with strategy process (in paper and electronically);
- Employees and functions involved in IT strategy planning;
- Current year work schedule;
- Current year budget and current state.

Activities:

1. Verify that IT strategy:
   - Exists in enterprise;
   - Is in accordance with business strategy and technological development;
   - Is approved by management;
   - Is basis for enterprise's IT actions;

Business objectives come from business strategy and there should be a clear link between business and IT strategy to convenience connectivity. IT strategy has to be led by business strategy. Assessing that a criterion, the business strategy assessment is not a subject. For example, more concrete assessment point could be an evaluation whether the information technology possibilities are considered to contribute business strategy and are the relevant issues added to IT strategy. In practice, the financial institutions use many IT solutions and it could be assumed, that there exist much relevant connections between business and IT side, and therefore also between business and IT strategy.

IT strategy process - assess the process of IT strategy planning and find out that both business and IT managers and responsible employees are involved into this process.

It is important that persons in relevant posts participate in IT strategic planning. Not only an opinion of IT manager, but also business impact analysis and assessment of ROI – return on investments - can be suggested as a basis for IT strategic initiatives. For composing IT strategy, a gap-analysis approach can be suggested: first it should be find out the current state of IT, next the desired future will be described and third, the steps will be worked out how to achieve the desired state (programs, projects etc.).

IT development plans – not only the goals need to be mentioned but also the way how the goals will be achieved. IT strategy should give exact clarification how the goals will be achieved, also the lower level goals should be stated through certain development plans, programs or projects.

Ensure that tasks in schedule have concrete objectives and measurable results.

IT strategy update – it is not enough if there is a statement for IT strategy update as needed. A more concrete statement should be pointed, like "IT strategy will be updated regularly once a year".
At least annual review of IT strategy document is necessary. Also, IT strategy should be updated in case of bigger change in business or in business strategy.
Regular review of IT resources – IT management should have a common picture about utilization of resources and have be ready to present it to business side if necessary
Upgrades and complete activities occur as needed.
Compliance with external requirements.

IT expenses – IT expenses can be originated from business needs.
IT investments – the need for IT investments comes from business needs.
Ascertain that in connection with new projects, besides of development costs also the maintenance costs are considered. Use for that TCO – total cost of ownership.
IT budget – IT budget should be an agreement between business and IT side.
To express contribution to strategic initiatives and conditions for applying a strategy, inside of IT strategy document a statement about investments should be highlighted. In case for planning investment a cost-benefit assessment is used, IT strategy should have clear answer to the question: what benefits are got in making certain investments.

Examine the working schedules, projects and budget to confirm that they are in accordance with IT strategy.

IT investments management

Documentation:

- IT work schedule;
- IT budget and its observation;

Activities:

1. Ensure that IT expenses inside of budget are in accordance with IT working schedule and relevant need for financial resources;
2. Ensure that by new IT development not only developing costs but also later maintenance costs are considered;
3. Identify how budget fulfillment is followed up.

Accordance with external requirements

Documentation:

- The legal requirements;
- Requirements from contracts with third parties;
- License conditions;
- Information security policy, rules for access management, contracts etc.

Activities:

- Find out external requirements in connection with information technology;
- Assess internal IT governance conformity with external requirements.

**For assessment**

Quantity

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| IT strategy document | X | X | X | | | |
| Development plans | X | X | X | | | |
| IT strategy statements | | | | X | X | X |
| IT budget | X | X | X | X | X | X |

Quality

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Link with business objectives | | | | | | |
| Approved by management | | | | | | |
| Current strategy | | | | | | |
| Development goals | | | | | | |
| IT investments | | | | | | |
| TCO | | | | | | |

Control

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Annual IT strategy update | X | | | | | |
| Principles | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| for making changes | | | | | | |
| Development projects success | | | | | | |
| Budget control | | | | | | |

**Information architecture**

**Description**

A company must have general rules for determining the owners of information assets and classifying information assets into security classes and owners must be appointed to all information assets. Depending on the security class of data, relevant access restrictions must be imposed on the data.

Security levels must be established, introduced and implemented for each security class of information assets of a company. Security levels must provide minimum requirements for security and control measures that are to be regularly inspected and supplemented, if necessary.

The management must lay down the procedures for determining the security classes of information assets. The owner of a relevant information asset shall be liable for the classification of information assets and imposition of access restrictions.

**Content and criteria**

Information assets classification – information asset classification assumes that information assets are identified beforehand. For information assets classification, any kind of scale can be used, but in common, it should be possible to distinguish critical information assets, important information assets and those not important.

Data owners – for each information asset or information asset class, the owner should be assigned.

Information security level – information security level should be determined by information asset owner.

Minimum security requirements – information security requirements and measures should be determined by information security manager in accordance with information security policy and approved by information asset owner.

Information architecture

Documentation:

- The rules for classifying information assets;
- Procedures which are connected with administration of information assets;
- Information assets inventory with owners and security levels assigned to information assets;

Activities:

1. Verify that exists list of information assets and there is recorded for each object:
   - Name;
   - Owner;
   - Current location;
   - Information security requirements.
2. Verify the measures and procedures which are implemented for keeping the list of information assets up to date;
3. Using interviewing verify, does the information assets owners understand their role and are the information security requirements clearly defined and documented;
4. Ensure that information assets owners information security roles and duties are documented according to information security policy;
5. Using interviews and other techniques verify, based on selection of information assets, are the information security requirements performed as information assets owners are determined;
6. Examine what kind of controls and reports to information assets owners exist in connection with information assets (access, change, etc.)?

**For assessment**

Quantity

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Asset classification | | | | | | |
| | | | | | | |
| | | | | | | |

Quality

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Data owners | | | | | | |
| System owners | | | | | | |
| Security level | | | | | | |
| Security requirements | | | | | | |

Control

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

**IT organization**

**Description**

For providing information technology support necessary for business processes, a company must have an IT organization suitable in terms of size and competence. If the information technology know-how is outsourced, it is necessary to determine the areas where and by whom such outsourcing can be used and by whom and how the services ordered from outside are administered.

A company must establish relevant procedures for recruiting IT personnel that enable to assess the suitability of a person for a position. In addition to professional competence, the field of operation of the company and the need to work with sensitive information must be taken into account.

The IT organization of a company must have a clearly defined structure and tasks. It is necessary to ensure the existence of necessary resources for the performance of these obligations. Employees must possess clearly defined and required skills, rights, liability and obligations and these must be reviewed regularly.

A company must implement the separation of the functions of information technology development, maintenance, use and control. If the introduction of the separation of duties of employment proves to be impossible, additional controls must be implemented for risk management.

**Content and criteria**

IT organization structure, tasks – IT organization structure and division of labor should ensure that all IT related processes are covered with competent human resources. Human resources should be doubled in connection with critical processes to enable to continue with processes in the absence of one person.

Recruiting procedures – suitable person in this context also means the background checks.

Outsourced know-how.

Separation of duties, additional controls.

IT organization

Documentation:

- Organization structure chart;
- IT organization structure chart;
- Recruitment procedures;
- Documentation connected with outsourcing;
- Job instructions for IT personnel.

Activities:

1. Examine IT organization structure and position in accordance with enterprise structure;
2. Estimate, how many of positions in IT structure are occupied and what is the number of personnel interchange?
3. Take an overview IT personnel recruitment procedures and practice. Ensure, that outsourced attainment is under control;
4. Control that all the IT employees have current job instructions;
5. Check that employees' duties, rights and responsibilities written in job instructions conform to practice;
6. Ensure that updating of job descriptions occurs if needed;
7. Using interviews, verify that it is ensured continual segregation of duties;
8. In case segregation of duties is not ensured, ascertain the reasons. Assess the adequacy of additional controls which compensate the risk as a result of lack of segregation of duties.

**For assessment**

Quantity

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| IT organization structure | | | | | | |
| | | | | | | |
| | | | | | | |

Quality

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Tasks | | | | | | |
| Recruitment | | | | | | |
| Outsourcing partners | | | | | | |
| Segregation of duties | | | | | | |

Control

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Personal checks | | | | | | |
| Additional controls for segregation of duties | | | | | | |
| | | | | | | |

**IT risk management**

**Description**

The management of a company must ensure the functioning of the risk management process connected to information technology that would determine risk management methodology, reporting requirements and control mechanisms. It is necessary to ensure regular risk assessment updates and the continuity of the risk management process.

Expenses of IT security and IT services should be justified with risk assessments and cost-effectiveness assessments. In the course of risk analysis it is necessary to determine any possible threats, weaknesses, to assess the likelihood of realization of threats and damages resulting from them, to choose suitable measures for reducing the effect of realization of threats, to assess their cost-effectiveness and determine the size of acceptable residual risk.

Risk assessment must accompany any major changes in information systems or processes. In planning any changes to an information technology system it must be determined whether and how the change influences the security of the system and the process and in every way to reduce the effect of risks that accompany the change.

**Content and criteria**

Information security risk:

- Information security is not only a technical issue, but a business and governance challenge that involves adequate risk management, reporting and accountability.
- A key goal of information security is to reduce adverse impacts on companies to an acceptable level of risk. Information security protects information assets against the risk of loss, operational discontinuity, abuse, unauthorized disclosure, inaccessibility and damage. It also protects against the ever-increasing potential for civil or legal liability that companies could face as a result of information inaccuracy and loss, or the absence of due care in its protection.
- Information security covers all information processes, physical and electronic, regardless whether they involve people and technology or relationships with partners, customers and third parties. Information security addresses information protection, confidentiality, availability and integrity throughout the life cycle of the information

Risk management process.

Regular risk assessment.

Threats and weaknesses.

Residual risk – management should make decision about residual risks – neither information asset owner nor information security manager can make such of decision, they can only present their suggestions.

Major changes – before bigger changes which affect on information technology, an IT risk analysis should be performed and during the change, the results of risk analysis should be considered. Risk analysis should not be only limited with information system under change, but should also cover all connected systems which could be affected.

Risk management

Documentation:

- the policies and procedures which regulate risk assessment;
- risk analysis;
- risk reports to the management;
- report about incidents and problems;
- the documentation about last bigger change in information systems/information technology infrastructure to ensure that risks were analyzed appropriately.

Activities:

1. Check the risk analysis and ensure that:
   - information assets are identified and classified;
   - threats to the assets are identified reasonably;
   - technical and organizational vulnerabilities are analyzed.
2. Ensure that risk analysis gives an adequate base to information security strategy, security controls and security testing.
3. Ensure that risk assessment process is:
   - systematic and governed;
   - unified;
   - reported;
   - documented;
   - updated regularly.
4. Ensure that risk analysis is updated before bigger changes of information systems or information technology, before implementing new products or new services and in other cases which could affect on risk assessments;
5. Ensure that risk analysis is reviewed at least annually;
6. Ensure that management confirms and follows risk management process.

**For assessment**

Quantity

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Risk management process | | | | | | |
| | | | | | | |
| | | | | | | |

Quality

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Information security risk | | | | | | |
| Threats | | | | | | |
| Weaknesses | | | | | | |
| Residual risk | | | | | | |

<u>Control</u>

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Regular risk assessment | | | | | | |
| Risk assessment in case of major changes | | | | | | |
| | | | | | | |

## Acquisition and implementation

The acquisition and implementation part consists of six sub-parts: IT development, IT change management, outsourcing IT services, volume and performance management, problem management and operations management. Each sub-part contains definition, description, content and criteria and format for assessment.

### IT development

### Description

In order to create suitable solutions for meeting business requirements it is necessary to determine user requirements and assess alternative solutions beforehand. The decision of the management regarding the initiation of the development project and the choice of an alternative solution must be based on the cost-benefit analysis that indicates the technical, operational and economic justification of the project.

The separation of development, testing and production environment must be guaranteed in developing application software.

In developing a solution it is necessary to specify the functional and operational requirements of the solution, including maintenance, performance, reliability, monitoring, security and compatibility with existing systems. Testing standards and acceptance criteria of the system must be defined clearly. System requirements, standards, acceptance criteria and intellectual property rights must also be fixed upon ordering development from external service providers.

Each important development project in the field of information technology must have a specified and measurable objectives and a specific commencement date and end date. The development of an information system must be derived from the needs of the company and the decision regarding the initiation of projects must be made by the management on the basis of the approved IT strategy.

A project organization must be established for the implementation of each project. The course, budget and time-scheme of the project must be constantly monitored.

### Content and criteria

User requirements;

Cost-benefit analysis;

Separation of environments;

Solution testing;

Acceptance criteria;

System development.

Documentation:

- Documentation connected with development and/or procurement: standards, methods, policies, procedures etc.;
- Documentation of the last bigger system development (effect analysis, launching decision, protocols, risk analysis etc.).

Activities:

1. Ensure that development process conforms to established system development requirements and methods;
2. Ensure that decision about development is based on effect analysis;
3. Ensure that responsibilities are clearly defined and allocated through the development process;
4. Ensure that security, auditing and quality personnel is established;
5. Ensure that through development process a segregation of duties is guaranteed or compensate controls implemented;
6. Appreciate risk assessment procedures;
7. Ensure that requirements for system under development are clearly defined;
8. Give an opinion to the testing and implementation procedures;
9. Assess processes according to system development documentation and user manuals creation;
10. Ensure that approve criteria conform to the presented requirements, and that the product conforms to expectations;
11. Find out how the users will be trained to work with developed systems.

**Project management**

Project objectives.

Project organization.

Project monitoring mechanism – one example about such mechanisms is project steering committee.

System planning and acceptance - Percentage of emergency, high, medium and low risk changes. Numbers and trends of rolled-back/reversed-out changes, rejected changes vs. successful changes. Percentage of systems that (a) are supposed to comply with defined baseline security or similar technical security standards; and (b) have been proven by benchmarking/testing to comply fully with those standards.

Project management

Documentation:

- Documentation in connection with the last bigger development project: Effect analysis, launching decision, development assignment, specifications, meeting protocols, delivery papers etc.

Activities:

1. Overview project management methods;
2. Overview the progression of projects in comparison with project plans (financial, time and human resources);
3. Find out if business and IT side consent to projects' results and process;
4. Ensure that purpose of the project is formulated and it comes from business objectives;
5. Overview the experiences of project managers;
6. Ensure that project teams are approved by management and members of teams have relevant rights and responsibilities;
7. Ensure that business side contributes to necessary phases of IT/IS projects;
8. Assess how is organized testing, employment of new solutions and user training, in addition how is organized change-over from development to administration;
9. Ensure the adequacy of project plans in assessing that it is determined:
    - The results of phases;
    - The criteria based on that the results will be accepted;
    - Information security and control requirements;
    - Testing requirements;
    - Documentation requirements;
    - The adequacy of realization examination;
    - Through the different phases (design, development, testing and employment) adequate following of standards and procedures;
    - The adequacy of change controls;
    - Involvement of proper employees through project lifecycle;
    - Effective communication and reporting procedures;
    - Accuracy and adequacy of project management instruments.

Procedure management

Documentation:

- Effective policies and procedures which deal with composing user manuals, system administration guidelines, employee's instruction etc.
- User manuals;
- Instruction materials;
- System administration procedures (guidelines).

Activities:

1. Ensure that there exist user manuals for applications, they satisfy user needs and they are practicable;
2. Verify that user manuals are up to date and represent the current state of applications;
3. Find out what kind of training the users get to work with applications;
4. Ensure that system administration procedures are documented, documentation is up to date and renewable.

**For assessment**

Quantity

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Development procedure | | | | | | |
| | | | | | | |
| | | | | | | |

Quality

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| User requirements | | | | | | |
| Cost-benefit analysis | | | | | | |
| Separation of environments | | | | | | |
| Solution testing | | | | | | |
| Acceptance criteria | | | | | | |
| Project management | | | | | | |
| Project objectives | | | | | | |
| Project organization | | | | | | |

Control

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| Project monitoring mechanism | | | | | | |
| | | | | | | |
| | | | | | | |

**IT change management**

**Description**

The correctness and controllability of the execution of changes shall be guaranteed for the reduction of any disruptions and errors that may arise from the changes in the information system. An action plan must be compiled for the execution of changes. An audit trail must be recorded from the execution of changes that would enable to identify the time of the execution of the change, the executer and content of the change.

Upon executing and planning the changes in an information technology system it must be determined if and how the changes affect on the security of the system. A prior analysis for determining new security requirements is necessary in case of major changes regarding the acquisition of new hardware, software or service. Any planned change in the hardware and software of the system must be tested beforehand. The execution of emergent and planned changes must be approved.

**Content and criteria**

The process of change management

1. Who can apply to changes and what channels are used to apply?
2. What could be the reasons that IT side may deny to make change if requested by business side?
3. How often the changes in change management procedures will be made and what are the reasons?

Urgent changes

4. Considering any kind of circumstances, what changes will be classified as urgent changes?
5. Are these principles written down?
6. Who does decide about change urgency for each concrete case?
7. Following what kind of procedure the urgent changes will be implemented?

Change testing beforehand

8. How it will be ensured that all the change can influence is considered by testing?

9. Should all the change tests necessarily succeed 100% or are there some admissions? What are they?
10. Is business side contributed to testing, in what cases and how?
11. Are external service providers contributed to testing, in what cases and how?
12. Who should give a final approval to testing results?

<u>The log of changes</u>

13. What kind of logs in connection with changes are recorded and saved?
14. What kind of information do the logs contain?
15. What is the time period the logs will be maintained?
16. Does anyone have the possibility to change the logs afterwards?

<u>Release/version management and rollback</u>

17. In which circumstances release will be cancelled, it means the roll-back procedure will be activated?
18. Who has to accept roll-back and how its impact will be assessed?
19. When change is implemented for some time and problems occur, what action will be taken – new corrective change or something else?
20. How are the versions originated – is it case of enough of changes or rather during some certain time period?
21. Is the responsible person of business continuity informed about important changes to ensure his/her readiness and how does it happen?

The issues to consider:
Action plan;
Audit trail;
Security analysis;
Change test;
Changes approve.

Change management

Documentation:

- Policies and procedures for making regular or urgent changes in information systems;
- Log file or journal with information about realized changes and corresponding approvals;
- Schedule of planned changes;
- Documentation in connection with making changes.

Activities:

1. Using interviews ensure:
   - Who does give the priority to changes and who does approve the changes;
   - How will user requirements expressed to the programmers;
   - How will changes be tested;

- Who does assign the changes;
- How will changed applications be implemented into actual environment?

2. Ensure the integrity of changes:
    - Will all proposed changes be analyzed;
    - Does the business value exceed the cost of change generally or is the change needed because of other reasons;
    - Will all approved changes be implemented as scheduled?

3. Ensure that in acceptance and implementation of changes relevant employees are involved:
    - End-users to consider that change is relevant;
    - IT personnel;
    - Other employees if necessary – for example, quality manager, information assets owners, information security persons etc.

4. Review emergency procedures;
5. Review procedures for making a single change (for example, detail correction);
6. Ensure that log of changes is complete and describes real situation (ordinary and extra changes are logged);
7. Find out how will implemented change occur inside of business continuity plan and/connected environment;
8. Find out the following:
    - What kind of programs can programmers control;
    - What kind of programs can programmers change;
    - Who, moreover, can control or change programs;
    - Who can implement changes in working environment
9. Ascertain, who and with which arguments will decide that current change is tested sufficiently;
10. Ascertain that segregation of duties between tester and programmer exists;
11. Ascertain that standards and requirements are used for testing;
12. Ascertain that testing results and conclusions are recorded;
13. Ascertain that testing plans are adequately detail;
14. Ascertain that in testing process single programs tests and the whole system tests are accompanied;
15. Ascertain, that through testing it is possible assure that information system processes data correctly and gives signals if something is incorrect;
16. Ascertain that there exist adequately documented testing plans which include testing scenarios, testing requirements, expected testing results and testing criteria;
17. Ascertain that real testing results will be documented and compared with expected testing results;
18. Ascertain that testing plans are reviewed by management and recorded in way that plans can be audited to ensure the reach of concluded tests;
19. Ensure that real testing is made in testing environment and it is created separate

live and real working environment;

20. Ensure that testing environment has the same arrangements like live environment (hardware, operating system, database solution etc.);
21. Ensure that access to the testing environment is restricted;
22. Find out how will be testing data collected:
    - To imitate real business operations, there should be adequate set of data in hand;
    - The real users who will start work with new solution should be engaged in collecting testing data;
    - To protect testing data for unauthorized publishing or modifications, there should be access control system or software used. The real data used by testing should be deleted after tests.
23. Is a parallel testing used (new system is under operation in parallel with old system and the outcomes will be compared to establish differences).

**For assessment**

Quantity

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Change management procedure | | | | | | |
| | | | | | | |
| | | | | | | |

Quality

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Action plan | | | | | | |
| Audit trail | | | | | | |
| Security analysis | | | | | | |
| Change test | | | | | | |
| Change approval | | | | | | |

Control

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Roll-back plan | | | | | | |
| | | | | | | |

**Outsourcing IT services**

**Description**

All external service providers must be identified and any organizational relationship and technical interface with them must be documented.

No access shall be allowed to external service providers to the means of the organization until the necessary security measures have been taken and a contract specifying access conditions has been signed.

Selection procedures of external service providers must be implemented in a company that would ensure the use of a functioning and efficient service for the company.

The procedures of a company must ensure that services are contracted with all external service providers and that regular review of the compliance with the terms and conditions and the needs of the company are carried out.

**Content and criteria**

Service level agreement.

Compliance with firm’s policies and roles for:

- Security
- Business continuity

Right to audit.

Monitor third party service delivery.

Use of external service providers

External service provider selection procedure.

Contracting

Third party service delivery management – cost of downtime due to non-fulfillment of service level agreements. Performance evaluation of third party providers to include quality of service, delivery, cost etc.

Use of external service providers

Documentation:

- Outsourcing policies, procedures and requirements to the outsourcing contracts;
- A list of external service providers;
- Selection of outsourcing contracts related to services in connection with certain functions, process and/or system;
- In connection with selected outsourced services extract of payments, reports, process of contract observation etc.;
- The list of employees who can sign the outsourcing contracts and determine the monetary limits.

Activities:

1. Find out, respectively the returns of outsourcing and business case (direct and indirect costs and benefits);
2. Ensure that all external service providers have contracts, these contracts are effective and the services are presented in agreed level (at least capacity and quality);
3. Ensure that organizational relations and technical interfaces with external service providers are documented;
4. Ensure that risk assessment is done before contracting with external service provider;
5. Evaluate the process of deciding on external service provider;
6. Evaluate the process of payments;
7. Evaluate the procedures of technical support;
8. Find out how the access is allowed to external service providers (operating systems, applications, networks and accesses outside of enterprise premises);
9. If possible, overview physical security measures and controls, system development and administration of external service provider;
10. Ensure that external service provider is taken measures to secure enterprises information (for example of other clients);
11. Evaluate enterprise internal procedures taken to monitor of service delivery;
12. Give an opinion how difficult (considering cost, time etc) it could be to disclaim of services by external service provider;
13. Ensure that in inside of contract there is stated following:
    - Requirements and expected results,
    - cost of services,
    - payment conditions,
    - process of resolving problems,
    - monetary demands in case of service disruptions,
    - changes in contract and contract updating conditions
    - contract termination conditions,

- reporting procedures (content, frequency, communication)
- participants' roles and responsibilities,
- business continuity assurance,
- contract period,
- access rights and access levels,
- ownership rights if necessary,
- security requirements,
- guarantee.

**For assessment**

Quantity

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Service level agreement | | | | | | |
| Contract main points | | | | | | |
| Selection procedure | | | | | | |

Quality

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Access conditions | | | | | | |
| Compliance with internal policies | | | | | | |
| Right to audit | | | | | | |

Control

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Monitoring of service delivery | | | | | | |
| | | | | | | |
| | | | | | | |

**Volume and performance management**

**Description**

A company must have a functioning process for the monitoring of the performance of the information system and for reporting. Requirements of users on the availability and performance of the information system must be determined and reviewed regularly. Timely meeting of performance needs of the information system must be guaranteed on the basis of the results of monitoring of the performance of the existing system and the forecast of future performance needs.

A company must have a complete and regularly updated list of inventory of the information technology hardware and software configuration used. The hardware and software platform used must be standardized, if possible.

A company must lay down requirements that would preclude the use of unauthorized and unlicensed software. A company must perform routine checks for the discovery of unauthorized software and for the control of conformity with license agreements.

**Content and criteria**

IS user’s requirements.

IS performance monitoring.

Configuration management.

Inventory of information technology configuration.

Unauthorized and unlicensed software.

Control of conformity with license.

Capacity management

Documentation:

- Systems availability requirements from service level agreements (SLA);
- The reports of the problems in connection with systems availability, problem solution descriptions (process, documentation);
- Protocols in connection with systems availability;
- Monitoring records in connection with capacity and availability indicators;
- Documentation regarding capacity and availability planning, expenses in IT

budget.

Activities:

1. Find out how is organized monitoring of systems availability;
2. Observe what kind of technology is used for monitoring systems availability and what kind of reviews or analyses occur;
3. Find out what kind of parameters and indicators are under monitoring;
4. Find out how the capacity planning process is planned, is it business side involved and how are the external factors analyzed.

Configuration management

Documentation:

- Established requirements for software and hardware platforms;
- Established rules for users using computers;
- A list of hardware and software in use.

Activities:

1. Ensure that employed hardware and software platforms are standardized;
2. Find out how inventory of hardware and software is organized, review the information of last inventory;
3. Ensure that measures are taken to avoid unauthorized hardware and software installation;
4. Control some server or computer hardware and software platform's conformity with established requirements.

**For assessment**

Quantity

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Performance management procedure | | | | | | |
| | | | | | | |
| | | | | | | |

Quality

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| IS users' | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| requirements | | | | | | |
| Configuration management | | | | | | |
| | | | | | | |

Control

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Control of conformity with licenses | | | | | | |
| IS performance monitoring | | | | | | |
| | | | | | | |

**Problem management**

**Description**

Official procedures and duties must be laid down for the reduction of damages resulting from security attacks, emergencies and system failures, for registration of security incidents, responding to them and drawing conclusions from them.

Notification procedure in regard to different types of security incidents (violation of security, threat, defect or failure) that may affect the security of the assets of an organization must be communicated to all relevant employees and contract partners. Relevant security points must be notified of any discovered or suspected security incidents as soon as possible.

**Content and criteria**

Official problem and incident management procedure.

Security incident notification procedure.

Problem and incident management

Documentation:

- Policies and procedures for problem and incident management;
- Extract from incident/problem registry and review of some cases – incident/problem start date, level of importance, impart date, analysis, reporting, communication, connected documentation (in paper and in the electronic form);
- Reviews and reports.

Activities:

1. Ensure that during incident/problem solving internal policies and procedures are followed;
2. Find out whether during incident/problem solving the next is appointed:
    - Determined incident/problem identification and attached importance to adequate risk level;
    - Analysis of incident/problem impact and reasons;
    - Documentation of identified problems and status observation;
    - A solution for incident/problem;
    - Reporting to the management;
    - Contact lists and communication of all relevant information:
        - Contact persons names, posts and phone numbers;
        - A list of groups, who and about what should be informed (for example, business management, publicity, media, business partners, public relations etc.).

**For assessment**

Quantity

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Incident management procedure | | | | | | |
| Problem management procedure | | | | | | |
| | | | | | | |

Quality

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Incident notification | | | | | | |
| Different | | | | | | |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| types of incidents |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Control

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Incident monitoring |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Operations management**

**Description**

Main standard IT operations must be documented and reviewed regularly in order to ensure the systematic processing (in terms of timing, order, quality, etc.). Operations logs must be checked in order to ensure the correctness and integrity of processing.

Documented work instructions and procedures must be laid down for the management and use of the information system. Upon making changes in the information system, relevant procedures must also be reviewed and the users must be notified of the changes made.

Requirements for the control and assessment of information technology activities must be provided for in a company. It is necessary to assess whether internal requirements of the company, efficiency of IT services and correspondence of IT activities to business objectives have been followed in information technology activities. Independence of the assessment must be ensured in providing the assessment.

External audit must be used, if necessary, for the assessment of compliance of information technology controls, laws and regulations concerning information technology and the performance of contractual obligations in the field of information technology. Assessment results must be presented to the management of the company.

Information technological means supporting critical or sensitive functions must be installed in security areas with restricted access and they must be physically protected from unauthorized inquires, damage, security threats (e.g. fire) and environmental risks.

**Content and criteria**

IT operations documentation.

IT operations logs.

Management of procedures.

IS work instructions.

Monitoring and assessment.

Requirements for the control and assessment of information technology activities.

Monthly report should include:

- Accounts added or modified without proper authorization
- Information security violations
- Average number of
    - external system probes / attempted attacks per system
    - internal system probes / attempted attacks per system
    - database denied access attempts
    - network denied access attempts
    - viruses quarantined (found, recognized, identified, destroyed, erased) within email /network

Auditing issues.

IT governance maturity model:

- non-existent
- initial/ad hoc
- repeatable but intuitive
- defined process
- managed and measurable
- optimized

**Facility management**

Security areas.

**Compliance with external requirements**

Regular IT organization compliance assessment – the period of making compliance assessments or audits should be assigned by supervised entity, but it should be ensured that in every case of bigger changes in external requirements assessment or audit will be performed.

External requirements – the external requirements for information technology field may come from legislation (for example, personal data protection act), sector-wide legislation (for example, credit institutions act), the regulations from supervision authority (the requirements for the organization of the field of information technology), but also from different decrees (for example, decrees of national bank, European Union etc.) and also from standards and good practices.

Measures – the possible solutions may be the changes in internal policies, regulations and standards. To find out the necessary measures, additional audit could be performed.

Exploitation management

Documentation:

- Information technology administration rules and procedures;
- Information systems administration logs.

Activities:

1. Review the process of making changes in information systems – only authorized persons can make changes with responsible persons confirmation;
2. Find out whether logs about administration activities will be made and whether according log files exist. Ensure that administration journal (what should be done) conforms to log (what is done) and review the progress (success, failures);
3. Ensure that after administration activities, systems' security mechanisms work as needed and such controls are documented;
4. Review how the use of administration interfaces is regulated and how they are implemented in practice;
5. Find out how the external service providers will be accompanied to administration activities – if there is a need for accompany external service providers, observation by qualified and authorized IT personal should be in place and service providers' activities should be enrolled to administration journal;
6. Find out if there exists a commitment to follow arrangement about keeping confidential information in case external service provider specialists are involved in administration activities;
7. Find out how external service providers get an access to the information systems for performing administrative activities – external service providers should not be allowed to access before security measures are implemented and contracts with terms and conditions are agreed;
8. Find out whether remote administration is used and what kind of security measures are taken;
9. Ensure that logs will be made and kept about the administration activities;
10. Find out who reviews and how often administration log files with purpose to detect unauthorized activities.

**Monitoring and assessment**

Documentation:

- Reports from internal audit;
- Reports from external audit;
- Risk assessments;
- Service level agreements (SLA);
- Reports of services availability, etc. (according to SLA's).

Activities:

1. Ensure that exists independent IT auditor or internal auditor who performs IT auditing;
2. Review independency of IT auditor – find out subordination and reporting lines;
3. Find out the tasks for IT audit and how these tasks are performed;
4. Find out whether IT audit reports will be presented to the management;
5. Find out whether a time table will be made to revise IT audit findings and find out whether the problems are solved;
6. Ensure that *follow-up* controls are performed;
7. Find out the IT services about service level agreements with business side are contracted;
8. Ensure that requirements described inside of contracts (availability, upgrades, continuity, backups, etc.);
9. Ensure that process for regular review of SLA's terms and conditions are in operation and reporting to business side about performance of SLA contract is regular;
10. Review the last external audit reports and point out the findings;
11. Ensure that external audit findings are presented to the management;
12. Ensure that process for dealing with weaknesses and improving processes and controls exist as recorded in audit reports.

**For assessment**

<u>Quantity</u>

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| IT operations documentation | | | | | | |
| | | | | | | |
| | | | | | | |

<u>Quality</u>

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| IT operations logs | | | | | | |
| Management of procedures | | | | | | |
| IS work instructions | | | | | | |
| Facility management | | | | | | |
| | | | | | | |

Control

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Monitoring and assessment | | | | | | |
| Compliance with internal requirements | | | | | | |
| Compliance with external requirements | | | | | | |

Information security

The information security part consists of nine sub-parts: information security policy, information security organization, logical security, physical security, communications and operations, access control management, information systems security, information security incident management and information systems audit considerations. Each sub-part contains definition, description, content and criteria and format for assessment.

**Information security policy**

**Description**

Common information security principles of supervised entity shall be represented inside of information security policy. Management should set clear direction with information security policy, demonstrate contribution and assistance in ensuring information security inside of organization.

Information security assurance is a part of entity’s risk management, and information security policy should conform to risk assessment results and correspond to information security level.

Inside of information security policy, conception of information security should be defined, the measures for ensuring information security, responsible persons for information security and programs, standards, procedures and guidelines for implementing information security should be described.

The employees of supervised entity should be aware of current information security policy, arisen regulations from information security policy and their roles and responsibilities in ensuring information security. In case of bigger changes in information security policy, communication of employees should be conducted, also the new employees should be instructed in current information security policy.

Considering supervised entity’s business domain, business and IT strategy and risk toleration, bringing information security policy up-to-date frequency should be established. Also, it should be ensured that information security policy review occurs in case when reforming business operations or making changes in information technology governance.

**Content and criteria**

Information security policy document

Written policy document or written policy statements have to be at present to prove

information security engagement.
Separate document.
Information security policy statements may be included to action plans, standards, procedures or guidelines which contribute policy implementation.
Management direction – demonstration of management approval.
The management can show their contribution best by following policy statements and more practically, management is ready to guarantee resources for conducting proper information security programs and projects.
It should be ensured that information security is continuously effective, for example, by adding clause that policy is effective until changes occur.

The content of policy document – a list of topics which should be included into policy document and :

- Introduction
- Purpose
- Vulnerabilities
- Scope of Information Security Policy
    - Definition of Security
    - Security Domains
    - Reasons for Information Security
- Roles and Responsibilities
    - Policy Management
    - Policy Implementation
    - Custodians
    - Owners
    - Individuals
    - Services
    - Standards and Guidelines
    - Availability
    - Changes
- IT Security Principles
    - Basis of Current Policy
    - Compliance with Legislative and Contractual Requirements
    - Responsibility
    - Reporting of Gaps and Breaches
    - Residual Risk
    - Security Documentation and Audit
    - Ability to Trace
    - Access on the Principle of Least Privilege
    - Security Awareness and Training
    - Review of Policies
    - Security Adherence

<u>Part of risk management</u>

Asset Classification and Control

Risk analysis – information security policy should consider the results of risk assessment and information about risk analyses conducted by enterprise.

Reported risks:

- Meaningful monitoring and metrics of security performance
- Align with corporate goals
- Provides meaningful information as business-centric metrics
- Reports residual risk
- Highlights significant trends and events

Security level – considering the risks, the decision about acceptable level on risks should be stated (risk appetite). Considering the risk appetite, a suitable security level should be assigned, it means how much and what kind of measures will be taken to reduce risks. Considering the information processed in financial institutions and its sensibility, it will be assumed that accepted risk level is rather low than high and regarding that, information security level is rather high than low.

Information Security & Controls Framework Key Areas (ISC) Domains:

- Application Controls
- Application Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Legal, Regulations, Compliance & Investigations
- Operations Security
- Physical (Environmental) Security
- Security Architecture & Design
- Telecommunications & Network Security

The measure could be policy coverage, for example percentage of sections of ISO/IEC 27001/2 for which policies plus associated standards, procedures and guidelines have been specified, written, approved and issued.

Risk control

*Extent of policy deployment and adoption across the organization (measured by Audit, management or Control Self-Assessment).*

Definition of IT security – how is information security understood inside of enterprise, what part of business and what kind of services are captured etc. What kind of information security aspects are important in connection with information assets and information security level:

- confidentiality – protection of information against unauthorized publication;
- integrity – protection of information against counterfeiting and unauthorized alteration;
- availability – timely availability of information and services for authorized persons.

Assessment information security – to assess whether information security level is in effect.

Security assessment:

- Abide by Service Level Agreements
- Incidents

- (Compliance)audit results

Information about the assessment results is reasonable to collect for some time period, because the single events could not show the real situation. Having the information for period, it is possible to conduct trend analysis to find out the topics where information security measures are not appropriate.

Responsibilities for information security – overall responsibility and responsible person (CISO – Chief Information Security Officer or duties for suitable and competent person). Overall responsibility – through management due diligence.

Ensuring information security:

- Strategy and action plans
- Standards
- Procedures
- Guidelines

Security awareness

Inside of enterprise a process should be established how the new employees get know about current information security policy – for example, as a part of information packet for new employees, need to sign a paper to ensure that policy statements are understood etc. Also, it should be regulated how all the staff gets know about the changes in information security policy – an informative e-mail to all employees, notification in intranet, informing event etc. Also, it should be stated how current information security policy document will be made available to all employees – intranet etc.

Review of security policy

Time period or some cases should be established when information security is to be reviewed and if necessary, is to be updated. Time period is considered in practice annually and the cases when information security needs review could be, for example:

- Adding important services for business (i.e., giving loans);
- Adding the channels for offering services; (i.e., internet banking);
- In case of serious incident (i.e., important business disruption);
- New or changed external regulation (i.e., changes in laws);
- New or changed internal regulation (i.e., tighter SLA conditions).
- The results of risk analysis (i.e., increased risks in certain area).

*ISO 27k guidance (for asset classification):*

*Responsibility for assets - Percentage of information assets at each stage of the classification process (identified / inventoried / asset owner nominated / risk assessed / classified / secured).*

*Information classification - Percentage of key information assets for which a comprehensive strategy has been implemented to mitigate information security risks as necessary and to maintain these risks within acceptable thresholds*

*Percentage of information assets in each classification category (including not-yet-classified).*

Systems security

Documentation:

- Information security policies, procedures, rules, etc.;

Activities:

Identify systems which have been lately modified (hardware, software, connections, configuration, etc.). Find out business processes in connection with these systems.
Assess security needs and the latest security incidents;
Ensure that physical, technical and organizational information security measures are implemented;

1. Ensure that management establishes information security policy, strategy and security organization that is responsible for information security activities, corresponding standards and procedures.
2. Ensure that information security policy document is up to date and is available for all employees;
3. Information security policy has to include at least following:
   - Main principles about information security and security needs for enterprise;
   - Management responsibility to nominate information security manager and establish the functions;
   - Employee's obligations to follow internal rules, standards and procedures for information security. There has to be stated that what is not clearly allowed is denied;

**For assessment**

<u>Quantity</u>

| **Criteria (yes/no)** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Separate document | X | X | X | | | |
| approved by management | X | X | X | X | X | X |
| Information security statements | | | | X | X | X |
| verified by management | X | X | X | X | X | X |
| Currently effective | X | X | X | X | X | X |

Quality

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Responsibility for information security | | | | | | |
| information security aspects – availability | | | | | | |
| information security aspects – integrity | | | | | | |
| information security aspects – confidentiality | | | | | | |
| security measurement mechanism | | | | | | |
| security measures | | | | | | |
| awareness statement | | | | | | |

Control

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Review period | | | | | | |
| Indicators for review | | | | | | |
| | | | | | | |

**Information security organization**

**Description**

Common responsibility for ensuring information security inside of enterprise resides in management. Information security responsibility should be assigned to certain employee and considering the size of enterprise and complexity of its business, a separate post should be created. It is suggested that responsibility for organizing information security is assigned to one member of board.

The primary obligations of responsible person shall be to ensure, that information security activities correspond to information security policy and internal and external regulations. One of the most important functions for responsible person should be coordination of staff's activities in ensuring information security inside of organization.

Accompanying business side into information security initiatives, it is suggested to create an information security steering committee which consists of managers of all important business units and functions and information security officer (ISO).

The requirements for confidentiality, information security roles and responsibilities described in information security policy shall be fixed for each employee. Ensuring information security in performing their duties should be a responsibility of each employee and it should be expressed in organizational culture and contracts with employees. The employees should be aware of their duties and responsibilities in ensuring information security.

Supervised entity should assess the risks connected with using external service providers, including risks to information security. Risk assessment should be done in choosing, in contracting and in stipulating service level agreements with external service providers. Considering the content of outsourced services it should be assigned what kind of security criteria the service provider must meet. Control mechanism should be established to assess external service provider information security efficiency. Detailed requirements for outsourcing are covered by the advisory guidelines of the Financial Supervision Authority "Outsourcing Requirements for Supervised Entities", established 25.10.2006 with management decision 1.1-7/84.

**Content and criteria**

Appropriate person for CISO – Chief Information Security Officer – position should have necessary practical experiences and theoretical knowledge. For example, one possibility to ascertain appropriateness is to have relevant certificates (for example CISM – Certified Information Systems Manager or CISSP – Certified Information Systems Security Professional). Also, appropriate employee should understand the business processes.

The tasks of person responsible for information security

Information security steering
Board of Directors

- Members of the board need to be aware of the organization's information assets and their criticality to ongoing business operations

Executive Management

- Provide IS reporting and recommendations to assist executive management in alignment and monitoring of information security activities in support of organizational objectives

Steering Committee

- Provide reporting & recommendations to ensure alignment of the security program with organizational objectives and in achieving behavior change toward a culture that promotes good security practices and policy compliance

Lines of Businesses

- Effectively communicate Information Security Risk vision, strategy and overall program to a broad range of technical and non-technical people

The roles and responsibilities of ensuring information security

Information security as responsibility for all employees (there has to be a concrete statement), obligations and responsibilities by role in an organization has to be highlighted.

BIRO – Business risk information officer, responsibilities:

- Information Security Governance & Oversight to their Lines Of Business (LOB)
- Access Management
- Vendor IS Assessments
- Project IS Assessments
- IS Training & Awareness
- Confidential Waste
- EUC Management
- Management of LOB IS Risk Assessments
- Oversight of IS Risk audit findings

The role of external service provider in ensuring information security.

Risks of outsourcing (Saas - Software as a service):

Confidentiality concerns

– Who has access to the information?<br>
– What controls are in place to limit access?<br>
– Are the files stored encrypted?<br>
– What controls are in place for granting access?<br>
– What controls are in place on the people who have access to the information?<br>
– How are the systems managed to prevent unauthorized access?<br>
– How are data separated between clients (law enforcement issue as well)?<br>
– Are real data used for testing?<br>
– How is the information protected when traversing unsecured networks?

Integrity concerns

– Who has the ability to modify the information?<br>
– What controls are in place to limit access?<br>
– What controls are in place for granting access?<br>
– What controls are in place to verify the information?

– What controls are in place on the people who have access to the information?
– How are the systems managed to prevent unauthorized access?
– How are data separated between clients?
Use control concerns
– What controls are in place to limit information use?
– What controls are in place on the people who have access to the information?
Availability concerns
– Do the vendor’s disaster recovery and business continuity plans meet the enterprise’s requirements?
– What about geographic dispersion?
– How does the vendor perform backups?
– Is there sufficient capacity in the vendor’s network to meet current and expected demands?
– What is the vendor’s software development process?
– Is customer data stored together on the same systems (law enforcement issue)?
– What search capabilities are provided by the vendor and how can the data be downloaded?

Controls for outsourcing:
Policies, standards, and procedural controls
– Control standards must be compatible
– Policy implementation must be compatible
– Vendor must meet the enterprise’s hiring standards
– Change control procedures must include both the vendor and the enterprise
– Enterprise procedures must be updated to include dealing with the vendor
Differences between the enterprise and the vendor should be minimized
• If the vendor is too lenient, the enterprise may not meet its requirements
• If the vendor is too strict, the enterprise may not realize cost savings
– Vendors may not be willing to change internal policies as their economies of scale may suffer
Technical controls
Management controls
- Note that any loss of management control must be compensated for using technical or contractual controls
– Proper management of outsourced activities requires:
• Clearly stated requirements
• Clearly defined reporting requirements
• Verification of the work
Influence over the vendor’s employee practices
• Hiring practices
• Rewards and penalties
• Career advancement and loyalty
– Impact to enterprise employees
• Outsourcing can destroy employee loyalty
• Retention of important skills and expertise
- Audit will replace day to day management oversight of employees

– Contracts must be written to allow audits
– Audits must be performed
Contractual controls
- The enterprise is attempting to exchange technical and managerial controls for legal controls over the vendor
– Contracts should be written with appropriate controls that place the liability on the vendor
– The vendor must be large enough to sustain the loss associated with the liability
- Vendors also try to manage their risk
– Vendors will not accept risk for which they do not have adequate controls
• SLAs for availability with limited risk for the vendor can be found
• Agreements where the vendor assumes all risk for the protection of confidential information will not be found
- The ability to change vendors may seem like the ultimate control but it is less than it appears
– Once an enterprise is deeply entangled with a vendor, it is very difficult to cancel the contract

*ISO 27k guidance*

*Internal organization - percentage of organizational functions/business units for which a comprehensive strategy has been implemented to maintain information security risks within thresholds explicitly accepted by management.*
*Percentage of employees who have been assigned formally accepted information security roles and responsibilities.*
*External parties - percentage of third party connections that have been identified, risk-assessed and deemed secure.*

Documentation

- List of external service providers and according services or systems;

Activities

4. Find out the quantity and qualifications of security team;
5. Find out how much outsourcing is used in IT activities (information processing, technological support, security management etc.);

ISF (2011) guidance

Principle - Control over information security should be provided by a high-level working group, committee or equivalent body, and be supported by a top-level executive.

- There should be a top-level executive (or equivalent) with overall responsibility for information security.
- A high-level working group, committee or equivalent body should be established for coordinating information security activity across the organization. The group should meet on a regular basis (i.e., three or more times a year) and document actions agreed

at meeting.

- Membership of the high-level working group should include:
  - top management (i.e., a board-level executive or equivalent)
  - one or more business owners (i.e., people in charge of particular business applications or processes)
  - the head of information security, or equivalent (i.e., the Chief Information Security Officer)
  - representatives of other security-related functions (i.e., legal, operational risk, internal audit, insurance, human resources, and physical security)
  - the head of IT (or equivalent).
- The high-level working group should be responsible for:
  - considering information security enterprise-wide
  - ensuring information security is addressed in a consistent, coherent manner
  - approving information security policies and standards / procedures
  - monitoring the organization's exposure to information security threats
  - monitoring information security performance (i.e., analyzing the current security status, handling information security incidents and costs)
  - approving and prioritizing information security improvement activity
  - ensuring information security is addressed in the organization's IT planning process
  - emphasizing the importance of information security to the organization.

Principle specialist information security function should be established, which has responsibility for promoting information security enterprise-wide.

- The organization should be supported by an information security function (or equivalent), which has responsibility for promoting good practice in information security enterprise-wide. The head of the information security function should be dedicated to information security full-time.
- The information security function should:
  - develop and maintain an information security strategy
  - co-ordinate information security across the organization
  - define a set of security services (i.e., identity services, authentication services, cryptographic services), which provide a coherent range of security capabilities
  - develop information security standards / procedures and guidelines
  - provide expert advice on all aspects of information security (i.e., information risk analysis, information security
  - incident management and malware protection)
  - oversee the investigation of information security incidents
  - run one or more information security awareness programs and develop security skills for staff enterprise-wide
  - evaluate the security implications of specialized business initiatives (i.e., outsourcing, electronic commerce initiatives and information exchange)
  - monitor the effectiveness of information security arrangements (i.e., using tools such as the ISF's FIRM, ROSI and security health check).

The information security function should provide support for:

  - information risk analysis activities
  - important security-related projects

- major IT projects with security requirements
- security audits / reviews
- classification of information and systems according to their importance to the organization
- the use of cryptography
- incorporating information security requirements into documented agreements (i.e., contracts or service level agreements)
- the development of business / service continuity plans.

The information security function should monitor:

- general business trends (i.e., prospects for growth, internationalization, electronic commerce and outsourcing)
- technological developments (i.e., web-based technology, service oriented architecture (SOA) and Voice over IP)
- new and emerging threats (i.e., identity theft, spear phishing and Bluetooth attacks)
- new vulnerabilities in key operating systems, applications and other software (i.e., using vendor websites and mailing lists)
- new information security solutions (i.e., digital rights management and intrusion prevention)
- emerging industry / international information security-related standards (i.e., the Standard of Good Practice, ISO/IEC 27002 (17799), and COBIT v4.1)
- emerging legislation or regulations related to information security (i.e., those related to data privacy,
- digital signatures and industry-specific standards such as Basel II 1998 and the Payment Card Industry (PCI) Data Security Standard).

The information security function should:

- be adequately resourced in terms of the number of staff, their range and level of skills, and tools or techniques (i.e., information risk analysis methodologies,
- forensic investigation software and an enterprise-wide security architecture)
- have sufficient impact on the organization and strong support from top management, other business managers and IT managers
- maintain contact with counterparts in the commercial world, government and law enforcement agencies and with security experts in computer / software companies and service providers
- be reviewed on a regular basis (i.e., to ensure it performs as expected).

**For assessment**

Quantity

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Information security organization structure | X | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |

Quality

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Management responsibility | X | | | | | |
| Separate post for CISO | X | | | | | |
| Steering committee | | | | | | |
| Employee roles | | | | | | |
| Employee responsibilities | | | | | | |
| Requirements for outsourcing partners | | | | | | |

Control

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Control of outsourcing partner | | | | | | |
| | | | | | | |
| | | | | | | |

**Logical security**

**Description**

The mechanisms should be established to control background of employees who will be in charge of important functions (for example, the employees who have special rights in information systems). In addition to competences of specialty, the features of enterprise sector and need to work with sensitive information should be considered.

Before giving access to the information assets, it should be ensured that users are aware of current policies and procedures (including security requirements and other functions) and they know how to use information technology and systems on purpose. It is suggested to regularly organize instructions to all employees (including management) to arise the knowledge about information security. The instructions would present in first order information security policy, the reasons of information security importance, the duties and procedures connected with information security, requirements, reporting about information security incidents and their influence.

As an additional information security measure, it is suggested to add clause to the contracts with employees about the obligations to keep confidential information and responsibilities in being mistaken these obligations also after employment.

Employees' rights, obligations and responsibilities should be clearly defined and determined inside of instructions and information security regulations.

**Content and criteria**

Background checks of responsible employees. In addition to our demands, there are other possibilities. It is essential for organizations to verify the backgrounds of those with access to personal data.

- Educational Verification
- Past Employers
- Certifications and Affiliations

For example, certification demands are a growing field in Estonia as well. For public sector institutions, a security audit is allowed only by certified auditors like CISA or similar.

Relevant training.
Security awareness

- Get management support
- Have a plan and document it
- Evaluate annually
- Keep it simple
- Recognize your audience

Commitment to work with confidential information – for example, in banking sector appropriate.

The rights, duties and responsibilities of employees in connection with information security.

*ISO 27k guidance*
*Prior to employment - percentage of new employees plus pseudo-employees (contractors, consultants, temps etc.) that have been fully screened and approved in accordance with*

*company policies prior to starting work.*
*During employment - response to security awareness activities measured by, say, the number of emails and calls relating to individual awareness initiatives.*
*Termination or change of employment - percentage of user ID-s belonging to people who have left the organization, separated into active (pending deactivation) and inactive (pending archival and deletion) categories.*

ISF guidance

Principle - specific activities should be undertaken, such as a security awareness program, to promote security awareness to all individuals who have access to the information and systems of the organization.

Specific activities should be performed to promote security awareness enterprise-wide. These activities should be:

- endorsed by top management
- the responsibility of a particular individual, organizational unit, working group or committee
- supported by a documented set of objectives
- delivered as part of an on-going security awareness program
- subject to project management disciplines
- kept up-to-date with current practices and requirements
- based on the results of a documented information risk analysis
- aimed at reducing the frequency and magnitude of information security incidents
- measurable.

Security awareness should be promoted:

- to top management, business representatives, IT staff and external individuals
- be provided with information security education / training (i.e., using techniques such as presentations and computer-based training (CBT))
- by supplying specialized security awareness material, such as brochures, reference cards, posters and intranet based electronic documents.

Staff should be provided with guidance to help them understand:

- the meaning of information security (i.e., the protection of the confidentiality, integrity and availability of information)
- the importance of complying with information security policies and applying associated standards / procedures
- their personal responsibilities for information security (i.e., reporting actual and suspected information security incidents).

The effectiveness of security awareness should be monitored by:

- measuring the level of information security awareness of staff
- reviewing the level of information security awareness regularly
- measuring the benefits of security awareness activities (i.e., by monitoring the frequency and magnitude of information security incidents experienced).

Security-positive behavior should be encouraged by:

- making attendance at security awareness training compulsory
- publicizing security successes and failures throughout the organization

- linking security to personal performance objectives / appraisals.

**For assessment**

Quantity

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Awareness training materials | | | | | | |
| | | | | | | |
| | | | | | | |

Quality

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Awareness regulation | | | | | | |
| Confidentiality clause | X | X | X | X | X | X |
| | | | | | | |
| | | | | | | |

Control

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Key person background controls | | | | | | |
| | | | | | | |
| | | | | | | |

**Physical security**

**Description**

Supervised entities shall mark secure areas, which need protection and only allowed persons can entrance. The information assets maintaining critical or sensitive functions should be located into secure areas with limited access and these assets should be physically protected against unauthorized applying, damage, security threats (for example, fire) and environmental risks.

To protect secure areas with limited access, the physical and logical controls shall be used in a way, that only authorized persons can get access to areas.

Also a mechanism should be in place to ensure that all the entries into secure areas get recorded.

Choosing the measures to protect secure areas, it is suggested to get as a basis the recommendations and standards of some independent and recognized organization. Deciding on measures should currently start when the areas will be constructed and furnished. Outsourcing secure areas as a service, the same standards should be in place for external service provider.

It should be avoided to mark secure areas with remarkable notes and to use references. In planning secure areas, the rooms with windows should be prevented.

The possibility should be anticipated to physically or accidentally damage communication and electricity cables. It is suggested to use for cables a certain carrying construction and for open rooms it should be covered with suitable structural materials. Connecting sides of communication and electricity cables should be marked to enable fast correction in case the problem with cables occurs.

**Content and criteria**

Mapping of secure areas
Physical protection of secure areas

Logical protection of secure areas

Choosing the measures for protection of secure areas
Implementing the measures in using outsourcing

Physical protection of communications
Logical protection of communications – where are the access points?
Technological protection of communications
Marking the connections

*ISO 27k guidance:*
*Secure areas - Reports from periodic physical security site surveys, including regular status updates on corrective items identified in previous surveys and still outstanding.*
*Equipment security - Number of stop- or stock-checks performed in the previous month, and percentage of checks that revealed unauthorized movement of IT equipment, media etc. or other security issues.*

Locations management

Documentation:

- Internal and external audit reports;
- Incident reports;
- Network diagram;
- Risk analysis, zoning, the procedures for physical access;
- Physical security measures description for data carriers;
- A list of persons allowed to entrance secure locations;
- Registration book for quests.

Locations under review:

- Server rooms;
- Rooms for network facilities;
- Locations for maintaining important hardware, software, data carriers and paper documentation.

Activities:

1. Ensure that physical security measures taken for facilities and processing are in principle at the same level or analogous as similar institutions have;
2. Ensure that sensitive information’s (in paper or digital) physical security is adequately ensured by creating, processing, maintaining, administration or destruction processes;
3. Ensure that:
   - Physical access process for locations, where critical or sensitive information is handled, is adequate;
   - There are procedures in place for registering guests, access permissions delivery, accompany for guests and registration book;
   - Access permissions can be cancelled through relevant method.
4. Ensure that facilities for information processing and communication are adequately secured for physical attacks, environmental threats and miss-administration;
5. Ensure that there are implemented adequate security measures for detection and protection like fire and smoke alarms and extinguishers, raised floors, temperature and humidity sensors etc.

**Physical security measures: Level 1 (server rooms, communication center – facilities used only by concrete institution and it is not transit-center)**

1. Server rooms have to correspond to the security rules and standards confirmed by management;
2. Information systems servers have to be located into security areas, which conform to the security class of information these systems process;

3. Inside of server rooms, eating, drinking and smoking should be forbidden;
4. The procedures have to be in place which ensure that persons who do not operate with information systems and attendant facilities can access to the server rooms only accompanied by authorized persons. Authorized persons should be only the IT staff who are listed „Persons with right to access to server room“, which is signed by management;
5. Procedures have to in place to label all servers with visible marks, which show the server name and inventory number;
6. There has to be a list in server room where are recorded server names with inventory numbers, IP (internet protocol) addresses, applications, administrative personal names and contact information;
7. It has to be ensured that in case of electricity interruption data are not destroyed – it means that interruptible power supply (UPS) system has to be implemented, which guarantees at least 15 minutes reserved electricity to ensure that servers and other facilities can shut down smoothly;
8. Server room temperature has to be controlled constantly;
9. Cooling system (air-condition) has to be in place in case the temperature is not between +15 - +25 °C.
10. Server room guest book has to be implemented.

**Physical security measures: Level 2 (server rooms where databases with delicate personal data are kept and communication centers, which are transit-centers)**

11. It has to be ensured that information technology exploitation location is hided and physical marks are restricted;
12. Periodic controls are necessary to ensure that network of facilities conform to the requirements and documentation. In case of deficiencies or problems it has to be ensured that improvement actions for facilities or documentation are taken;
13. To the facilities, which display or deliver information in readable format, cannot be left without guarding so that unauthorized persons can read the information;
14. In server rooms, directly unnecessary and passing water-, electricity- and other communications should be avoided;
15. Server room's door has to be fire- and physical attack proof;
16. In server room, smoke sensors and fire alarms have to be implemented;
17. A log of all persons visited server room has to be compiled and maintained. The authentication mechanism could be, for example, a signature, fingerprint, electronic key card etc.

**Physical security measures: Level 3 (server rooms where are located servers process confidential information, communication centers)**

18. Transition to the backup power supply occurs as system is determined, uninterruptible power supply (UPS) and power generator are required;
19. On demand the measures have to be taken to avoid electromagnetic radiation;
20. Inside of server rooms, automatic extinguisher system must be implemented;
21. Air conditioning system must be implemented;
22. Water sensors must be implemented;

23. Monitoring mechanism for uninterruptible power must be in place;
24. There must be a mechanism to continuously review the list of server room guests;
25. It must be prohibited to deliver information for internal use only or confidential information without relevant permission;
26. From rooms, contain mission critical information technology and extremely confidential information and information processing, to deliver information there must be special rules confirmed and delivery should be restricted only for limited number of persons. For extra cases, there must be top management license obligatory.

**Physical security measures: Level 4**

27. Main server room and contained mission critical servers must be backed up;
28. Secondary server room should be located at least 5 kilometers from main server room.

ISF guidelines

Principle All locations that house critical IT facilities, sensitive material and other important assets should be physically protected against accident or attack.
There should be documented standards / procedures for the provision of physical protection in areas housing critical IT facilities within the organization.
Standards / procedures should cover the protection of:

- buildings against unauthorized access (i.e., by using locks, security guards and video surveillance)
- important papers and removable storage media (e.g., CDs, DVDs and USB memory sticks) against theft
- or copying
- storage areas (i.e., that might be used to store organizational assets, computer equipment and media, or important paper-based documents)
- vulnerable staff against intimidation by malicious third parties.

Buildings that house critical IT facilities should be protected against unauthorized access by:

- providing locks, bolts (or equivalent) on vulnerable doors and windows
- employing security guards
- installing closed-circuit television (CCTV), or equivalent.

Important papers and removable storage media (eg CDs, DVDs and USB memory sticks) should be protected

- against theft or copying by:
- storing sensitive physical material in locked cabinets (or similar) when not in use (e.g., by enforcing a ‘clear desk’ policy)
- restricting physical access to important post / facsimile points
- locating equipment used for sensitive printed material in secure physical areas.

Staff should be protected against intimidation from malicious third parties by providing duress alarms in susceptible public areas and establishing a process for responding to emergency situations.

**For assessment**

Quantity

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Secure area map | | | | | | |
| | | | | | | |
| | | | | | | |

Quality

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| SRM 1 | | | | | | |
| SRM 2 | | | | | | |
| SRM 3 | | | | | | |
| SRM 4 | | | | | | |

Control

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Testing of physical and logical controls | | | | | | |
| | | | | | | |
| | | | | | | |

**Communications and operations**

**Description**

Security areas with limited access should be continuously monitored to anticipate possible damage and in case of damages to enable quick detection.

For detection of unauthorized activities and to ensure effectiveness of implemented access and control mechanisms, appropriate monitoring for access and activities inside of information systems should be established. Unauthorized activity is certainly an activity which conflicts with legal instruments or which purpose or content is inappropriate implementation or omission of financial supervisors or investigators acts or proceedings, including manipulation with information integrity or availability comparing with period before obtaining an act or performing a proceeding. In getting respective requisition from supervisor, a supervised entity should in detail give reasons for unauthorized activity described previously.

To perform monitoring, a track of realized activities in information systems should be created. Appropriate monitoring level for different parts of information system should be determined based on risk assessment results. Tracks or logs shall be created about important information for enterprise considering at least possible events as following:

- Users' enters into system;
- Display of information;
- Making a queries;
- Applying to systems and applications;
- Database changes and operations;
- Attempts to get access to sensitive information;
- Information systems use under special (broadened) user rights;
- Unauthorized operations inside of systems.

Examination of logs should be accomplished in cases there is a motivated suspicion that operations of employees or clients are not legitimate and in cases there occur real threats to violate information availability, integrity and confidentiality.

The procedures shall be implemented to manage recorded logs and the measures shall be established to ensure logs availability, integrity and confidentiality. It is suggested to store data carriers of log files inside of secure areas and separated from information processing environment which was logged.

There should be documented and implemented procedures for making backups in place. Making of backups should be regular and backups should be stored inside of secure areas which avoids unauthorized access and ensures physical security. One copy of backup should be regularly and securely stored geographically separated areas. The usability and completeness of backups should be controlled regularly. Backup procedures shall include at least the following topics:

- Information which has to be backed up;
- Scope and frequency of backups;
- The responsibilities of making backups;
- Time for maintaining backups;
- Recovery from backups.

The supervised entities shall have the rules for what kind of information is interchanged with external parties, what kind of channels are used and how is information secured. In case the risks realize, it should be possible to implement alternative way for information interchange.

Confidential information interchange should be secured if communicated through public channels and it should be ensured that availability to the third parties is avoided. Considering bigger risks, information interchange protection using cryptography should be thought out. Communications security measures should be implemented for access to the communications, for services used and for activities accomplished.

To detect and prevent malicious software and computer viruses timely, the adequate measures and responsibilities should be implemented. Also it should be ensured that users are aware of danger in case the real risks connected with malicious software and computer viruses are raised and that supposition bases on information of adequate sources.

Supervised entity should have protective measures for portable info technological devices (for example, portable computers) and for portable media (for example, memory sticks) in place. In case the risks to data carriers are increased, the measures (for example, data encryption) should be taken for protection.

**Content and criteria**

Documentation:

- Network diagram;
- A list of the most important products, services and systems;

Monitoring of secure areas

Access monitoring
Activities monitoring

Logs
Composing of logs depends on the business needs, information criticality level and for what the information will be used.
To decide about logs, the ability to answer to three main questions should be considered:

1. Who did? – necessary is account user name, but it should be not enough information. In addition, it should be considered to log IP address, which makes possible afterwards to follow concrete computing machine in network in case there is suspicion that account is used by fake user.
2. What did? – a list of the most important actions follows, where logging should be in place:
   - User entrances
   - Information views
   - Making queries
   - Apply to systems and applications

- Changes and operations in database
- Attempts to get sensitive information
- System use under privileged user rights
- Unauthorized operations in systems

3. When did? – in addition to who and what, when the action took place is important to determine timely order of individual actions and based on that create opportunity to reproduce a situation. Information about when something happened includes at least date and time.

Information contains confidential data needs to be logged and certainly is such kind of information personal data and information in connection with customers.

Also it should be considered that making logs about everything can be troublesome. The auditors or supervisors must consider that aspect and in assessing the security measures automatically higher amount of information under logging does not mean better measure.

Review of logs

It should be appointed who is responsible for reviewing of log information, how the summaries will be composed (it is because of huge amount of data) and who will be reported about the results.

*Monitoring - Percentage of systems whose security logs are (a) appropriately configured, (b) securely captured to a centralized log management facility and (c) routinely monitored/reviewed/assessed. Trends in the number of security log entries that have (a) been captured; (b) been analyzed; and (c) led to follow-up activities.*

What should be monitored and logged?

- Production environment
- Production systems
- Secured IT areas
- Business Units
- Test/development

What needs attention?

- Logins and logoffs – for employee activity research
- Administrative application - system changes
- Patches - hotfixes
- Unauthenticated devices and accounts

Log management

Besides of composing the logs, also the management of log files in important issue. The questions like where the log files are maintained, how long the log files should be kept, who can access to the log files and delete files etc. Change of logs should be forbidden.

Back-up procedure

*Back-up - Percentage of back-up operations that are successful. Percentage of test backup restores that are successful. Mean travel time to retrieve back-up media from off-site storage to successful restored state at all primary locations. Percentage of backups and archives containing sensitive or valuable data that are encrypted.*

Full back-up and incremental back-up should be distinguished.

The rules for exchange of information

*Exchange of information - Percentage of third party links for which information security requirements have been satisfactorily (a) defined and (b) implemented.*

*Electronic commerce services - "e-Security status", i.e., informed commentary on the overall management confidence level, based on analysis of recent penetration tests, current/recent incidents, current known vulnerabilities, planned changes etc.*

**Network**

*Network security management - number of network security incidents identified in the previous month, divided into minor/significant/serious categories, with trends analysis and narrative descriptions of all serious incidents and adverse trends.*

*Media handling - percentage of physical backup/archive media that are fully encrypted.*

**S**ensitive data

Sensitive data by the definition are "data (information) which have to be protected according to relevant judgment and its publishing, changing, deleting or vanishing can cause some essential loss". In essence, such kind of explanation is similar to confidential information.

For example, sensitive data are by credit institution act (§ 88) bank secret as all the information and opinions which is known to credit institution in connection with its client or client of other credit institution.

Public network

Public network is mostly considered as public Internet. Using the segment of network given by the Internet service provider for data transmissions does not make it private network because supervised entities do not control such network thoroughly and access to the network is not absolutely restricted.

Data protection

Data protection or information protection is by the regulation a protection of data (information) to ensure:

- confidentiality – protecting information against unauthorized publishing;
- integrity – protecting information against unauthorized change;
- availability – available and usable information on right time.

Wide-spread information security measure to ensure confidentiality and integrity is data cryptography and such kind of measure is meant by Financial Supervision Authority's guidelines.

Three level of cryptography can be highlighted:

1. End-to-end encryption
2. Session encryption
3. network encryption

For example, PCI DSS assessment testing procedures encryption over open, public networks

- Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks
- Verify that strong encryption is used during data transmission

- For SSL implementations:
  - Verify that the server supports the latest patched versions
  - Verify that HTTPS appears as a part of the browser Universal Record Locator (URL)
  - Verify that no cardholder data is required when HTTPS does not appear in the URL
- Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data are encrypted during transit
- Verify that only trusted SSL/TLS keys/certificates are accepted
- Verify that the proper encryption strength is implemented for the encryption methodology in use (check vendor recommendations/best practices.)

Audit checklist:

- Are all required TCP/IP applications supported - operational and secure?
- Are users properly authenticated by multi-factor and other forms of strong authentication?
- Are comprehensive security checks used to check remote workstations for:
- Viruses, spyware, and other malicious software?
- Compliance with required configurations and patches?
- Removal of cached/temporary files/credentials at the end of a session?
- Are the following properly encrypted:
- Client to VPN (Virtual Private Network) gateway?
- VPN gateway to application servers?
- Is there sufficient access control granularity for authorizing access to:
- Destination systems?
- Applications, folders, files, and other application elements?
- Are VPN sessions be effectively audited and monitored?

Network security measures

- External perimeter protection
- Internal network protection

Protection against malicious code and viruses

*Protection against malicious and mobile code - trends in the number of viruses, worms, Trojans or spams detected and stopped. Number and cumulative costs of malware incidents.*

Protection:

- Security policy
- Education and awareness
  - E-mail attachment
  - Execution of applications
- Acceptable usage policy
- Patch level up-to-date on gateways, servers and clients
- Enforcing acceptable usage policy
- Content inspection on gateways
  - Blocking sites, content and communication

- Control allowed protocols
    - http, https, messengers, p2p, telnet, ftp, even
- antivirus on gateways, servers, clients
- firewall
- never trust documentation - test

Mobile devices and media protection

- Smartphone
- iPod
- Laptop
- USB
- CD
- DVD
- PC Card / PCMCIA
- SD
- Compact Flash
- Tape
- Diskette
- PDA

Risks:

- A media type to match every data need
- Ubiquity of acceptance and use
- Quick and easy data movement
- Transparent to the user
- Data backup
- Easy to transport
- More data in smaller packages

Usage of mobile devices gets more and more popular thanks to the new technologies and devices. Considering the wide range of possibilities, also the risks in using mobile devices is increasing.

To avoid information security risks in connection with mobile devices, it should be determined in what cases mobile devices are allowed for information processing, also what kind of devices are allowed etc.

ISF guidance

Logging

Principle - Important security-related events should be recorded in logs, stored centrally, protected against unauthorized change and analyzed on a regular basis.

- There should be documented standards / procedures for security event logging that apply to the computer installation.
- Standards / procedures should cover:
    - management of security event logging (e.g., setting policy, defining roles and responsibilities, signing off budget and reporting)
    - identification of systems on which event logging should be enabled to help

identify security-related events (e.g., critical business systems, systems that have experienced a major information security incident, or systems that are subject to legislative or regulatory mandates)
  - configuration of systems to generate security-related events (including event types such as failed log-on, system crash, deletion of user account and event attributes such as date, time, User ID, file name, IP address)
  - storage of security-related events within event logs (e.g., using local systems, central servers, or by using storage provided by a third party service provider)
  - protection of security-related event logs (e.g., via encryption, access control and back-up)
  - analysis of security-related event logs (including normalization, aggregation and correlation)
  - retention of security-related event logs (e.g., to meet legal, regulatory and business requirements for possible forensic investigations).
- Security event log management should include: setting policy; defining roles and responsibilities; ensuring the availability of relevant resources and guidance on the frequency and content of reports.
- Security event logging should be performed on systems that:
  - are critical to the organization (e.g., financial databases, servers storing medical records or key network devices)
  - have experienced a major information security incident
  - are subject to legislative or regulatory mandates.
- Host systems should be configured to:
  - enable event logging
- generate appropriate event types (e.g., system crash, object deletion and failed login attempts)
- incorporate relevant event attributes in event entries (e.g., IP address, username, time and date, protocol used, port accessed, method of connection, name of device and object name)
- use a consistent and correct system date and time (e.g., by establishing a network time server and using the network time protocol (NTP)).
- Security-related event logging should be:
  - enabled at all times
  - protected from accidental or deliberate overwriting.
- Mechanisms should be established so that when event logs reach a maximum size, the system is not halted through lack of disk space and logging continues with no disruption.
- Security-related event logs should be analyzed regularly (e.g., using automated tools), and include:
  - processing of key security-related events (e.g., using techniques such as normalization, aggregation and correlation)
  - interpreting key security-related events (e.g., identification of unusual activity)
  - responding to key security-related events (e.g., passing the relevant event log details to an information security incident management team).
- Security-related event logs should be:
  - retained according to retention standards / procedures

- copied on to removable storage media that can preserve the event log information (in electronic format) for long periods of time
- stored securely for possible forensic analysis at a later date.

Backups

Principle - back-ups of essential information and software used by the application should be performed on a regular basis, according to a defined schedule.

- Back-ups of essential information and software (e.g., business information, systems information and application information) should be performed frequently enough to meet business requirements.

Back-ups should be:

- performed using a back-up management package to strengthen the security of backed-up information
- encrypted to protect important information (e.g., in the event back-up media is stolen or is lost in transit to an alternative location, such as an off-site storage facility)
- recorded in a log (or equivalent), which includes details about backed-up data, the date and time of the back-up, and the back-up media used
- verified to ensure that backed-up software and information can be restored successfully.

Back-up arrangements should enable software and information to be restored within a critical timescale (i.e., the timescale beyond which an outage is unacceptable to the organization).

Back-ups should be protected from loss, damage and unauthorized access, by:

- storing them in a computer media fireproof safe on-site, to enable important information to be restored quickly
- keeping copies off-site, to enable the application to be restored using alternative facilities in the event of a disaster
- restricting access to authorized staff (e.g., through the use of access control software, physical locks and keys).

**For assessment**

Quantity

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| List of operations | | | | | | |
| Back-up procedure | | | | | | |
| Backup management rules | | | | | | |
| Logging procedure | | | | | | |
| Logs | | | | | | |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| management rules |  |  |  |  |  |  |

Quality

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Log user name |  |  |  |  |  |  |
| Log IP address |  |  |  |  |  |  |
| Critical systems logins and logouts |  |  |  |  |  |  |
| Log critical systems' information views |  |  |  |  |  |  |
| Log critical systems' information change |  |  |  |  |  |  |
| Log critical systems' information delete |  |  |  |  |  |  |
| Log critical systems' inquiries activation |  |  |  |  |  |  |
| Log application executions and closing |  |  |  |  |  |  |
| Log database transactions |  |  |  |  |  |  |
| Log access to the sensitive information |  |  |  |  |  |  |
| Log operations under privileged user rights |  |  |  |  |  |  |
| Log unauthorized operations and attempts |  |  |  |  |  |  |
| Log date and |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| time |  |  |  |  |  |  |
| Back-up critical systems’ data |  |  |  |  |  |  |
| Back-up frequency considering RPO (Recovery Point Objective) |  |  |  |  |  |  |
| VPN (Virtual Private Network) use |  |  |  |  |  |  |
| Mobile media protection measures – what can be copied |  |  |  |  |  |  |
| Mobile media protection measures – where can be copied |  |  |  |  |  |  |

Control

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Log files review |  |  |  |  |  |  |
| Back-up recovery testing |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Access control management**

**Description**

The policies or procedures shall be in place to regulate access to the information systems and these policies or procedures shall enfold the all phases of access lifecycle, amongst registering users, changing the access rights of users and suspending or stopping the rights in case there is no need for information services for a certain user. Access policies or procedures shall define all possible access points, amongst access to the personal computers, access to network, access to operating systems, access to the applications and databases, mobile and remote access to information assets and access of temporary and external users. Access granting and the rest of management activities should be regulated with purpose to identify information assets users with certain reliability. The employees of enterprise and its associated concerns and members of management should be identified individually (and not collectively) in connection with every change or delete of information.

Supervised entity should have effective rules for choosing and administrating passwords. The passwords connected with user accounts should be difficult enough to avoid guessing them with trial.

Password administration rules shall be co-ordinated with information assets owners, these rules shall be communicated to the employees who have access to the information assets, and password administration rules shall at least include information as following – password creation and communication procedure, password changing frequency and conditions, password keeping, user responsibilities and password keeping rules for users with special rights.

The commitment about secure use of passwords should be communicated to the users. User who was allowed access to the information system with certain password is responsible for activities inside of information systems made using this password.

The access to data and information should be limited only for persons who need this information for the job. Granting access rights should be co-ordinated with information asset owner. Current access rights shall be documented and assigned by information asset owner.

Supervised entity should establish and implement access rights control procedure. Conformity of documented and real access rights should be controlled regularly, also the conformity of user access rights with real need should be assessed regularly. The access rights formed during control, which do not have real users, shall be eliminated.

Special attention should be paid to the closing of access rights in case employee leaves the job. In case of loss of confidence by employee, the access rights to the information systems shall be closed before formal announcement about termination.

In case of employee staying away for longer, it should be determined of withdrawing the access rights for this period.

All information assets users should be identified and authorized. Considering the sensitivity of information assets, a level of user identification and authorization should be determined and adequate rules should be established.

The use of information systems and services outside of enterprise intranet should be followed closely. Before opening the services and granting corresponding access rights, the real identity and authentication of external user should be verified for using certain services and performing proper activities. Considering the nature of service, two factor authentication solutions should be considered for identifying and authorizing the users.

**Content and criteria**

Access policy

- Giving access
- Controlling access rights
- Closing access rights

Defining access points

- Data
    - Electronic Files, Databases, Access, E-Mail, etc.
    - Seems like an infinite number of possibilities
- Applications
    - Business Applications
    - Internal or COTS
- Platform
    - Linux
    - Windows
    - AIX, etc.
- Systems
    - End-to-End Review
    - Internet-based apps should include firewalls, load balancers, web servers, middle-tier, web services, databases, etc.
    - IdM and IAM
    - Use Case Scenarios
- Physical Assets
    - Data Center and Data Closets
    - Access Control Systems

RBAC - Role Based Access Control
Ideal state:

- Every privilege is included in one or more roles
- Role hierarchies are used to group roles by application, division, enterprise
- A limited number of top-level roles exist depending on organization size and/or complexity
- Each user assigned handful of top level roles that map to a single job function
- No user has exceptions

Business owners involvement:

- How many total privileges in application?
- Do roles exist or are privileges assigned individually?
- What are the classes of users?
- Can privileges be collapsed into application roles?
- Use existing people as prototypes
- Obtain executive support to encourage application managers to engage
- Keep track of privileges, roles, users, job functions
- Establish clear requirements of business owners

*Business requirement for access control - Percentage of corporate application systems for which suitable "owners" have (a) been identified, (b) formally accepted their ownership responsibilities, (c) undertaken (or commissioned) risk-based application security and access reviews, and (d) defined role-based access control rules.*
An organization's approach to RBAC is driven by:
– Regulatory requirements
– Financial and legal exposure
– Organizational maturity
– Cost
– Risk appetite
– Size and/or complexity

Rules for composing passwords:

- Primary (generated by system) password;
- Requirements for passwords – minimal length, use of capital letters, numbers and special letters.

Complexity of passwords.

Password management rules

- Creating passwords
- Inform passwords
- Password regeneration – frequency and requirements (avoid last ones, etc.)
- Keeping passwords
- The rules for giving and keeping passwords for privileged users

User demands and responsibilities in keeping passwords.

Need to know

- Who has access to which systems?

• What level of access do they have?
• Is it appropriate to their job?

- What access to critical or sensitive systems does each user have?
- Do we know which systems are critical or sensitive?
- Can we record when access to those systems has been reviewed?

Documentation of passwords means that it is stated before what kind of roles get what kind of access rights.

Procedure for controlling access rights.

Closing access rights timely.

Identification and authorization of users:

- Authentication – ensuring a user is who he says
- Authorization – controlling what information and applications a user can access

Remote access management

Two factor authentication
Existing authentication methodologies involve three basic “factors”:
• Something the user ***knows*** (e.g., password, PIN);
• Something the user ***has*** (e.g., ATM card, smart card); and
• Something the user ***is*** (e.g., biometric characteristic, such as a fingerprint).
USA:
*The FFIEC believes that single-factor authentication (the use of a username and password) is now inadequate to protect users against recent internet scams such as phishing, pharming and RAT attacks. By the end of 2006, all US online banks will be required to implement two-factor authentication, which relies on something the consumer has, such as a token or smartcard to more strongly identify the individual.*
EUR:
A number of banks within Europe have made clear their intention to implement strong (two factor) authentication to secure both online account management and financial payment card transactions for their retail and commercial customers.

*ISO 27k guidance:*
*User access management - Average delay between access change requests being raised and actioned, and number of access change requests actioned in the previous month (with trends analysis and commentary on any peaks/troughs e.g. "New Finance application implemented this month"...).*
*User responsibilities - percentage of job descriptions that include (a) fully documented and (b) formally accepted information security responsibilities.*
*Network access control - firewall statistics such as percentage of outbound packets or sessions that are blocked (e.g. attempted access to blacklisted websites; number of potential hacking attacks repelled, categorized into trivial/of some concern/critical).*
*Operating system access control - System and network vulnerability statistics such as the number of known vulnerabilities closed, open and new; average speed of patching vulnerabilities (analyzed by vendor or in-house priorities/categories).*
*Application and information access control - percentage of platforms that are fully compliant with baseline security standards (as determined by independent testing), with notes on non-compliant systems (e.g. "Finance system due to be upgraded to compliant platform in Q4").*
*Mobile computing and teleworking - “Mobile/teleworking security status” i.e. informed commentary on the current security status of mobile IT (laptops, PDAs, cellphones etc.)*

*and teleworkers (home working, mobile workforce etc.), with notes on recent/current incidents, current known security vulnerabilities and projections of any increasing risks, coverage of defined secure configurations, antivirus, personal firewalls etc.*

Documentation:

- Access rules and procedures;

Activities:

6. Identify unique products and services and access needs for external service providers;
7. Find out internal and external network connections and access points (gateways, modems etc.);

8. Ensure that access management procedures in paper correspond to the practice:
    - Particular extract of some application or system access rights;
    - Granting access right should be allowed only by authorized person using formal and signed permission. Authorized person is mostly the owner of information asset.
    - Users have to be required to change temporal passwords immediately after first log-in;
    - There has to be mechanism in place to change the original passwords immediately after new software installation;
    - To avoid passwords disclosure, it is necessary not to keep the passwords inside of information systems in plain text;
9. Find out how is organized the change of passwords in case the user changes his/her position and how is organized stopping user rights inside of information systems in case the users leave;
10. Find out the procedures how is organized access right granting to the external service providers;
11. Find out the procedures how is organized remote access and what kind of security measures are implemented (for example in case calling back is possible, there is need for hardware-based affirmation like PIN-calculator or ID-card);
12. Ensure that it is implemented the following:
    - After few unsuccessful access attempts user account locks up and access is denied (or delayed);
    - Systems have to ensure that log-ins are in accordance with user profile. In case there is no conditions for user profile, it should be supposed that anonymous user rights and remote connections are denied;
    - It should be ensured that passwords must be changed regularly (for example after each 90 days and systems should initiate changing process);
    - Deny using, for example, at least 3 older passwords;
    - Establish and control password minimum length (for example 6 symbols).
13. Ensure that new employees get necessary training and that there is so called „packet for new employees“ in place;
14. Find out how is organized training for employees;

15. Find out whether internal security trainings are organized for users.

ISF guidance:

Principle - Identity and access management arrangements should be established to provide effective and consistent user administration, identification, authentication and access mechanisms across the organization.

- IAM arrangements should be incorporated into an enterprise-wide solution, and applied to new business applications when they are introduced into the organization.
- IAM arrangements should:
  - include a method for validating user identities prior to enabling user accounts
  - keep the number of sign-ins required by users to a minimum (i.e., reduced or single sign-in).
- IAM arrangements should provide a consistent set of methods for:
  - identifying users (e.g., using unique User IDs)
  - authenticating users (e.g., using passwords, tokens or biometrics)
  - the user sign-on process
  - authorizing user access privileges
  - administering user access privileges.
- IAM arrangements should be developed to improve the integrity of user information by:
  - making the information readily available for users to validate (e.g., by using an electronic information database or directory, such as white pages)
  - allowing users to correct their own user information (e.g., by providing users with a self-service application)
  - maintaining a limited number of identity stores (i.e., the location where User ID and authentication information is stored, such as a database, X500 / Lightweight Directory Access Protocol (LDAP) directory service, or commercial IAM product)
  - using an automated provisioning system (whereby user accounts are created for all target systems, following the creation of an initial entry for a user in a central IAM application)
  - using a centralized change management system.
- IAM arrangements should enable:
  - access rights to be quickly and easily granted, changed or removed for a large number of users (e.g., by deploying role-based access rights)
  - management of user access privileges to be performed by relevant system owners (i.e., rather than by system administrators / IT staff).

**For assessment**

Quantity

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Access | | | | | | |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| policy |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Quality

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Access to the PC |  |  |  |  |  |  |
| Access to the network |  |  |  |  |  |  |
| Access to operating systems |  |  |  |  |  |  |
| Access to the applications |  |  |  |  |  |  |
| Access to the databases |  |  |  |  |  |  |
| Mobile access |  |  |  |  |  |  |
| Remote access |  |  |  |  |  |  |
| Access of temporary users |  |  |  |  |  |  |
| Access of external users |  |  |  |  |  |  |
| Complexity of passwords |  |  |  |  |  |  |
| User responsibilities |  |  |  |  |  |  |
| Need to know |  |  |  |  |  |  |
| Closing rights timely |  |  |  |  |  |  |
| Identification |  |  |  |  |  |  |
| Authorization |  |  |  |  |  |  |
| Two factor authentication |  |  |  |  |  |  |

Control

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Access rights compliance with rules |  |  |  |  |  |  |
| Access rights |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| necessity |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Information systems security**

**Description**

Security requirements and adequate controls for information systems should be established by information assets owners or in co-operation with them. The information asset owner ensures integrity and availability of data desired by financial supervisors or investigators.

In developing, complementing and changing information systems, it should be ensured that information systems process information as supposed. Input and output controls should contribute data quality.

To reduce the presumptions of conflicts with legal acts in connection with changes in information systems, by planning changes and considering its purpose, conformity with legal acts should be assured.

In case of consequences or possible consequences of information systems change, if manipulation with information integrity or availability, requested by financial supervisors or investigators acts or proceedings, comparing with period before obtaining an act or performing a proceeding occurs, supervised entity should apply to financial supervisors or investigators motivated explanation about the change and description of legal protection instruments for information asset owner or other activities.

Considering the real need and information sensitivity to begin with ensuring confidentiality and integrity, encryption should be used. Supervised entity should establish the rules for use of encryption and these rules should determine the cases where encryption is obligatory. Also it should be agreed the cryptographic algorithm used, the minimum length of cryptographic keys and administration of cryptographic keys.

The rules for identifying, testing and applying the software updates should be established to avoid problems arisen from software defects. The responsibility about administration of software updates should be assigned for each separate software system.

Supervised entities should determine and establish time period for maintaining information assets considering the requirements of legal acts, deadlines for out of date and financial supervisors’ possible interest in information.

Supervised entities should ensure that business information (both composed and/or processed) will be saved immediately to hardware owned or used by enterprise also in case the employees of enterprise and members of management compose or process pointed business information outside of hardware owned or used by enterprise (for example, personal computer, personal outsourced e-mail account etc.).

**Content and criteria**

Information systems security needs

Why do businesses need to spend time, money and resources on additional testing measures to check the security of their applications?

- External compliance requirement – for example PCI (payment card industry standard)
- Internal compliance requirement – corporate data privacy standards
- Mission critical applications – applications that drive your business
- Critical data in applications – cardholder data, personal information
- Company's brand is important – defacements and hijacks repel current and future customers

*ISO 27k guidance:*

*Security requirements of information systems - percentage of corporate application systems for which suitable "owners" have (a) been identified, (b) formally accepted their ownership responsibilities, (c) undertaken (or commissioned) risk-based application security and access reviews, and (d) defined role-based access control rules.*

Information processing rules in information system

Testing methods:

- Static Analysis - execution path analysis
  - Typically thorough source code analysis
  - Testing without actual data
  - Analyze all possible execution branches of code
- Dynamic Analysis - data-driven analysis
  - Typically thorough black-box testing tools
  - Testing with pre-defined test data sets
  - Analyze behavior when different data sets are used

Data quality controls

*Correct processing in applications - Percentage of systems for which data validation controls have been adequately (a) defined; and (b) implemented and proven effective by thorough testing*

Rules for using cryptography

Obligation for encryption – certainly should be considered in keeping passwords in system, also in exchanging confidential information.

Encryption algorithm – use some recognized or standardized algorithm. Keeping algorithm itself in secret is not obligatory and it is not risky publishing it.

Secret key cryptography is still the most widely used of the encryption techniques and is still preferred when large number of data is to be encrypted. One key for both encrypting and decrypting (inverse process). Provides confidentiality and is fast (computationally). Key distribution and management problems. Recognized encryption algorithms are:

- AES
- DES
- Triple-DES
- IDEA
- RC2
- Blowfish
- RC4

Public key cryptography - two mathematically related keys (public-private key pair) - one encrypts while the other decrypts. Provides Authentication and non-repudiation in addition to Confidentiality and Integrity. Slow (computationally intense). Public key can be easily and safely distributed widely while private key is NOT distributed. Algorithms:

- RSA
- Diffie-Hellman
- DSA
- Elliptic Curve
- MultiPrime

PKIs rely on certificates

- Certificates are digitally signed (using public key cryptography) data by a trusted source
- Trusted sources are usually Certificate Authorities (CAs) that sign certificates for end users, applications, or other CAs

Different certificates are issued to different entities

- User certificates
  - Email
  - Encryption
  - Signing
- Web server / SSL
- IPsec certificates
- Coding signing

Encryption keys – the length of encryption key should be sufficient to ensure information security. In deciding encryption key length, a future perspective should also be considered and there has to be a process to periodically control the sufficiency of key length.

Today's sufficient key lengths could be for example:

- Symmetric – 128 bits
- Asymmetric (RSA) – 1024 bits

Management of encryption keys

Special attention needs encryption keys maintaining and management. Among other things, in encryption keys management procedures the difference of public and private keys should be made in case the PKI – Public Key Infrastructure is used. The whole lifecycle of encryption keys is to be considered in key management.

Typically, key management is tied directly to products and tends to exacerbate the

problem of systems as follows:
– Email
– Laptop / mobile device encryption
– VPN / IPsec
- Data backups
- Databases

Key management is the set of activities associated with the handling of cryptographic key material – from the initial key generation, thorough distribution, to the ultimate destruction of the key

– Generation – The creation of keys (of any type) according to the mathematical structure tied to the algorithm under which the key will be used, or the standards that the enterprise wishes to enforce;
– Distribution – The process of delivering the generated key to its intended recipient and the process for assurance that the recipient is the correct and that the key was delivered unaltered;
– Backup / Archive / Escrow – Creating and managing a copy, or other recoverable form of the key that may occur in different periods of the key lifecycle;
– Storage – The processes surrounding the protection of keys and key stores;
– Update / Renewal – The re-validation of a key thorough key derivation (for an existing key) or replacement;
– Recovery – Retrieving a key from the backup / archive / escrow process;
– Expiration – The process to enforce a limited key lifetime after which an update, renewal, or disposal event will occur;
– Revocation – Invalidating (removing) a key from use, typically before the end of its lifetime;
- Disposal – The permanent removal of a key (from the user and any back up or archive) and all traces of its use, e.g., any material encrypted under that key.

*Cryptographic controls - percentage of systems containing valuable/sensitive data for which suitable cryptographic controls have been fully implemented (3- to 12-monthly reporting period).*

The rules for change management in information systems
Roll-back procedures
Validation
Two types of patches:

- Security patches
- General updates

*Security of system files - Percentage of systems independently assessed as fully compliant with approved baseline security standards vs. those that have not been assessed, are not compliant, or for which no approved baseline exists.*
*Security in development and support processes - "Developing systems security status" i.e., informed commentary on the current security status of the software development processes, with notes on recent/current incidents, current known security vulnerabilities and projections of any increasing risks etc.*

*Technical vulnerability management - Patch latency i.e., deployment half-life (time taken to patch half the vulnerable population of systems - avoids seemingly random changes due to a few very late systems such as portables out in the field or in store).*

*ISO 27k guidance:*
*Operational procedures and responsibilities - security-related IT process maturity metrics such as the "half-life" for applying security patches (the time taken to update at least half the population of vulnerable systems - this measure helps avoid the variable tail caused by the inevitable few systems that remain unpatched because they are not in daily use, are normally out of the office or whatever).*

ISF guidance

Cryptographic solutions

Principle Cryptographic solutions should be approved, documented and applied enterprise-wide.

Cryptography should be used across the organization to:

- protect the confidentiality of sensitive information (e.g., by using encryption)
- determine if critical information has been altered (e.g., by performing hash functions)
- provide strong authentication for users of applications and systems (e.g., by using digital certificates and smartcards)
- enable the identity of the originator of critical information to be proven (e.g., by using digital signatures for non-repudiation).

There should be documented standards / procedures for the use of cryptography across the organization, which cover the:

- definition of circumstances where cryptography should be used (e.g., for high-value transactions involving
- external bodies or transmitting confidential information across open networks such as the Internet)
- selection of approved cryptographic algorithms (e.g., Advanced Encryption Standard (AES) for confidentiality, and SHA-1 or MD5 for integrity)
- management (including protection) of cryptographic keys
- restrictions on the export / use of cryptographic solutions
- suitability of cryptographic solutions employed (including algorithms and encryption key lengths).

Responsibilities should be clearly defined for managing cryptographic keys and dealing with licensing issues associated with the use of cryptographic solutions internationally.

Relevant business managers should have access to:

- expert technical and legal advice on the use of cryptography
- a list of approved cryptographic solutions
- an up-to-date inventory (or equivalent) detailing where cryptographic solutions are applied within the organization.

Cryptographic key management

Principle Cryptographic keys should be managed tightly, in accordance with documented standards /procedures, and protected against unauthorized access or destruction.

- There should be documented standards / procedures for managing cryptographic keys, which cover:
  - generation of cryptographic keys, using approved key lengths
  - secure distribution, storage, recovery and replacement / update of cryptographic keys
  - revocation of cryptographic keys (e.g., if a key is compromised, or a key owner changes job or leaves the organization)
  - recovery of cryptographic keys that are lost, corrupted or have expired
  - management of cryptographic keys that may have been compromised, such as by disclosure to a third party
  - back-up / archive of cryptographic keys and the maintenance of cryptographic key history
  - allocation of defined activation / de-activation dates
  - restriction of access to cryptographic keys to authorized individuals
  - sharing of cryptographic keys (e.g., using split key generation) required for protecting sensitive information and critical systems.

Individuals who clearly understand their responsibilities should be assigned to manage cryptographic keys.

Cryptographic keys should be protected against:

- unauthorized access
- destruction.

**For assessment**

Quantity

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| IS security requirements | | | | | | |
| | | | | | | |
| | | | | | | |

Quality

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Business side involvement in establishing security needs | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Presence of systematic security controls | | | | | | |
| Obligations for information encryption | | | | | | |
| Recognized encryption algorithm | | | | | | |
| Minimum key length | | | | | | |
| Encryption keys management procedure | | | | | | |

Control

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| IS security controls | | | | | | |
| | | | | | | |
| | | | | | | |

**Information security incident management**

**Description**

In case of information security breaches, it should be assured that immediate communication, registration, incident verification by competent employee and implementation of countermeasures follow.

In addition to the requirements for incident management, which are covered by the advisory guidelines of the Financial Supervision Authority “Requirements for the organization of the field of information technology”, established 22.09.2004 with management decision 44-4, section 18 “Problem and incident management”, in resolving information security incidents it should be considered that information collected during the incident is maintained in a way, that during further investigation it is possible establish what happened and it is possible to ensure that information used for making conclusions is not changed between incident occurrence and incident solution.

Internal procedures should ensure that for each detected and reported information security incident, a responsible person will be assigned and his/her main purpose is to co-ordinate incident solving during incident is open. Also the procedures should include description of potential escalation of incidents. Detailed requirements for resolving business continuity incidents according to the business continuity plan are covered by the advisory guidelines of the Financial Supervision Authority “Requirements for Organizing the Business Continuity Process of Supervised Entities”, established 06.12.2006 with management decision no 96.

Already occurred information security incidents should be analyzed to find out the reasons, ascertain deficiencies and work out the measures to eliminate deficiencies with intention to avoid similar incidents occurrence in the future. Also, the further analysis of incidents helps to find out what kind of knowledge and skills need to be expanded for employees and clients to avoid similar incidents and improve management of incident solving in the future.

**Content and criteria**

Respond to the security incident:

- informing
- registering
- verifying
- measures

Preserve information during incident, for example, 10 actions are highlighted which should not be taken on case of security incident:

1. No plan before incident happens;
2. Estimation of situation and background is insufficient;
3. Confuse *master* and *slave* hard drives;
4. Sterile media not used;
5. Insufficient documentation;
6. Incomplete chain of happenings;
7. Asking help too late or no asking;
8. Use of unlicensed software;
9. Using of experts with distorted expertise or experience;
10. Expert is taking a snapshot about own computer.

Preservation of Evidence - for evidence to be admissible, you must prove that it was not tampered:

- Disconnect the system from the network, but do not shut it down
- Don’t open log files
- Don’t use the system (if possible)

Responsible persons for solving sort of incident should be appointed.
The rules for incident escalation should be described. For example, scale could be trivial

– serious – critical and how to reach next level should be described.

The analysis of incidents should follow and additional security measures should be taken.

*ISO 27k guidance:*

*Reporting information security events and weaknesses - IT Help/Service Desk statistics with some analysis of the number and types of calls relating to information security (e.g., password changes; queries about information security risks and controls as a Percentage of all queries). From the status, create and publish a league table of departments (adjusted for number of employees per department), showing those that are clearly security-conscious vs. those that are evidently asleep at the wheel.*

*Management of information security incidents and improvements - Number and gravity of breaches, if not some assessment of their costs to analyze, stop and repair the breaches and any tangible and intangible losses incurred. Percentage of security incidents that caused costs above acceptable thresholds defined by management.*

Documentation:

- Extract from security incident register;

ISF guidance

Principle Information security incidents should be identified, responded to, recovered from, and followed up using an information security incident management process.

- o A capability for governing the management of information security incidents (i.e., event (or chains of events) that compromise the confidentiality, integrity or availability of information) should be established.

The information security incident management capability should be supported by documented standards /procedures, which:

- o cover the involvement of relevant stakeholders (e.g., legal department, public relations, human resources, law enforcement agencies, media and industry regulators)
- o detail the types of information needed to support information security incident management (e.g., security event log data, network configuration diagrams and information classification details)
- o specify the tools needed to support information security incident management (e.g., checklists, forms and templates, log analyzers, incident tracking software and forensic analysis software).

Standards / procedures for information security incident management should be:

- o approved by top management (board-level executives or equivalent)
- o reviewed regularly
- o kept up-to-date.

There should be a process for managing individual information security incidents, which includes:

- identifying information security incidents (e.g., receiving information security incident reports, assessment of business impact, categorization and classification of the information security incident, and recording of information about the information security incident)
- responding to information security incidents (e.g., escalation to the information security incident management team, investigation, containment and eradication of the cause of the information security incident)
- recovering from information security incidents (e.g., rebuilding systems and restoring data, and closure of the information security incident)
- following up information security incidents (e.g., post-incident activities such as root cause analysis, forensic investigation, and reporting to the business).

There should be a defined individual / team responsible for managing information security incidents, which have:

- defined roles and responsibilities
- sufficient skills / experience in managing information security incidents
- authority to make critical business decisions
- methods of involving internal and external stakeholders (e.g., legal department, public relations, human resources, law enforcement agencies, media and industry regulators).

Information relevant to managing information security incidents (e.g., network diagrams, event logs, business processes, and security audit reports) should be made available to help staff follow, and make important decisions during, the information security incident management process.

Individuals responsible for managing information security incidents should be supported by tools (e.g., software for security information management, evidence handling, back-up and recovery, and forensic investigation) to help complete each stage of the information security incident management process.

**For assessment**

Quantity

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Procedure for handling security incidents | | | | | | |
| | | | | | | |
| | | | | | | |

Quality

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| Incident recognizing | | | | | | |
| Incident verification | | | | | | |
| Incident registration | | | | | | |
| Incident information maintenance | | | | | | |
| Appointment of incident owner | | | | | | |
| Analysis on incidents | | | | | | |

Control

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Incident reporting | | | | | | |
| | | | | | | |
| | | | | | | |

**Information systems audit considerations**

**Description**

In addition to the requirements covered by the advisory guidelines of the Financial Supervision Authority “Requirements for the organization of the field of information technology”, established 22.09.2004 with management decision 44-4, section 21 “Monitoring and assessment”, attention should be paid to information security auditing. In planning information technology and information security activities, efficient assistance for performing supervision activities should be ensured to supervision authority. In planning internal audits, the activities in connection with information security should be also considered.

Compliance of information security requirements should be constantly assessed, if necessary, consultation by experts should be used and for assessment compliance with security requirements, an independent control function should be established.

The need for information security audits should be find out during risk analysis. As a result of risk analysis, the most critical areas appear about auditing should be considered.

The main purpose of information security audits should be independently assess whether enterprise conforms to internal and external information security requirements.

In planning information security auditing, the audit function, auditing procedures, audit plan, particular activities by auditor and the duties of employees in connection with audit should be confirmed.

In case the audit need is ascertained and adequate know-how is missing inside of enterprise, it should be considered to outsource auditing services. In outsourcing auditing services, outsourcing partner's competences and experiences in organizing similar audits should be assessed and the extra attention should be paid to outsourcing partner's obligations in maintaining and protecting the confidential information recorded during audit. Detailed requirements for outsourcing are covered by the advisory guidelines of the Financial Supervision Authority "Outsourcing Requirements for Supervised Entities", established 25.10.2006 with management decision no 1.1-7/84.

Audit findings and observations should be considered in managing and planning enterprise's information security activities. In case there are found critical deficiencies, a sequel audit should follow.

To find out possible weaknesses of critical information systems, a penetration testing as alternative to thorough audits should be considered. In performing penetration tests, it should be ensured that normal work is not disturbed and information is not corrupted.

**Content and criteria**

Determine what to audit

- Focus on areas of the highest risk
- Create the IT audit universe
    - Centralized IT functions
    - Decentralized IT functions
    - Business applications
    - Regulatory compliance
    - COBIT
- Rank the universe
    - Known internal control issues in the area
    - Inherent risk in the area
    - Benefits of performing an audit in the area
    - Quantity of assets represented by the area
    - Results of previous audits
    - Rotation schedule
    - Management input

Application controls audit:

- new implementation
- application upgrade

        - periodic certification and audits

Control:

- A process designed to provide reasonable assurance on:
    - Effectiveness and efficiency of operations
    - Reliability of financial reporting
    - Compliance with applicable laws and regulations
- Can be preventive or detective
- Can be manual or automated

Monitor how the security requirements are realized

Advantages of Information Security:

- Ability to intervene in projects before completion to ensure controls are implemented
- Often works within the IT department and is able to get a pulse on new projects and initiatives and their impact on risk
- Has reporting responsibilities to executive management

Risk analysis and compliance control

- enhance the sustainability of IT compliance programs
- move beyond traditional compliance objectives and look at operational performance
- IT compliance program supports overall IT operational maturity
- various strategies can be employed to enhance sustainability
- prioritize the anticipated value add and ease of implementation
- regular monitoring of a balanced set of metrics

The procedure of conducting audits

- Determining what to audit
- Planning
- Fieldwork and documentation
- Issue discovery and validation
- Solution development
- Report drafting and issuance
- Issue tracking

Audit effectiveness:

- Design vs. operating effectiveness
- Indicators of weakness
- Compensating controls
- Super users
- Testing with IT general controls
- Common mistakes
- Using CAATS
- Audit automation software

Procurement of information security audits

Decide profile of auditor regarding audit task:

- Career IT Auditors
  - Strong foundation in control and audit theory
  - Lack of operations experience can impact depth of analysis
  - Important to find those with technical knowledge beyond basic general controls
- IT Professionals
  - Positive impact on depth of reviews and credibility
  - Often struggle to develop risk assessment and process analysis skills
  - Important to find those who can learn new things quickly and have strong communication skills

Take the audit results into account.

The role of information security

- Conducts risk assessments
- Develops policy to address risk
- Sells policy to senior management
- Evaluates new products and systems
- Serves as a consultant to various project managers
- Negotiates contracts with vendors to make sure security concerns are met

The need for post-audit.

Penetration testing

Negative testing:

- How does the application behave in adversity?
- Test the application against known possible attacks
- Attack vectors such as hacking, DDoS, and more
- Intentional miss-use
- Test against malicious use-cases
- Testers must have a library of known attack data
- Unintended functionality
- Test for unintended functionality in the application
- Test for logic flaws, race conditions, others

*ISO 27k guidance:*

*Number of audit issues or recommendations grouped and analyzed by status (closed, open, new, overdue) and significance or risk level (high, medium or low).*

*Percentage of information security-related audit findings that have been resolved and closed vs. those opened in the same period.*

*Mean actual resolution/closure time for recommendations relative to the dates agreed by management on completion of audits*

Documentation:

- Information security audit reports.

ISF guidance

Principle The information security status of critical IT environments should be subject to thorough, independent and regular security audits / reviews.
Independent security audits / reviews should be performed regularly for environments that are critical to the success of the organization, including:

- business applications
- computer installations and networks
- systems development activities
- key enterprise-wide security activities (e.g., managing a security architecture, running awareness programs or monitoring information security arrangements)
- end user environments (e.g., a claims processing department, sales and marketing office, research and development operation, manufacturing plant or call center).

Security audits / reviews should be:

- agreed with the owner of the environments under review
- performed by individuals who are equipped with sufficient technical skills and knowledge of information security
- conducted thoroughly (in terms of scope and extent) to provide assurance that security controls function as required
- focused on ensuring that controls are effective enough to reduce risk to an acceptable level
- supplemented by the use of automated software tools
- validated by competent individuals
- complemented by reviews carried out by independent third parties.

Security audit / review activity should be managed by:

- agreeing requirements for special processing routines or tests (e.g., penetration testing) with the owners of the environments under review
- restricting access to systems by audit / review teams
- monitoring and logging the activities of audit / review teams
- disposing of business information copied for the purpose of audits / reviews as soon as it is no longer required
- protecting software tools used in carrying out audits / reviews (e.g., by keeping them separate from tools /utilities used in the live environment, and holding them in secure storage facilities, such as restricted software libraries).

Recommendations following security audits / reviews should be agreed with the owners of environments under review and reported to top management.

**For assessment**

Quantity

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Audit procedure | | | | | | |
| Requirements for external auditor | | | | | | |
| | | | | | | |

Quality

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Investigation the need for audits | | | | | | |
| Security requirements monitoring | | | | | | |
| Compliance assessment | | | | | | |
| The use of audit results for improvements | | | | | | |

Control

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Post-audits | | | | | | |
| | | | | | | |
| | | | | | | |

Business continuity

The business continuity part consists of five sub-parts: business continuity process, preparation of business continuity plans, the content of business continuity planning, communication and business continuity testing. Each sub-part contains definition, description, content and criteria and format for assessment.

**Business continuity process**

**Description**

Business continuity management should be treated as an integral part of a supervised entity's risk management program, while the management policies, standards and processes should be implemented throughout the organization.

The management board ensures that the entity's business continuity process is functioning and has the role of ensuring that the supervised entity has updated and adequate business continuity plans for its critical business processes.

The management board of a supervised entity is to allocate sufficient resources and appoint competent staff for the development of business continuity plans. The person appointed to manage the business continuity process should be supplied with sufficient powers to perform his or her obligations. It is advisable that the management board set up a relevant committee, which is led by the person responsible for business continuity and which organizes all the activities pertaining to business continuity.

A clear framework (policies, procedures, etc.) should be created for the preparation of business continuity plans, their later administration, testing, and staff training, which supplies the management board and supervisory board of the supervised entity with regular reporting on the business continuity process, covering amongst other things the implementation status, incident reports, test results, and activity plans prepared on their basis.

The management board of a supervised entity should review and approve the business continuity plans and their testing results regularly, at least once a year.

The management board of a supervised entity is responsible for training the staff and ensuring that they are aware of their roles in the business continuity process and plans.

**Content and criteria**

Risk management program

Business continuity process

Critical business processes

Resources

Business continuity committee

Responsible person for business continuity

Business continuity framework

Regular review

Roles in the business continuity process

Documentation:

- A list of implementing employees (persons dealing with business continuity issues);
- Organization chart;

Activities:

1. Ensure that business continuity plans in general conform to relevant standards and legal acts and ensure that business continuity plans are adequate and up to date.
2. Ensure that business continuity plans are usable in reviewing tests results initiated by IT employees and end users;
3. Assess the appropriateness of offsite location in reviewing facilities, inside and controls of security including environmental;
4. Ensure that IT staff and users are able to react to emergency situations in reviewing procedures of emergency situations and employees training and awareness including emergency simulations;

**For assessment**

Quantity

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| List of critical business processes | X | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Risk management program | | | | | | |
| | | | | | | |

Quality

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Business continuity process | | | | | | |
| Steering committee | | | | | | |
| Responsibilities | | | | | | |
| Roles | | | | | | |
| Resources | | | | | | |
| BC framework | | | | | | |

Control

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Regular review | | | | | | |
| | | | | | | |
| | | | | | | |

**Preparation of business continuity plans**

**Description**

The process of business continuity planning should cover the entire entity. The supervised entities' goal of business continuity planning should ensure business continuity in the event of extraordinary disruptions and recover business and IT systems after such disruptions.

A major disruption of the business of one participant in the financial system may influence the ability of its customers and other participants in the financial market – possibly also of the financial system – to continue normal business operations.
This is why supervised entities should assess, in the course of risk analysis, the scope of the potential risk they can cause to the entire financial system. The scope of business continuity plans should correspond to the nature, scope, and complicacy of the entity's business.

An effective business continuity plan is based on thorough business impact and risk analyses. Business continuity planning begins with defining a supervised entity's critical business processes. Since the availability of the resources needed for complete recovery of the business may be limited, a supervised entity should use business impact analysis to identify the business functions and activities to be recovered in the first order. Both business and IT staff should be involved in the process of a successful business impact analysis.

To recover its critical business functions, a supervised entity should set appropriate recovery goals (e.g., scope, time) for major business disruptions, which would be proportional to the entity's impact on its customers' activities and the functioning of the entire financial system.

The management board of a supervised entity should approve the critical business processes and their priorities, which have been identified as a result of the business impact analysis, as well as the recovery goals.

Supervised entities should conduct a risk analysis to assess the potential risks and their impact on processes and systems. Potential event scenarios may be classified as follows:
- information system problems;
- physical breakdowns (buildings, equipment, etc.);
- loss of human resources;
- the above scenarios in conjunction.

A risk analysis should be conducted periodically at least once per year and upon major changes in the supervised entity's business (major organizational changes, launch of new products, emergence of new customer segments, introduction of new information technology solutions, etc.).

In order to handle business disruptions, alternative operating models and recovery procedures should be prepared for the prioritized business processes, and it should be ensured that the critical information required for business recovery can be restored and renewed.

Based on the priorities set in the business impact analysis and the required recovery times, priorities should be identified for IT systems and applications, and their mutual dependencies and resource needs defined. Appropriate IT solutions should be used which ensure compliance with the time criteria defined in the business impact and risk analyses. IT system recovery plans should be prepared to describe how the various IT systems can be re-launched after a disruption.

The larger the scope of business and risk level of the supervised entity and the entity's impact on the financial system as a whole, the greater the amount of attention the supervised entity needs to pay to a potential alternative location. The alternative location should be far enough from the main location and should not depend on the same infrastructure components (e.g., power supply, communication channels) as the main location. An entity should keep in mind that the alternative location should have sufficient updated data and the necessary equipment, systems and alternative workstations in order to recover and administer critical processes and services during sufficient time in case the main location is damaged or access to it is limited.

Since the staff of the main location may be unavailable, the business continuity plan should define how the entity intends to supply (substitute) staff, which is adequate in terms of numbers and experience/knowledge to ensure the recovery of critical processes and services during the time specified in the recovery goals. Where necessary, the logistical movement of the existing staff from the main to the alternative location should be covered.

Security requirements (physical and data security) should not be overlooked when planning recovery operations.

**Content and criteria**

Business major disruptions

Critical business processes

Risk analysis – certainly for critical business processes.

Recovery goals:

- Recovery point objective:
- Recovery time objective: the maximum time
- Maximum tolerable outage:

Recovery procedures
1. recovery priorities

Recovery resource needs

Alternative location:

- Cold site
- Warm site
- Hot site

Substitute staff.

Documentation:

- Policies in connection with business continuity and disaster recovery;
- Business continuity plan, disaster recovery plan, business impact analysis, business risk analysis;

**For assessment**

Quantity

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

Quality

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| Major business disruption | | | | | | |
| RPO – recovery point objective | | | | | | |
| RTO – recovery time objective | | | | | | |
| MTO – maximum tolerable outage | | | | | | |
| Recovery priorities | | | | | | |
| Recovery resources | | | | | | |
| Substitute staff | | | | | | |
| Hot site | | | | | | |
| Warm site | | | | | | |
| Gold site | | | | | | |

Control

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

**The content of business continuity planning**

**Description**

The business continuity plan of a supervised entity should contain at least the following components:

- Emergency procedures to ensure the safety of all employees;
- An information services function, the roles and responsibilities of recovery service suppliers, service users, and administrative support staff;
- A list of system resources that require alternatives (hardware, peripheral equipment, software, etc.);
- A list of applications, beginning with the higher priorities, required recovery times and expected performance standards;
- Sufficiently detailed recovery scenarios for step-by-step implementation, beginning with minor and ending with greater losses, and the corresponding responses;
- delimitation of special equipment and supplies (e.g., communication equipment, telephone, etc.) with the defined source and alternative source;
- the existence and announcement of and training in individual and collective roles;
- schedule for testing, last test results, and additional measures taken based on previous test results;
- a list of contractual service provides, services, and expected responses;
- logistical information on the location of important resources, including the alternative location of necessary contracts, customer files, operating systems, applications, data files, operating instructions, and program, system and user documentation;
- logistical information for transporting important resources, including employees, from the main building to the alternative location;
- updated information on key employees – names, addresses, and all telephone numbers;
- alternatives for re-launching business operations (e.g., if the system has been restored at the alternative location, but the user workstations have been completely destroyed).

The regular backup copies of the electronic data of a supervised entity should be stored at a sufficient distance from the main IT center so as to ensure that the data and the backup copies are not destroyed simultaneously.

Where the supervised entity requires non-electronic data (e.g., hardcopy contracts, etc.) to conduct critical business processes, such backup copies should be stored at a sufficient distance from the main location of data and they should be available at the alternative location.

If the supervised entities outsource recovery services to a third party (e.g., an external service provider), the service provider and extent to which the services cover the entity’s needs should be thoroughly assessed using objective sources of information. Where the supervised entities are too superficial in assessing the recovery service and rely mainly on the supplier’s information, this may lead to solutions that might not adequately cover the entity’s needs as they arise.

The business continuity plans of supervised entities should clearly specify liabilities and powers of action.

### Content and criteria

Emergency procedures

Information services function

System resources

Applications with priorities

Recovery scenarios

Special equipment and supplies

Roles

Contractual service provides

Logistical information

Key employees
Particularly critical is to ensure that outside working hours people working in key positions would be available. This may also be used to pay additional fees for so-called preparedness.

Alternatives

Analysis of business continuity plan:

1. Ensure that business continuity planning process bases on the reliable and steady philosophy and framework;
2. Test particular copies of business continuity plan to find out these are up to date;

3. Ensure that critical applications and services are identified, priorities are determined and support to them is planned;
4. Analyze the contact lists of employees connected with business continuity, hot-site contacts and contacts of important purveyors to find out that information is applicable, integrity is ensured and contacts are up to date;
5. Ensure that formal contracts with purveyors are agreed to get services in case of need for recovery (including offsite locations);
6. Ensure that names, telephone numbers and addresses inside of contact list are correct and these persons have an effective copy of business continuity plan;
7. By interviewing responsible persons ensure that they understand their duties and responsibilities in case of emergency situations;
8. Assess the procedures of testing business continuity and documenting the results;
9. Assess the procedures of updating business continuity plans. Ensure that updating is regular and administration of business continuity plans is documented.

Content of business continuity plans:

- Emergency procedures to assure the safety for all employees;
- The function of information services, roles and responsibilities of purveyors supporting recovery actions, service consumers and administrative stuff;
- recovery framework in connection with continuity perspective;
- The list of resources (hardware, software, external facilities) which need alternatives;
- List of applications starting with highest priority, required recovery times and expected norms for execution;
- Administrative functions for recovery situations with assisting services and declarations (subsidies, compensations, communication and calculation of expenses);
- Recovery scenarios for step-by-step performing starting with single activities until complete recovery and relevant reactions;
- Possible special appliances need (for example, communication devices, phones etc.) and sources (alternative sources);
- Knowledge about individual and collective roles, awareness training;
- Continuity testing schedule, the results of last tests and corrective measures taken based on testing results;
- Details about contractual services with external service providers and expected results;
- Purvey information and location (backup location) of critical resources like operation systems, applications, data files, exploitation manuals and documentation of programs, systems and user manuals;
- Current information about key employees names, addresses and phone numbers;
- Plans for reconstruction of primary location in case of emergency;
- Working activity starting alternatives for all employees and alternative working places (IT resources are recovered in secondary location).

**For assessment**

Quantity

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Business continuity plan | | | | | | |
| | | | | | | |
| | | | | | | |

Quality

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Emergency procedures | | | | | | |
| Information services function | | | | | | |
| System resources | | | | | | |
| Applications with priorities | | | | | | |
| Recovery scenarios | | | | | | |
| Special equipment and supplies | | | | | | |
| Roles | | | | | | |
| Contractual service provides | | | | | | |
| Logistical information | | | | | | |
| Key employees | | | | | | |
| Alternatives | | | | | | |

Control

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Communication**

**Description**

Supervised entities should include in their business continuity plans the communication procedures for internal communication and external communication with key parties. Communication plans should cover informing the various interest groups (employees, suppliers, business partners, customers) of the crisis situation (in the business continuity context) and the recovery status. The Financial Supervision Authority has to be informed, as one of the parties, using the general contact details.

A supervised entity's communication procedures (crisis communication) should:
- identify the person responsible for communication with the staff and external parties;
- identify the potential problems that may arise during major disruptions, e.g., how to behave if the primary communication systems break down;
- be regularly updated and periodically tested.

To avoid any potential risk to their reputation, a supervised entity shall give timely and sufficient information to the public. Standard press releases may be prepared to simplify the dissemination of primary information.

Supervised entities are required to inform the Financial Supervision Authority of major business disruptions at the earliest opportunity. Not later than within three working days after solving the problem, a description of the event should be submitted to the Financial Supervision Authority using the general contact details and specifying:
- the time of the disruption;
- the scope and impact of the disruption;
- a description of how the disruption was treated;
- the reason for the disruption;
- measures to be taken to avoid similar events in the future.

**Content and criteria**

Communication procedures
Internal communication
External communication
Crisis communication

Press releases

Major business disruption
To satisfy that criterion, supervision must observe if supervised entities inform about business disruptions and compare it with the feedback by customers or by press.
The purpose of that requirement and criteria to meet the requirement is to ensure that both supervision authority and supervised entity have exactly the same information in communicating with press or with customers. Having the same information prevents misunderstanding and additional confusion.

Description of the event

After localization and/or conclusion with incident, an analysis of incident causes should follow.
Development and implementation of measures to be taken to avoid similar events in the future has to be with high priority.

**For assessment**

Quantity

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Communication procedures | | | | | | |
| | | | | | | |
| | | | | | | |

Quality

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| | | | | | | |
| Required informing 1 h | X | X | | | X | |
| Required informing 8 h | | | X | X | | X |

Control

| Criteria | BB | SB | BI | SI | IF | FM |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Business continuity testing**

**Description**

The relevance and adequacy of supervised entities' business continuity plans can be determined only by way of testing or actual implementation. Supervised entities should test their business continuity plans to be certain of their ability to restore the business processes during the specified time, while identifying any shortcomings in the plans.

Business continuity plans should be tested regularly. The scope and frequency of testing should be determined depending on the criticality of the business functions, the entity's role on the wider market, and significant changes in the entity's business or external environment.

The staff's awareness and understanding of their roles and responsibilities is important for ensuring the business's continuity and recovering the business processes of a supervised entity. Business continuity plans should be tested with the involvement of the staff whose duty it is to act in the event of major disruptions.

By virtue of paragraph 4 of these guidelines, according to which business continuity management is an integral part of a supervised entity's risk management program, a document on the time schedule of the planned tests should be submitted to the Financial Supervision Authority once per year and the Authority should be informed of the main results of the test after the test results have been analyzed. The testing schedule should be submitted at least one month before the tests and test results should be submitted not later than one month after the test. The document should contain at least the following information:

- the name of the supervised entity to conduct the test;
- the time of testing;
- the reason for testing (scheduled or non-scheduled, with reasoning);

- scope of testing (organization covered, processes covered, etc.);
- expected/achieved results along with conclusions.

The results of completed tests should be duly documented and contain at least the following information: the purpose, scope, and time of the test, resources involved, the performer and results of the tests.

The test results should be analyzed and, based on the analysis results, changes should be made in the supervised entity's business continuity and recovery plans.

Any changes in a supervised entity's processes, staff, and resources, should be reflected in the business continuity plan. Reflecting changes in the business continuity plan should be a mandatory part of the entity's change administration process. Changes are reflected in the business continuity plan together with the conduct of the risk analysis.

Internal or external audit of a supervised entity's business continuity plan should be conducted regularly.

A supervised entity's business continuity plan should be reviewed and, as necessary, supplemented or amended at least once a year or more frequently if needed (e.g., after the launch of a new critical business process, infrastructure component, software application; upon changes in key employees, etc.).

**Content and criteria**

Business continuity testing

Regular testing – supervised entity should determine regularity of testing. For critical services kind of periodicity should be determined, for example annually or bi-annually. Besides, supervised entity should constantly monitor internal and external environment to decide about business continuity testing.

Schedule of the planned tests – supervision authority constantly collects testing results and testing plans to ensure their compliance.

Analyzing test results – the analysis of testing results should follow and if necessary, the changes should be implemented and re-testing should be the case. If supervision authority gets information about unsuccessful tests, it can be presumed that necessary measures will be taken and tests will be repeated.

Evaluation of continuity testing results:

1. Ensure that business continuity manager possesses documentation about business continuity testing results;
2. Analyze testing results and ensure that activities need to be taken are included

into business continuity plan;
3. Assess the tendency of problems and ensure that solutions are found.

Risk analysis with changes in BC plan

Auditing BC plan

Review of BC plan – certainly BC plan needs review in case business continuity incident occurs. The changes in plan can also be based on testing results.

Documentation:

- Reports of incidents;
- Reports produced by internal and external auditors;
- Business continuity testing reports and action plans;
- Contracts in connection with alternative locations.

In addition:

1. Ensure that all the written emergency procedures are composed thoroughly, appropriately, accurately, timely and comprehensibly;
2. Ensure that all recovery teams have written procedures to follow in case of emergency;
3. Ensure that there exists relevant procedure for updating written emergency procedures;
4. Ensure that recovery procedures for users are documented;
5. Ensure that there is relevant description about relocation to the secondary site;
6. Ensure that recovery plans describe sufficiently recovering from emergency site,
7. Find out where is maintained equipment for recovering information processing center (hardware list, communications diagrams etc.);
8. Ensure that business continuity plan defines meeting places for crisis committee to decide about launching continuity plan;
9. Ensure that documented procedures are relevant for successful recovery;
10. Ensure that into continuity plans are involved descriptions about duplicate communication channels (data and voice);
11. Ensure that inside of continuity plan there exists description about relocation to the secondary information processing site in case the primary site is not recoverable;
12. Ensure that inside of continuity plan there exists description about how manually processed data will be put into information processing systems;
13. Ensure that critical and delicate information and according applications are regularly backed up;
14. Ensure that there exists a list of priorities of services to the users;
15. Ensure that there exists relevant documentation for recovering in case of emergency or data loss.

Ascertain security of offsite location:

- Ensure that controls (physical, environmental and logical) are in place for *offsite facilities*: access controls, raised floors, humidity control systems, temperature control systems, uninterrupted power supply (UPS), water establishment and supplant systems, smoke alarms and relevant extinguisher.

Assessment of alternative processing contract:

- Provide a copy of contract with service provider of alternative processing site;
- Ensure that service provider is competent in providing services and service provider has assured it with necessary signatures.

**For assessment**

Quantity

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Annual business continuity testing plan | | | | | | |
| Test reports | | | | | | |
| | | | | | | |

Quality

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Analysis of testing results | | | | | | |
| Frequency of testing critical functions | X | | | | | |
| | | | | | | |

Control

| **Criteria** | **BB** | **SB** | **BI** | **SI** | **IF** | **FM** |
|---|---|---|---|---|---|---|
| Auditing of business continuity plans | | | | | | |
| Monitor of | X | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| changes | | | | | | |
| business continuity plan overview after major incident | X | | | | | |
| business continuity plan overview after business continuity testing | X | | | | | |
| business continuity plan regular overview | | | | | | |