VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

Laima KAUŠPADIENĖ

INFORMATION SECURITY MANAGEMENT FRAMEWORK FOR SMALL AND MEDIUM ENTERPRISE

DOCTORAL DISSERTATION

TECHNOLOGICAL SCIENCES,
INFORMATICS ENGINEERING (T 007)

VGTU
LEIDYKLA
TECHNIKA
Vilnius 2019

Doctoral dissertation was prepared at Vilnius Gediminas Technical University in 2012–2019.

Scientific Supervisor

Prof. Dr Habil. Antanas ČENYS (Vilnius Gediminas Technical University, Informatics Engineering – T 007).

The Dissertation Defence Council of Scientific Field of Informatics Engineering of Vilnius Gediminas Technical University:

Chairman

Prof. Dr Dalius MAŽEIKA (Vilnius Gediminas Technical University, Informatics Engineering – T 007).

Members:

Prof. Dr Rimantas BUTLERIS (Kaunas University of Technology, Informatics Engineering – T 007),

Prof. Dr Habil. Gintautas DZEMYDA (Vilnius University, Informatics Engineering – T 007),

Prof. Dr Habil. Ioan DZITAC (The Agora University of Oradea, Romania, Informatics Engineering – T 007),

Dr Jevgenijus TOLDINAS (Kaunas University of Technology, Informatics Engineering – T 007).

The dissertation will be defended at the public meeting of the Dissertation Defense Council of Informatics Engineering in the Senate Hall of Vilnius Gediminas Technical University at **10 a. m. on 23 August 2019.**

Address: Saulėtekio al. 11, LT-10223 Vilnius, Lithuania.
Tel.: +370 5 274 4956; fax +370 5 270 0112; e-mail: doktor@vgtu.lt

A notification on the intend defending of the dissertation was send on 22 July 2019.

A copy of the doctoral dissertation is available for review at VGTU repository http://dspace.vgtu.lt at the Library of Vilnius Gediminas Technical University (Saulėtekio al. 14, LT-10223 Vilnius, Lithuania) and the library of Kaunas University of Technology (K. Donelaičio st. 20, LT-44239 Kaunas, Lithuania).

VGTU leidyklos TECHNIKA 2019-027-M mokslo literatūros knyga
http://leidykla.vgtu.lt

ISBN 978-609-476-185-0

laimakausp@gmail.com

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Laima KAUŠPADIENĖ

INFORMACIJOS SAUGOS VALDYMO KARKASAS SMULKIAM IR VIDUTINIAM VERSLUI

DAKTARO DISERTACIJA

TECHNOLOGIJOS MOKSLAI,
INFORMATIKOS INŽINERIJA (T 007)

VGTU
LEIDYKLA
TECHNIKA
Vilnius 2019

Disertacija rengta 2012–2019 metais Vilniaus Gedimino technikos universitete.

Mokslinis vadovas

prof. habil. dr. Antanas ČENYS (Vilniaus Gedimino technikos universitetas, informatikos inžinerija – T 007).

Vilniaus Gedimino technikos universiteto Informatikos inžinerijos mokslo krypties disertacijos gynimo taryba:

Pirmininkas

prof. dr. Dalius MAŽEIKA (Vilniaus Gedimino technikos universitetas, informatikos inžinerija – T 007).

Nariai:

prof. dr. Rimantas BUTLERIS (Kauno technologijos universitetas, informatikos inžinerija – T 007),

prof. habil. dr. Gintautas DZEMYDA (Vilniaus universitetas, informatikos inžinerija – T 007),

prof. habil. dr. Ioan DZITAC (Oradea Agora universitetas, Rumunija, informatikos inžinerija – T 007),

dr. Jevgenijus TOLDINAS (Kauno technologijos universitetas, informatikos inžinerija – T 007).

Disertacija bus ginama viešame Informatikos inžinerijos mokslo krypties disertacijos gynimo tarybos posėdyje **2019 m. rugpjūčio 23 d. 10 val.** Vilniaus Gedimino technikos universiteto senato posėdžių salėje.

Adresas: Saulėtekio al. 11, LT-10223 Vilnius, Lietuva.
Tel.: (8 5) 274 4956; faksas (8 5) 270 0112; el. paštas doktor@vgtu.lt.

Pranešimai apie numatomą ginti disertaciją išsiųsti 2019 m. liepos 22 d.

Disertaciją galima peržiūrėti VGTU talpykloje http://dspace.vgtu.lt ir Vilniaus Gedimino technikos universiteto bibliotekoje (Saulėtekio al. 14, LT-10223 Vilnius, Lietuva) ir Kauno technologijos universiteto bibliotekoje (K. Donelaičio g. 20, LT-44239 Kaunas, Lietuva).

Abstract

Information security is one of the concerns any organization or person faces. The list of new threats appears, and information security management mechanisms have to be established and continuously updated to be able to fight against possible security issues. To be up to date with existing information technology threats and prevention, protection, maintenance possibilities, more significant organizations establish positions or even departments, to be responsible for the information security management. However, small and medium enterprise (SME) does not have enough capacities. Therefore, the information security management situation in SMEs is fragmented and needs improvement.

In this thesis, the problem of information security management in the small and medium enterprise is analyzed. It aims to simplify the information security management process in the small and medium enterprise by proposing concentrated information and tools in information security management framework. Existence of an information security framework could motivate SME to use it in practice and lead to an increase of SME security level.

The dissertation consists of an introduction, four main chapters and general conclusions. The first chapter introduces the problem of information security management and its' automation. Moreover, state-of-the-art frameworks for information security management in SME are analyzed and compared.

The second chapter proposes a novel information security management framework and guidelines on its adoption. The framework is designed based on existing methodologies and frameworks.

A need for a model for security evaluation based on the organization's management structure noticed in chapter two; therefore, new probability theory-based model for organizations information flow security level estimation presented in chapter three. The fourth chapter presents the validation of proposed security evaluation models by showing results of a case study and experts ranking of the same situations. The multi-criteria analysis was executed to evaluate the ISMF suitability to be applied in a small and medium enterprise. In this chapter, we also analyze the opinion of information technology employees in an SME on newly proposed information security management framework as well as a new model for information security level estimation.

The thesis is summarized by the general conclusions which confirm the need of newly proposed framework and associated tools as well as its suitability to be used in SME to increase the understanding of current information security threat situation.

Reziumė

Informacijos sauga yra viena iš problemų, su kuriomis susiduria tiek šiuolaikinės organizacijos, tiek ir individualūs asmenys. Kadangi nuolat atsiranda naujų saugos grėsmių, tai informacijos saugos užtikrinimas privalo būti vykdomas ir atnaujinamas nuolat. Dėl šios srities sudėtingumo didesnėse organizacijose steigiamos papildomos darbo vietos ar net padaliniai. Tačiau dėl savo ribotų resursų mažas ir vidutinis verslas ieško priemonių, kurios leistų ir ne saugos, o pavyzdžiui informacinių technologijų specialistui, įsisavinti šią sritį.

Šioje disertacijoje analizuojama informacijos saugos valdymo problematika mažame ir vidutiniame versle. Darbo tikslu išsikeliama supaprastinti informacijos saugos valdymo procesą mažame ir vidutiniame versle, susisteminant reikiamas žinias ir pasiūlant įrankius informacijos saugos valdymo karkase. Pasiūlytas informacijos saugos valdymo karkasas leis ir ne informacijos saugos ekspertams perprasti organizacijai kylančias saugos grėsmes ir skatins didinti organizacijos saugos lygį.

Disertaciją sudaro įvadas, keturi pagrindiniai skyriai ir bendrosios išvados. Pirmajame skyriuje apibrėžiama informacijos saugos valdymo problema, apžvelgiami egzistuojantys informacijos saugos valdymo karkasai ir galimi taikyti įrankiai.

Antrame skyriuje siūlomas naujas informacijos saugos valdymo karkasas, kuris remiasi egzistuojančiomis gerosiomis praktikomis ir egzistuojančiomis metodikomis.

Kadangi antrame skyriuje nustatyta, kad organizacijos valdymo struktūros modeliavimui ar vertinimui saugos atžvilgiu įrankių nėra, siūlomas naujas tikimybių teorija paremtas modelis. Šis modelis leidžia įvertinti informacijos srauto saugumo lygį duomenų konfidencialumo, prieinamumo ir vientisumo atžvilgiais ir yra aprašytas trečiame skyriuje.

Ketvirtame skyriuje aprašomas pasiūlytų modelių taikymo eksperimentas, kurio rezultatai lyginami su ekspertų įvertinimais. Atlikta daugiakriterinė analizė, kuri leidžia nustatyti informacijos saugos valdymo karkaso tinkamumą taikyti mažoje ir vidutinėje įmonėje. Šiame skyriuje taip pat analizuojama, ar pasiūlytas informacijos saugos valdymo karkasas yra suprantamas mažo ir vidutinio verslo atstovams.

Disertacija apibendrinama bendrosiomis išvadomis, kurios patvirtina informacijos saugos valdymo karkaso ir su juo siejamų įrankių poreikį bei jų tinkamumą mažo ir vidutinio verslo informacijos saugos rizikų pilnesniam suvokimui.

Notations

Symbols

BS_j – BS_j is modified CVSS base score for vulnerability j

$conf$ – employee confidentiality level coefficient for node

$IMPACT_{conf}$ – confidentiality impact value

$IMPACT_{Integ}$ – integrity impact value

$IMPACT_{Avail}$ – availability impact value

ISC_{Base} – modified CVSS v3.0 base score

nl_j – data leakage likelihood value for threat j

$P_a()$ – channel accessibility by external attacker

$P_{An}()$ – receiver's availability

$P_{AN}()$ – probability that the version is available in at least one of nodes which stores the version of information object

$P_{As}()$ – receiver's storage availability

$P_{At}()$ – probability of data availability in transfer channel

$P_{Av}()$ – versions availability

$P_{Av\text{-}1}()$ – previous versions availability

$P_C()$ – object data leakage probability

$P_{Cn}()$ – the probabilities of data leakage in a node

P_{Ct}() – data leakage probability in transfer between enterprise nodes
P_{If}() – the integrity of information flow
P_{Ih}() – integrity corruption probability by its user (human factors) in node
P_{Is}() – integrity corruption probability while storage in node
P_{It}() – integrity corruption probability during transfer between two nodes
P_{Iv}() – integrity of objects version
P_r() – attack probability against this type of enterprise

Abbreviations

AHP – analytic hierarchy process
BPMN – Business Process Model and Notation
PE-BPNM – privacy-enhanced extensions to the BPMN
CISO – Chief Information Security Officer
COBIT – Control Objectives for Information and Related Technologies
EAAT – Enterprise Architecture Analysis Tool
CySeMoL – The Cyber Security Modeling Language (an extension to the EAAT)
EMS – enterprise management structure
ENISA – European Union Agency for Network and Information Security
ETTIS – European security trends and threats in society
IT – information technologies
ITC – information technology and communication
ITIL – Information Technology Infrastructure Library
IS – information system
ISM – information security management
ISMF – information security management framework
HISMF – high-level information security management framework
ISO – International Organization for Standardization
SABSA – Sherwood Applied Business Security Architecture
PDCA – Plan-Do-Act-Check cycle, also known as Deming cycle
SME – small and medium enterprise
MCDM – multiple-criteria decision-making

Contents

[1] The annexes are provided in the enclosed disc.

Introduction

Problem Formulation

Business processes of a modern organization are increasingly growing to be reliant on information technology. Therefore, information security is one of the main concerns of any enterprise. All enterprise data must be available to execute operations of the enterprise, provide services to its customers. The enterprise must ensure the confidentiality, availability, and integrity of the enterprise and its customers' data. However, news on data breach, distributed denial of service attacks on different systems occur daily if not hourly. Even extensive information technology-related companies are vulnerable to some security issues. It is crucial to see information security management as a continuous process. Large enterprises typically have departments of information security management established. Experts in information security analyze existing security standards, best practices, look for, and apply the newest security systems. Meanwhile, small and medium enterprises (SME) are lacking resources while the same threats for information security apply. In SMEs information technology (IT) department or even a single person is responsible for all the maintenance and management of IT and enterprise information security. It is not enough, as information security management (ISM) requires specific knowledge and skills. Non-professional information security

personnel needs constant monitoring of the current situation in the enterprise and time to look for new recommendations, solutions, and at the same time, need to look after the enterprise IT infrastructure. Such a workload can be exhaustive and prove insufficient to ensure the quality of the processes. Therefore, the information security management framework (ISMF), dedicated to SME, might improve the situation.

A variety of information security management frameworks exist. However, an ISMF with most important information security management elements, high-level processes, and stakeholders of ISM is missing. This leads to a situation an SME need to look for multiple frameworks and combine them individually. It takes time and requires additional resources. As well the time is necessary to get a list of tools, dedicated to analyze the existing ISM situation or/and to improve it. The list of ISMF associated tools is not present in existing ISMF as well.

Relevance of the Thesis

Variety of tools and standards, dedicated to information security regulation, risk evaluation, and management exist. However, most of the tools are not adapted to SME or covers just a part of ISM. Therefore, it is a hard, resource demanding task to adjust them in practice. The consequences of partially adapted tools or usage of no support system for ISM leads to cases when security vulnerabilities in the enterprise exist, attacks on the enterprise are executed, enterprise data and services are corrupted, the enterprise cannot operate, the damage is done to customers or partners systems, etc.

By providing the SME focused and up-to-date information security management framework, the SME could keep up with evolving security baseline and ensure proper level information security management in the enterprise even with lacking resources for ISM.

The Object of Research

The Object of this dissertation – information security management frameworks for usage in the small and medium enterprise.

The Aim of the Thesis

The main aim is to enrich the area of information security management frameworks by proposing an information security management framework with extended lists of stakeholders and tools for SME simplified usage.

The Objectives of the Thesis

To achieve the aim of the thesis, the following objectives were formulated:

1. To analyze the existing frameworks for information security management;
2. To design a new information security management framework which will combine high-level processes and stakeholders of ISM;
3. To provide a list of associated tools for proposed ISM framework to automate or simplify the framework usage in SME;
4. To evaluate the proposed ISM framework and tools as information security management improvement solution for a small and medium enterprise.

Research Methodology

To achieve the aim of the thesis, the following research methods were used:

1. Comparative research and systematic literature research for information security management and existing information security management frameworks;
2. An experiment research method was applied to validate the proposed ISM ideas;
3. Generalization for structuring the research and analysis results.

Scientific Novelty of the Thesis

The scientific novelty is proven by the following results:

1. New information security management framework designed to concentrate main best practices of information security management and concentration to all types of stakeholders introduced to ensure broad perspective of the information security management. At the same time the ISM framework simpler applicability in SME is assured by providing a list of needed tools;
2. Information security level estimation models developed to model the impact of information flows and human factors. The use of these models allows information flow security evaluation by considering both hardware, software technologies as well as information flows and human factors.

Practical Value of the Research Findings

The proposed ISM frameworks with a list of existing and newly proposed tools require fewer resources to evaluate and model the ISM in the small and medium enterprise. By using the proposed framework and tools, SME can reduce the need for ISM resources as automated information security level evaluation and modeling require less time and knowledge, comparing to manual assessment. The decrease of resources during the usage of automated information security evaluation tools in SME allow maintenance or increase the information security level where information security experts do not exist as numeric values for comparison of different situations are more understandable.

The Defended Statements

1. Integration of all type stakeholders into the ISM framework allows assurance of wider range information security threads in the enterprise and increases the understanding of security policy importance.
2. Probabilistic methods are suitable for SME information security level evaluation and can replace the experts work in security risk ranking, therefore, can reduce the information security management cost.
3. Quantitative evaluation of information security management framework suitability for small and medium enterprise requires multi-criteria decision-making and analytical hierarchy process.

Approval of the Research Findings

The material of this dissertation is published in *Clarivate Analytics Web of Science* databases refereed journals. One with a citation index and two without a citation index. The author has made two presentations at two international scientific conferences:

1. The 1st IEEE Workshop on Advances in Information, Electronic and Electrical Engineering AIEEE'13, Riga, Latvia, November 26–27, 2013;
2. IEEE International Conference, Hamburg, Germany 4th October 2018.

Dissertation Structure

The scientific work consists of an introduction of the dissertation, four chapters, general conclusions, references, list of author's publications and annexes. The total scope of the dissertation – 114 pages without annexes. There are 39 pictures and 16 tables in the text. 132 references were used in the dissertation text.

1

Information Security Management and Existing Information Security Management Frameworks

To manage information security, a deep understanding of this area and existing tools must be considered. Therefore, in this chapter, the main principles of information security management and existing solutions are presented. The result of the systematic literature review is summarized by topics as well as publication year and demonstrates researchers' interests in information security management area during the last ten years. The existing ISM frameworks are analyzed and compared according to different criteria to highlight the missing components or problems for application in SME. The results are essential as ideas of the proposed Information security management framework are concentrated and generated based on this comparative analysis.

Analysis presented in this Chapter was published in (Kauspadiene, 2017)[2].

[2] The references are given in the list of publications by the author on the topic of the dissertation

1.1. Information Security Management

Information security management covers tools, links, interconnections, documented policies, data, technologies and other means that help to ensure a minimal level of information security risks within and outside the organizational processes, therefore ensuring business continuity.

By sustaining systematic and well-timed processes of information security management, the organization can protect its assets and sensitive data from being breached, leaked, or exposed to other damaging elements, e.g., human factor errors. Due to poorly established information security management processes, valuable assets of an organization face unimaginable risk. Irreversible damage can be made for all aspects of the organization's activities – from sensitive personal data of employees, customers to commercial activities while breaching servers, cloud services and, even, physical security measures.

Further on in this dissertation, three key elements that information security stands for will be referred to. These are Confidentiality, Integrity, Availability. ISO/IEC 27000 – Information security management systems – standards family, defines Confidentiality as where "Information is not made available or disclosed to unauthorized individuals and entities or processes." Integrity is defined as "the property of accuracy and completeness of assets." Finally, Availability is defined as "the property of being accessible and usable upon demand by an authorized entity." In short, information must have specific limited access, be trustworthy, accurate and accessible by authorized people.

1.2. Existing Information Security Management Researches

This study has been undertaken as a systematic literature review, partly based on a Guidelines, proposed by Kitchenham (Kitchenham 2007). This section asks questions that scope future research activities and are intended to identify the existing basis for the research work and should make it clear where the research fits into the current body of knowledge. As further research is going to be on the topic of ISM process optimization, it is needed to investigate what frameworks are already composed for the ISM. For that reason, it is necessary to perform a relevant literature review.

1.2.1. Search Process and Study Selection

The search process was performed in digital libraries and search engines. For searching, the keywords were extracted from the research questions, e.g., Information security management, Information security governance, cyber-crime

defense, etc., and a list of synonym words was conducted. For the search process, the following databases were used:

1. ACM;
2. InterScience;
3. Google scholar;
4. IEEE Explore;
5. Inspec;
6. ISI Web of Science;
7. ScienceDirect;
8. SpringerLink.

Search results exceeded 2400 references. Evaluation of the title enabled to reject approximately 1150 references. After the assessment of the abstracts there was a list of 350 papers, and finally, after a more in-depth sight into the papers and the evaluation of their relevancy, a final list of 80 articles was established. The process of papers‘ selection is shown in Fig. 1.1.

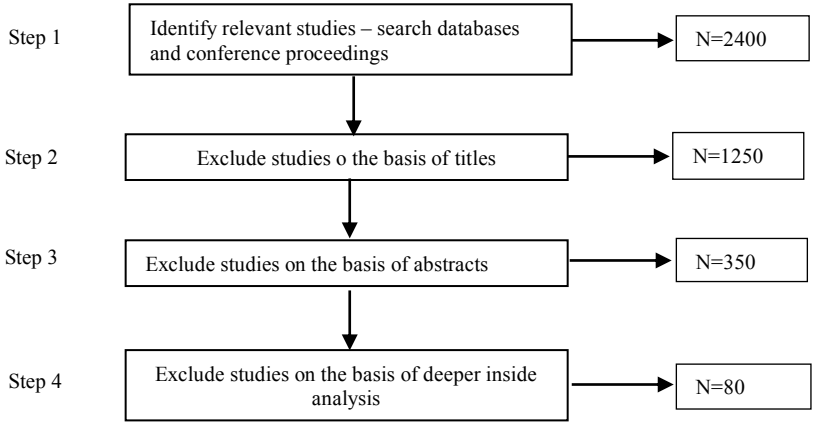


Fig. 1.1. Steps of the paper selection process

Following the recommendations of Kitchenham et al. (2010), relevant studies were assessed for their actual relevance. Main inclusion criteria for selecting studies were:

1. Paper describes research on ISM;
2. Issues, concerning ISM are discussed, e.g. standards, methodologies, policies, applications;
3. An ISM framework is proposed.

Criteria for exclusion of research works were:

1. Pure technical approach to ISM system;

2. Lack of ICT approach.

As the main task of this systematic literature review is to prepare for further detailed investigations of information security management and its framework development, all the papers were divided into six groups. One group serves as an umbrella for a sub-group of similar topics. The classification was established after the revision of the literature contents and semantic analysis of further investigation's topic. Thus, all the groups will serve as a foundation for going on the research of information security management framework concept. Established groups will cover the research questions, as well. The groups are as follows:

1. disclosure of information security management;
2. analysis of Information security management conceptual models:
   a) risks and solutions in organizational level;
   b) the operational system frame;
   c) an integrated system platform layer;
   d) information security conceptual frameworks.
3. innovative cloud computing, distributed systems;
4. analysis of standards and methodologies;
5. methodological grounds of the research.

The classification was developed for the purpose of our review and is not intended to be a general-purpose classification of information security management studies. Most of the categories are nonexclusive; thus, a paper applies to more than one research approach. This general schema serves as a starting point for more in-depth investigation of findings that seem to suggest possibilities for improvement.

In the next section, the results of the research are given. A chronological approach for the research is chosen. The special attention was given to papers, where a particular solution on Information security management conceptual frameworks/models is suggested.

1.2.2. Disclosure of Information Security Management

Principles of information security management are presented in most ISM related papers. However, a portion of scientific papers is oriented on the description of information security management or sharing of experience in this area.

Von Solms (1998a) was one of the first who started working on information systems management and attempted to define guidelines for information technology (IT) security systems. This author was one of the initiators of information security management investigation and provided multiple scientific papers on information security management. He clarified the information security concepts and terms (Von Solm, 2005) and led in this area.

By sharing his experience, on 2004 Von Solms (Von Solms et al., 2004) republished a work about main mistakes that are made by information security officers. The title of this paper was high-sounding – "The 10 deadly sins of information security management". This article is intended to promote and systematize the author's experience of the last six years.

There exist more papers on information security management both by Von Solms and other authors. However, those papers are more related to a more specific area, rather than defining the main concepts and personal experience. There those papers are analyzed in other categories of information security related scientific papers.

1.2.3. Analysis of Information Security Management Models

As Von Solms was the initiator of information security management area investigation, he participated in an analysis of the conceptual nature of IT security systems. Von Solms (Von Solms, 1998b) released an article about information security conceptual modeling. This approach was more applicable, and it was a continuity of the article, published earlier by the same author.

In the area of ISM conceptual modeling, new authors raised. But the variety of conceptual modeling was so broad, so we divided it into four groups.

Risk and Solutions in Organizational Level

Von Solms are active in this field and presents a paper, dedicated to the evaluation of risk solutions in the organizational level (Von Solm et al., 2005).

Information security as a management process was analyzed by Gary Stoneburner, Alice Goguen, and Alexis Feringa (Stoneburner, 2002). These researches were interested in risk, arising at an organizational level and risk impact for the organizations. Therefore, their research activities result in the preparation of systematic information security risk management documentation for information technology systems. This is one of the first officially recognized and well-known implementation of the risk management processes application in the organization's ISM processes.

The evaluation of the risk assessment during the implementation of information security solutions is analyzed. Arora Ashish (Ashish, 2004) in his group of publications, analyzes the risk of information security systems. System framework, it's architectural and technical solutions are being examined by Shahram Gilaninia (Gilaninia et al., 2012), who seek to evaluate the efficiency of ISM on information system management. Those are papers, oriented to system level risk, while a more significant number of papers was geared to organizational level risks.

Economic potentials for information security risk assessment was analyzed by Rok Bojanc and Borka Jerman-Blažič (Jerman-Blazic, 2008) too. Their

research is oriented to the risk's economical cost evaluation and organization security risk assessments.

In organizational-level risk management, Walter Baer and Andrew Parkinson analyzed the role of cyber insurance in security management (Baer et al., 2007). They examined the organization-level risks of management decisions, investigated economic possibilities to ensure information systems from possible informational leakage and analyzed options for risk management. Meanwhile, Baer Wade and Linda Wallace explained potentials of information security control, with an emphasis on quality in the field of ISM. These authors defined the evaluation criteria for ISM process quality, but, as the evaluation of conceptual information model is not set yet, these scientists' attempts and proposed solutions are episodic.

Thomas L. Wheeler (Wheeler, 2008) investigated organizations' security metrics' calculation methods, and according to the data of successful cyber attacks, analyzed if organizations are capable of protecting themselves. The author brings up a question of a need for a governmental organization for information security. Stefan Fenz and Ekelhart Andreas (Fenz et al., 2011) represented possibilities for ISM evaluation, identification, and standardization. Meanwhile, Zhanna Mingaleva and Kapuskina Tatiana (Mingaleva et al., 2009) studied a specific case – the impact of information security on the economy of Russia.

The quantitative evaluation and discrete solutions were actual in analyzed papers. Therefore, Pooya Jaferian el al. (Jeferian et al., 2014) highlighted the need for quantitative analysis. In their article, a heuristic of ISM tools was analyzed. It can be stated, that the first organizational research was based upon user's motivation model analysis and was oriented to the evaluation of organization's information security, and the other study by Pooya was adapted to the applicable review of organization's ISM tools and was more coherent to the technical management of ISM processes. Mayer (Mayer et al., 2018) supports the vision and proposes to integrate information system security risk management with enterprise architecture management.

Herrmann Mimi (Herrmann, 2009) analyzed security strategy rather than economic possibilities or quantitative security metrics. While in the field of information security conceptual model Van Niekerk together with Von Solms (Van Niekerk et al., 2010) described information security culture from the management perspective.

Tohidi (Tohidi, 2011) presented a paper about the role of ISM processes and risk management in organizations' information systems. At the same time Jian Zhang, Wei Hua Yuan, Wenjing Qi (Zhang et al., 2011) and Mike Faessler with Mark Morgan (Faessler et al., 2011) defined possibilities to optimize information security risk management and ISM.

There through distinguishes two key aspects of ISM:

1. risk control;
2. operations‘ management.

Organization-level risk and solutions are also analyzed by scientists‘ groups Anil Kumar Chorppath with Tansu Alpcan (Chorppath et al., 2012) and Hyeun-Suk Rhee, Young U Ryu with Cheong-Tag Kim (Rhee et al., 2012). The first group of researchers analyze information security risk management, compare theoretical and practical aspects of information security risk management. Meanwhile, the second group of scientists skeptically take the achievements of the last 15 years of ISM researches, define the human factor, and introduce new indeterminacy elements into the science of ISM.

Mario Spremic describes ISM model of organization, represents a holistic approach to the information systems, risk management. His model is based on Von Solms‘ ontological solution, that was proposed in 2002. The second researcher analyzes the application of integrated ISM to the governmental institutions, offers a conceptual solution based on ISO 27000 standard and PDCA (Plan-Do-Act-Check) cycle. The author integrates conventional solutions and systematically represents them. This article can be assigned not only to the group of the articles on information security conceptual model evaluation but to the group of ISM literature review articles‘ group as well.

The Operational System Frame

The previously analyzed papers defined there should be a separate area of risk management – operations management. One of the first authors, which explained specifically this area was Fredrik Bjorck (Bjorck, 2004). In 2004 he analyzed security and decision making issues and described the institutional information security theory from the perspectives of the application of information systems‘ organizing principles.

Von Solms was active in this area too, as they examined the operation level of ISM, were dedicated to disclosing fundamental obstacles for implementing ISM. In 2015 Von Solms (Von Solm, 2005) released paper in the Journal of Computers & Security and proceeded their work in the spectrum or ISMS analysis. In the second disquisition paper, Von Solms (Von Solms et al., 2005) analyzed interactions between information security and business security on purpose to reveal how information security influences business security. The point of this article is that the discipline of information security has outgrown its name and information security has become a critical component to corporate governance. It proposes that business security is a more appropriate name than information security because information security activity is now broader than just the protection of data, information, and software. In the context of the generally accepted notion that the objective of information security is to protect organization‘s asset, the article poses the question „if we accept that such protection mitigates business risks, should we not start calling it business security instead of information security?“.

The information security management relations to enterprise management are analyzed by Jo Malcolmson (Malcolmson, 2009) too. This author analyzes information security culture from the organizational perspective. Meanwhile, Kenneth Knapp (Knapp et al., 2009) analyzed the policy of information security in the level of the organization process model.

The more specific area was an article about information security conceptual model by Jai-Yeol Son (Son, 2011) and Karin Hedström et al. (Hedstrom et al., 2011). These authors analyzed information security conceptual model through the prism of the human factor. Articles were based upon Janine L. Spears and Henri Barki 2010-year research data on users' participation in ISM.

The operational system security management is essential, and nowadays research activities in this area are still seen: Cezar (Cesar et al., 2017) analyzes outsourcing related ISM; Tweneboah-Koduah (Tweneboah-Koduah et al., 2018) concentrates on critical infrastructure systems; Radanliev (Radanliev et al., 2018) investigates security operational management in internet of things area.

An Integrated System Platform Model

Hong Kwo-Shing (Hong, 2003) in his paper proposed the theory of integrated information security management systems. It was the beginning of information security management as a complex, multi-component problem. The same idea was supported by G. Whitson (Whitson, 2003) as he provided clarifications of the compositional facility of the three common elements in computer security – theory, process, and management. All this crystallization of ISM processes and ISM sciences and it's body of knowledge leads to an integrated approach to its research field.

The need of engineering solutions is highlighter in article "Information security management: a new paradigm" a system framework was analyzed by Jan HP Eloff and Mariki Eloff (Eloff et al., 2003), who delivered a need for a robust engineering system design.

The analysis of an integrated system's platform-level is presented by Ernest Chang Shuchih and Chienta Bruce Ho (Ernest Chang et al., 2006). This group of scientists researches the impact of the organization factors on the efficiency of the ISM solutions, i.e., how the environment of the organization effects ISMSs.

The integrated system platform level is analyzed by Maxim O. Kalinin (Kalinin, 2010) too. He proceeded the analysis that was started by Beznosov scientific group and introduced an innovative solution for that period – information system security method by applying integrated control and automated security solutions.

Also, based on these articles in an article by G. Pavlov and J. Karakaneva (Pavlov et al., 2011), about ISMS in organizations was published. Researchers in the article appealed to the results of Beznosov's researches that were announced in 2009 and works of Von Solms in the field of information security conceptual model and standardization. Scientific solutions by Pavlov and Karakaneva can be

considered as a prolongation of Kalinin‘s works on automated security and integrated control systems at the conceptual theoretical level.

With a rise of the internet of things using the threat management has to be implemented for it too. Therefore Ko (Ko et al., 2018) proposes a threat information management platform.

It is essential to mention that not only high-level proposals existed. Some of the analyzed papers were very detailed and oriented to implementation, while Shervin Erfani (Erfani, 2003) patented his invention – the Security management system and method.

Information Security Conceptual Frameworks

While multiple models and solutions for information security risk evaluation and management exist, it can be consolidated into one framework. One of the first attempts to adjust concepts and terms, and with respect to the earlier proposed information security conceptual models propose a framework was in 2003 by Denis Trèek (Trèek, 2003). This author submitted the article about the integral systematic framework application into the ISM.

Farn Kwo-Jean, Lin Shu-Kuo, and Andrew Ren-Wei Fung (Fam et al., 2004), also published a paper in the category of system framework analysis. Authors seek to execute the evaluation of ISM, to define vulnerability, threats, and weaknesses. This article has a diagnostic character, where authors present in what way while applying COBIT standards, it is possible to avoid information security procedural gaps in the organization as well as what type of system can be used for the same purpose.

Bill Tsoumas and Gritzalis Dimitris (Tsoumas et al., 2006) represented a paper in the field of systems‘ framework analysis. Authors in the International scientific conference Advanced Information Networking and Applications presented an ontology-based concept of the security management model, thereby brought a significant scientific contribution to the analysis of ISMS frames.

Ellie Myler and George Broadbent with the paper on security standards in 2006 made a foundation for further studies, which were performed in 2007 while investigating the level of integrated system platform. Integrated system platform level is also used by David Botta, Andrew McGee, and Richard Tracy. David Botta (Botta et al., 2007) in his paper analyzed tools that are used by information security professionals. Andrew McGee (McGee et al., 2007) studied the implementation of Bell labs‘ security framework and submitted proposals for ISMS improvements, thus unveiled the potentials for further development of integrated system platform. Meanwhile, Richard Tracy (Tracy, 2007) in his article about ISM and business processes‘ automatization challenges, perspectives, and benefits, presented further dimensions of integrated platform development.

In 2008 upspring a paper, that is a continuity of Von Solms information security conceptual framework indoctrination, that he presented in the ISM

guidelines. The article was composed by Kirstie Hawkey, Kasia Muldner, and Konstantin Beznosov (Hawkey et al., 2008). Authors explored a conceptual framework that should equilibrate organization‘s ISM and proper interaction with the external environment. Further, in 2009 these researches were proceeded by Rodrigo Werlinger, Kirstie Hawkey, and Konstantin Beznosov (Werlinger et al., 2009).

One more group of scientists that analyzed information security framework was Parkin Simon (Parkin et al., 2010) with joint authors. They studied potentials and were looking for solutions on how information security managers, adopting an integrated information security platform, could optimize the process of security management.

An article that analyzes the information security system platform framework was represented by Y.Monfelt, S.Pilemalm, J.Hallberg, L.Yngstrom (Monfelt et al., 2011). Here authors investigate 14 layered ISM framework from social and organizational aspects.

A case study on implementing an Information Security Management Framework in a green energy production plant was presented by A. I. Hohan et al. (Hohan et al., 2014), where the paper highlighted a part of the results of information security management systems research in the context of business excellence. The study was focused on the design and implementation of an Information security management framework for protecting a grid-connected renewable energy power plant – a critical infrastructure with growing relevance in the energy markets, and heavily dependent on industrial information systems. The proposed approach was intended for use by all grid-connected renewable energy producers, either solar, wind or biomass generation.

Currently, more specified, dedicated to specific area frameworks are proposed. For example, Hussain (Hussain et al., 2018) offers a conceptual framework for the security of mobile health applications; Jouini (Jouini et al., 2019) published a paper on security framework for secure cloud computing environments.

Innovative Cloud Computing, Distributed Systems

During the technological progress of information technologies, occurred solutions for the application of innovative cloud distributed systems due to ensure the security of ISM processes. This topic was analyzed by Jung Youngmin and Mokdong Chun (Jung et al., 2010). They submitted a solution to adaptive security management model in the cloud-computing environment.

Together with the rise of Industry 4.0 approach, a significant shift in the thematic of the researches of information security can be noticed. Major ICT elements, such as the Internet of Things, Big data, Artificial intelligence, Virtual and Augmented reality, Smart everything everywhere, empowered a significant number of articles in that field. However, no significant alterations were observed in the field of information security management. Governmental regulatory, e.g.,

European Union General Data Protection Regulation, illustrates the importance of the holistic approach regarding information security management. Nonetheless, there is very few researches on ISM. However, during the last year, a patent exists in this area, which defines system and method for enhanced security and management mechanisms for enterprise administrators in a cloud-based environment (Kiang and Lee, 2018).

Analysis of Standards and Methodologies

Publication with the pure subject of information security standards came up by Von Solms in 1999 and was one of the first of its kind papers.

Later ISM process applicability standards were analyzed by Karin Höne and Jan H. P. Eloff (Karin et al., 2002). In their relevant approach activity, researchers seek to perform a review of information security policy application in terms of international information security standards as well as analyze information security paradigm at the international level. Meanwhile, Clive Vermeulen and Rossouw Von Solms (Vermeulen Clive, 2002) proceed their investigations and in 2002 represents a paper on ISM tools application in an organization.

Standards and methodologies were studied by René Saint-Germain (Saint-Germain, 2005) in the paper „Information security management best practice based on ISO/IEC 17799". In this article, that was published in the Information Management Journal, the author presents the analysis of ISO standard, and elaborates on which ISO standards ISMS should be based.

The domain of information security standards was analyzed by Ellie Myler and George Broadbent (Myler and G. Broadbent, 2006). The object of their analysis was security standard ISO 17799. Research results and comprehensive analysis of ISO 17799 were published in the Information Management Journal – Prairie Village.

Later a paper by Edward Humphreys (Humphreys, 2008) was published. This article is about ISM standards, where the author makes a review of information security management, certification, and risk management. This article holistically combines previous publications: 1998–1999 Von Solms, 2002 Karin Höne and Jan H. P. Eloff, 2005 René Saint-Germain, 2006 Ellie Myler and George Broadbent. The comparison of views of these authors gives a basis for the further researches of Konstantin Beznosov's scientific group.

Standards and methodologies were analyzed by Edward Humphreys (Humphreys, 2008). Shoichi Morimoto, Mikko Siponen, and Robert Willison. Morimoto (Morimoto, 2009) started studies on this topic and paid special attention for possibilities to adjust COBIT security management standards to the formation of information systems. Meanwhile, Mikko Siponen and Robert Willison (Siponen et al., 2009) performed an analysis of ISM standards' issues and solutions.

Tati Ernawati and Nugroho Doddi (Emawati et al., 2012) published an article by representing the information security risk management framework, based on

primary studies and ISO 31000: 2009 standard. This framework was presented in an international conference ICSET in 2012. Meanwhile, Razieh Sheikhpour and Nasser Modiri (Sheikhpour et al., 2012) published a paper, where analyze best practices for integrating ITIL and ISO IEC 27001 into the processes of ISM. These both articles attempted to review the role of standards to the operation of ISM ensuring and to proceed with the analysis of standards and methodologies.

Best practices are included in Antoni Lluı́s Mesquida and Antonia Mas (Mesquida et al., 2012) paper "Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security Extension" presented extension that may be relevant for a software development company involved in a process improvement program according to the ISO/IEC 15504 international standard. The significant contribution of the work is the development and validation of the software extension, built from a thorough mapping between the ISO/IEC 27002 security controls and the ISO/IEC 15504-5 base practices for software lifecycle processes. The extension details the changes that software companies should make in the software lifecycle processes for the successful implementation of the related security controls. To attain research objectives, the authors evaluated the ISO/IEC 15504 Security Extension through case studies in a sample of software development organizations. This study followed the design science research paradigm that is based on constructive research. Proposed security extension could complement existing information security management frameworks with additional security control features.

B. Borgman (Borgman et al., 2015) came up with the article "Cybersecurity readiness in the South Australian Government." In this paper, authors conducted a series of face-to-face interviews with 17 participants from 11 SA government entities, to validate whether existing processes and strategic direction were sufficient to satisfactorily achieve the implementation of an ISMS and classification of data for the respective SA government entities. Based on interviews and review of ISMS associated reviews conducted within other Australian State and Territory jurisdictions, authors identified key areas that the SA Government may need to consider as part of the progressive roll-out of the different phases of ISMF version 3 implementation up and to June 2017. Observations outlined the specific areas that have been directly attributed to the implementation and overall classification of data as part of the general transition project. These are information security management systems, governance, risk assessment, government strategic direction, information security documentation, government reporting, classification of data, project resourcing, awareness training, and finally, certification. In summary there were identified vital areas that SA government entities may need to consider as part of the implementation of the ISMS and classification of data: (i) increased levels of engagement and general project governance by senior management; (ii) further development as part of the ongoing awareness training pitched at

multiple levels throughout government entities; (iii) continues review of project resourcing levels to ensure that key project milestones are achieved; (iv) increased monitoring of government entities' progress at a whole of government and (v) continued review of the project scope to ensure that expectations are appropriate and achievable.

Human service organizations were analyzed by S.Mubarak (Mubarak, 2016) in the article "Developing a theory-based information security management framework for human service organizations." This paper identified organizations' information security issues and explored dynamic, organizational culture, and contingency theories. It includes a critical review of global information security management issues for HSOs and appropriate multidisciplinary organizational methods to address them. In consideration of the unique nature of the organizational environment in HSOs, the author developed a new generic information security management framework based on the dynamic theory of organizational knowledge creation, organizational culture theory and contingency theory. This paper highlights the importance of addressing information security issue by providing and unpacking a new theory-based generic framework of how to embed information security management into the organizational culture. The author claims that adopting the proposed framework may be a useful step in beginning the process of developing an HSO-sector culture of awareness of the responsibilities and risks of working in electronic information storage and sharing the environment and instituting information security systems within each organization.

Methodological Grounds of the Research

In 2000, regarding the Von Solms doctrine of the practical applications of information security conceptual model, two papers, describing information security developmental trends, emerged. According to Gurpreet Dhillon and James Backhouse (Dhillon et al., 2001), in the field of investigation of information security, technical instead of management approach should be dominant. In their work „Information System Security Management in the New Millennium," published in The communication of ACM journal, authors analyze information security management systems' technical principles in the enterprise level, provide terms and definitions as well. Also, in 2000 emerged an ontological classification of information security management processes and systems. This work was published in Computer and security journal, and the authors are Mariki M. Eloff and SH Von Solms (Eloff et al., 2001). Following Von Solms, Gurpreet and Backhouse investigations, in 2001 another two interpretative works of information security topic came into being. This time the work results in analyzing terms and definitions were represented by Basie Von Solms (Von Solms, 2001a). Scientist has developed and defined information security concepts in the articles about joint management of the organization and information security, as well as emphasized the importance of information security, as an interdisciplinary science (Von

Solms, 2001b). This article presents information security as a multidimensional discipline. The intent is to view information security as a business issue, and not only a technical one. The various dimensions of information security identify are:

1. strategic/corporate governance (senior management responsibilities);
2. governance/organizational (information security organizational strucure);
3. policy (corporate policy);
4. best practices (prescribed standards);
5. ethical (professional ethics);
6. certification (professional organizations);
7. legal (statutory requirements);
8. awareness (stakeholders‘ security awareness);
9. measurement/monitoring (policy enforcement).

The proposed multidimensional discipline of information security demonstrates a need for a formal “standards” approach to information security management. For this approach to be successful, the various information security dimensions outlined in the article would have to be inter-dependent.

According to the researches of years 2000, 2001 and 2007–2009, in the topic of organization-level risk management, came up a paper that analyzes methodological grounding of the researches – this is the first empirical research with the attempt to explore and evaluate users‘ participation in ISM. This article was written by Janine L. Spears and Henri Barki (Spears et al., 2010).

M. Moeti and B.M.Kalema in 2014 presented the paper “Analytical Hierarchy Process Approach for the Metrics of Information Security Management Framework.” The primary objective of this study, therefore, was to identify metrics needed for the development of an information security management framework. From related literature, relevant metrics were identified using textual analysis and grouped into six categories of; organizational, environmental, contingency management, security policy, internal control, and information and risk management. These metrics were validated in a framework by using the analytical hierarchical process (AHP) method. Results of the study indicated that environmental metrics play a critical role in the information security management as compared to other metrics whereas the information and risk management metrics was found to be not so significant during the rankings. The article came up with some practical recommendations, e.g., an organization’s top management should provide proper and adequate support for the security program. This in terms of supporting information security policies and procedures, budget, employing skilled IT personnel and providing in-service training to the employees is paramount for substantive improvement of the stature and effectiveness of the overall corporate security; there is a need for the security team to understand the business processes of the organizations; security managers or the chief information security officers (CISO) should conduct periodic reviews or briefings to the top

management; the security team should ensure that they document and periodically publish security reports that should include but not limited: Data breach investigations reports, success and failed incidents, near-misses, latest security threats and any other security events that actually occurred within the organization.

While scientific papers were using information security management definitions, proposed mostly by Von Solms, till 2008 there were no attempts to codify the information of cyber security articles. This attempt was made by Aggeliki Tsohou (Tsohou et al., 2008). He examined the research field of information security, summed up the results of the investigations and their practical applications, has identified weaknesses in the analysis of standards. The primary input of this scientist into the research field of information security development was that he defined till then latent topics and identified directions for further investigations.

1.2.4. Historical Overview of Information Security Management Researches

Based on the executed analysis, we can see that in 1998–2003 together with rapid ISM science crystallization three phases of this branch of science development were passed:

1. purification of a scientific concept, concepts‘ and terms‘ clarification;
2. analysis of standards and its definitions;
3. conceptual modeling and tools‘ formation.

Between 1998 and 2002, ISM originator‘s, Von Solms‘ contribution to the development of information security science is significant, as researcher initially analyzes standards, concepts, and ISM processes, and in 2002 goes on with the creation of ISM conceptual framework. The researcher could be considered as a precursor of information automates systems applications.

It should be noted, that during the decade starting 1998 of Von Solms works, the paradigm of ISM changed significantly. In the first stage, till 2001 in the field of information security development concepts and standards were necessary, in the second stage of information security, scientific researches and process development field processes and economic costs became important. Scientists strived to identify system framework, define organization-level risk.

2010–2011 was necessary for distributed and cloud computing information security management as researchers understood the new technologies require a different view to information security management.

While analyzing the groups of the articles according to the popularity, it can be noted, that the majority of the papers were written on the topic of organization risk management issues. The second place goes to the articles and scientific researches, dedicated to the analysis of standards and methodologies. In the third place remains analysis of integrated system platform, information security

conceptual model, concepts, terms, and frameworks. These are conceptual fundamental studies with a purpose to reveal what is ISM and in what level it is implemented. Least works were performed in analyzing literature and in exploratory tactical level. In summary and after structuring articles by categories, it can be assumed, that most favored field in ISM processes is a risk as well as process management and organization-level solutions 'retrieval. Since 2014, there were no new disruptive approaches to ISM; only specific areas of information security management systems were analyzed.

The literature review covers 80 papers starting in 1998. According to the number of papers of each group, class (their number) per year is shown in Fig. 1.2.

Group, class of papers		Year	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	Total
	1		1						1	1															3
	2	a					2		1	1		1	2	2	1	3	3		1				1		18
		b							1	2				2	1	2						1	2		11
		c						4			1			1	1	1							1		9
		d						1	1		1	4	1	1	1	1			2				1	1	15
	3														1								1		2
	4			1			2			1	1		2	1			3			1	1				13
	5				2	4							1		1				1						9
Total			1	1	2	4	4	5	4	5	3	5	6	7	6	7	6	0	4	1	1	1	6	1	80

Fig. 1.2. Chronological distribution paper's groups and sub-groups

The chronological distribution of information security management related scientific papers show active publication in period from 2001 till 2012, while a gap is noticeable in period from 2013 till 2018. During these five years just several scientific papers were published in topic, related to information security management. However, the information security management area becomes popular in the last years as the number of scientific papers increases.

1.3. Existing Information Security Management Frameworks

Currently, there exist a large number of ISM frameworks, proposed by scientists, universally accepted organizations, business companies, governmental initiatives for protecting information security and others. All these ISM frameworks concentrate on a specific domain or have its own point of view. The framework selection depends on many factors including industry sector and geography (EY, 2014). Therefore, in this section we will provide an overview of some relevant ISM frameworks to form a general view on existing solutions.

1.3.1. Overview of Information Security Management Frameworks

M. M. Eloff and S. H. von Solms (Eloff et al., 2000) proposed a hierarchical framework for various approaches consisting of three levels, where the top level of the hierarchical framework represents IT in its broadest sense and includes all activities and tools associated with and all approaches adopted to IT in general. This all-covering category is entitled Assessment of Information and Related Technologies. The second level is divided into two areas, namely Information Technology: General and Information Technology: Security. The area entitled Information Technology: General includes all IT activities and tools that cannot incur any security-related risks. The area entitled Information Technology: Security is divided into the areas entitled Technology and Processes. The area entitled IT: Security Processes is allocated to all IS management actions that should be performed; The area entitled IT: Security Technology is reserved for all the 'visible' aspects involved in IT security, such as the controls that are put into place to prevent possible damage by malicious software. The areas IT: Security Processes and IT: Security Technology is mapped onto the third level of the framework. Going down IT: Security Processes are divided into four terms (fourth level): (1) guidelines, code of practice, (2) standards, (3) legislation, (4) benchmarking. The area of IT: Security Technology consists of the same terms except for legislation, as it is replaced by evaluation. At the fifth level of the framework, some of the above conditions are subdivided further as being either internal or external. Internal guidelines are dictated by the specific in-house requirements of an organization. It should be noted, that in terms of the framework, international standards, as endorsed by an international standards organization, are classified as being external standards.

Denis Trček (Trcek, 2006) proposed an integral framework for information systems security management based on layered multipanes (see Fig. 1.3). The author declares that to protect the information, an organization has to start with the identification of threats related to business assets. Based on threats analysis, he proposed a layered multiplane approach. The first plane is focused on interactions, starting with security mechanisms and therefore, deploying security services, which are linked to human-machine interactions. Finally, human interactions have to be covered. Thus, in parallel, to make things operational, scientist proposes to address another perspective, which includes technological, organizational and legislative planes.

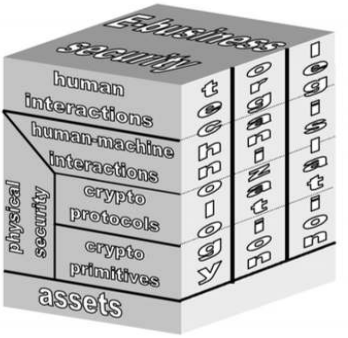


Fig. 1.3. Layered multi-panes model for information systems security (Trček, 2006)

Bradley and Josang (Bradley et al., 2004) propose an open framework for enterprise security management. This framework is intended to be a technology-dependent and comprises an information repository, manager programs, and configuration agents — the information repository stores network and security policy information. Manager programs are technology-domain-specific and act as expert systems querying the repository and communicate with configuration agents. Configuration agents provide the required expert system functionality. The study proposes a technical solution to information security management problem. Since the proposed framework is technology-dependent, it would not provide the type of flexibility that may be required in some instances.

John Sherwood, Andrew Clark, and David Lynas (Sherwook et al., 2009) represented the SABSA (Sherwood Applied Business Security Architecture) framework for Enterprise Security Architecture. SABSA is intended for developing risk-driven enterprise information security and information assurance architectures and for delivering security infrastructure solutions that support critical business initiatives. It is an open standard, comprising several frameworks, models, methods, and processes. The SABSA Model covers the life cycle of operational capabilities and shall consist of six layers. For each horizontal layer, there is a vertical analysis based on the six questions: What (assets)? Why (motivation)? How (process and technology)? Who (people)? Where (location)? When (time)? This leads to a six-by-six cell matrix called the SABSA Master Matrix. The sixth layer, the service management layer, is overlaid on the other five layers and further vertically analyzed to produce the five-by-six cell SABSA Service Management Matrix. Some of the key features of the SABSA are: it can be implemented incrementally, may be used in any industry sector and in any organization whether privately or publicly owned, can be used for the development of architectures and solutions at any level of granularity of scope, enables relevant existing standards to be integrated under the single SABSA framework, enabling joined up, end-to-

end architectural solutions, is continually maintained and developed and up-to-date versions are published from time to time.

SABSA is a generic architectural development framework that can be used for the operational-risk-based development and maintenance of operational capabilities in any business organization (Institute, 2014). It provides a holistic approach to information security and is baselined against the Security Architecture' standard ISO 7498-2:1989 (ISO, 1989). Five-layer SABSA framework answers the what, why, how, who, where, and when questions for security architecture. Five layers of SABSA are (see Fig. 1.4): Contextual Architecture, Conceptual Architecture, Logical Architecture, Physical Architecture, and Component Architecture. A sixth layer is added for Service Management Architecture and is synonymous with Operational Security Architecture.

Manuel Suter (Suter, 2007) introduced a Generic National Framework for Critical Information Infrastructure Protection (CIIP). CIIP is universally acknowledged as a vital component of national security policy. To protect their critical infrastructure, countries establish sophisticated and comprehensive CIIP organizations and systems, involving governmental agencies from different ministries, with a variety of initiatives. In the paper, the author offers a few building blocks for a functional CIIP unit and states, that by concentrating on top priorities, cooperation between various stakeholders, flexibility, and adaptability, relatively inexpensive solutions can be developed to meet country-specific needs. Essential tasks of CIIP author arranges in a "Four-Pillar Model." The four pillars of this model are Prevention and early warning; Detection; Reaction; and crisis management. While the aim of Prevention and early warning is to reduce the number of information security breaches; Detection aims to discover threats as quickly as possible, Reaction includes the identification and correction of the causes of disruption, Crisis management aims at minimizing the effects of any disorders. In the paper, essential partners of the framework, organizational structure of the CIIP unit are also discussed, as well as the case study provided.

Shuyuan Mary Ho (2008) represented a solution and procedures of coordinated defense. In the paper, the nature of attacks has been analyzed, and countermeasures of coordinated defense have been provided, the weakest link (the human element) in the layered defense has been identified. This paper contributes to the information systems security by providing a framework for approaching coordinated defense. It benefits research into information systems security by introducing the evolutional concept of coordinated defense. According to the author, his solution of a coordinated defense framework aims to protect information as assets by technologies, policy, and best management practices for defending against coordinated attacks.

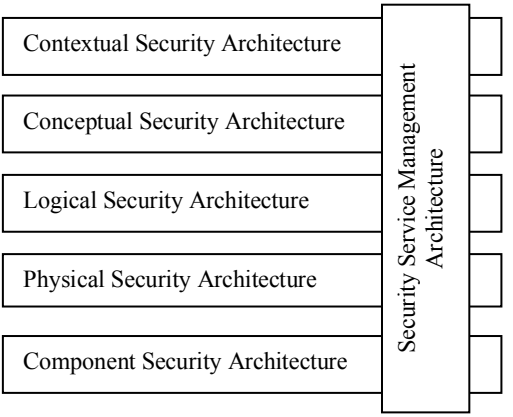


Fig. 1.4. SABSA model (SABSA Institute, 2014)

Also, it is noted that the framework forms unique characteristics of an information security culture for the organization. Layered defense covers all aspects of defense, including social and technical aspects. Building security mechanisms and infrastructure comprise the first layer of this defense strategy. Secondly, a fundamental "deny all unless specified" access control security policy is proposed for implementation. The third layer in the coordinated defense model should conduct infrastructure threat analysis and intrusion forecasts. The fourth layer in the coordinated defense model would be to monitor and detect intrusion. In the framework sensor technology at an infrastructure level, or systems level are built to identify and control activities. Besides, human (physical) activities could be monitored. Finally, an overarching layer of the defense emphasizes the resiliency and sustainability of the defense infrastructure, where the damage assessment and impact analysis lead to the rebuilding of recovery and response mechanisms.

Qingxiong Ma, Mark B. Schmidt and J. Michael Pearson (Ma et al., 2009) propose an integrated framework for ISM (see Fig. 1.5), in which ISM is conceptualized as a continuous decision making process. The rationale of this framework is based on four guiding principles: (1) have a goal in mind, (2) align security goals with business strategy, (3) ISM is a multivariate system, and (4) ISM is a dynamic process. Key components of the proposed ISM framework include the following steps: assess the organizational environment, establish information security objectives, analyze information security requirements, develop information security controls, and train/evaluate information security controls. The authors define ISM as a continuous improvement process intended to assure business continuity, customer confidence, and protection of business information assets and the minimization of damage to the business by preventing or minimizing the impact of security incidents. They declare, that the framework is beneficial because it serves as a common ground for integrating all types of information security

functions, helps answer questions of how to react to information security issues and it helps identify what the critical components involved in establishing and maintaining information security initiatives are.

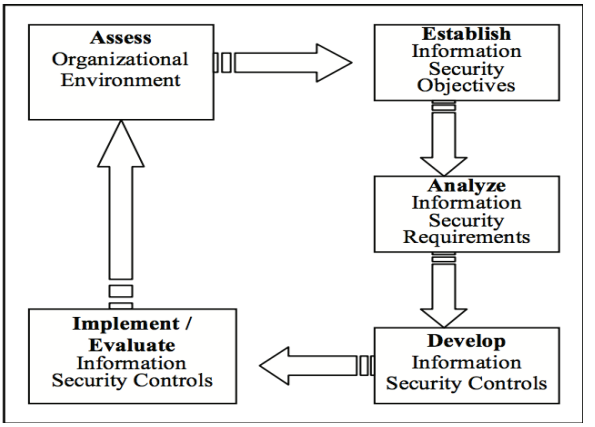


Fig. 1.5. Information security management framework (Ma, 2009)

An organizational-level process model in Information security policy was proposed by Kenneth J. Knapp et al. (Knapp et al., 2009). The model (see Fig. 1.6) suggests that a security governance program together with the organization's information security office, an ongoing process of interrelated policy management activities, and the proper gauging of critical external and internal influences together contribute significantly to the success of an organization's information security policies. The model provides unique value through its comprehensive, real world representation of an information security policy process in modern organizations. The data used in the development of the model is rooted in the broad based experiences of those who have been most active in developing and implementing organizational information security policies. Thus, this model provides a more complete, practice based framework that informs organizations and researchers concerning the interactions of critical processes and influences that form an effective information security policy process.

In the model, information security governance is an overarching category directly affecting the entire policy management process. The organization information security office is depicted as a category supporting the policy management phases. The internal and external influences are depicted as global influences on the entire policy management process. Internal influences include senior management support, organization culture, technology architecture, etc. External double arrows illustrate the two-way interaction between the policy management processes and the internal and external influences.

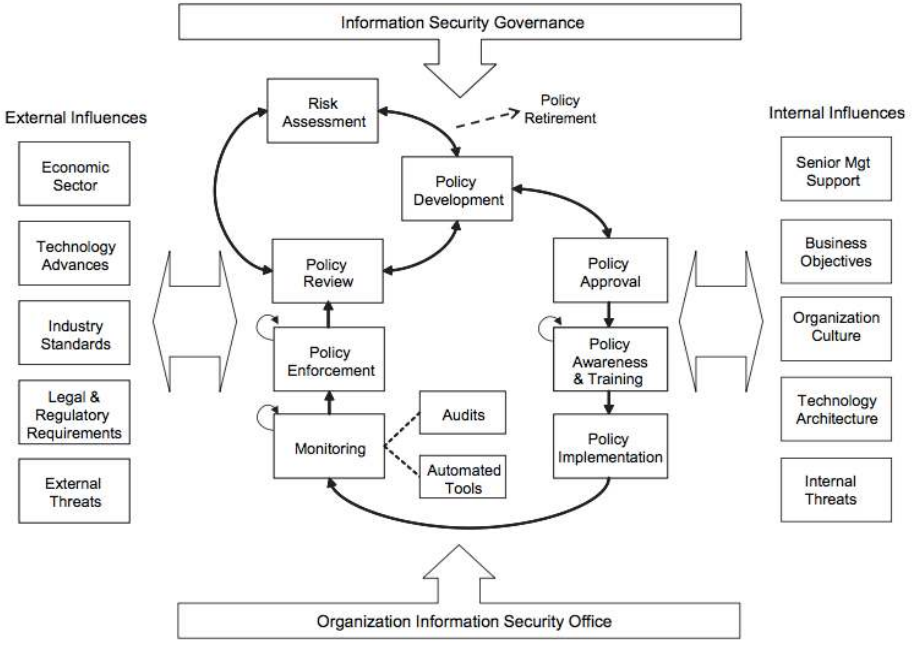


Fig. 1.6. Comprehensive information security policy process model (Knapp et al., 2009)

External influences include economic sector, industry standards, legal and regulatory requirements, etc. The central part of the model pictures the entire process of organization's security policy – it is a continuous cycle, affected by internal and external factors, where key elements are policy approval, training, implementation, monitoring, enforcement, review, risk assessment and, finally, policy development.

In September 2014, the Government of South Australia approved the Information Security Management Framework (Government of South Australia, 2014), which provides maximum coverage for control and risk management objectives by providing a wide array of risk management controls and is not purely mapped directly to the most recent standards publications, but refers to a suite of publications in order to provide government agencies with a comprehensive set of risk controls in order to appropriately protect their information and support their business undertakings. This framework references a set of policies, standards, guidelines, and control mechanisms for South Australian Government Agencies to use in developing their information security capabilities. It has been designed as a practical, useable framework, which can be implemented readily by South Australian Government Agencies and Suppliers to the Government of South Australia.

In 2018, Gaute Wangen et al. came up with a framework, that is dedicated to estimating information security risk assessment method completeness. A paper, representing the framework, proposes the Core unified risk framework as a comprehensive approach to compare different methods. All-inclusive since the Core Unified Risk Framework was grown organically by adding new issues and tasks from each reviewed method. If a task or issue was present in surveyed information security risk assessment method, but not in Core unified risk framework, it was appended to the model, thus obtaining a measure of completeness for the studied methods. The scope of this work is primarily functional approaches risk assessment procedures, which are the formal information security risk assessment methods that focus on the assessment of assets, threats, vulnerabilities, and protections, often with measures of probability and consequence. The proposed approach allowed for a detailed qualitative comparison of processes and activities in each method and provided a measure of completeness.

Romain Laborde et al. published (2019) a situation driven framework for dynamic security management. Authors present a dynamic security management framework where security policies are specified according to situations. Situation based policies easily express sophisticated vigorous security measures, are closer to business, and simplify the policy life cycle management. Situations are determined using complex event processing techniques. The framework is supported by a modular event based infrastructure where a dedicated situation manager maintains current situations allowing the command center to take dynamic situation–based authorization and obligation decisions. The whole framework has been implemented and showed good performance by simulation.

1.3.2. Comparison of Information Security Management Frameworks

To compare the surveyed frameworks, defined characteristics (features) had to be used. For this reason, we decided to use the logic modeling theory (ENISA, 2014) as the security strategy of the enterprise has the same principles as national cybersecurity is. ENISA presented a number of general and specific security objectives (ENISA, 2014), while we grouped them into five more abstract characteristics. All given frameworks were evaluated by the following defined characteristics: application of standards (C1), implementation or performance model provided (C2), whether the framework is a process (C3) or goal (C4) oriented, framework integration regarding different approaches and/or ISM levels (C5). C1 refers to application, implementation or reference to standards, such as ISO 27000 series, COBIT and others, into the framework proposed. For a successful framework adoption, it is essential to have in place all the steps, participants and relations among them; therefore, implementation or performance model (C2) of the

framework is among features in evaluating the ISM frameworks. Characteristics C3 and C4 are essential to discern whether the framework is developed for managerial purposes of organization whether to assure the main aspects of the information security – confidentiality, integrity, and availability. Value added is provided for the framework when one or more approaches (e.g., Plan-Do-Check-Act cycle, Command and Control system, etc.) are applied and different levels, from operations/service managing to international matters, are covered.

Thinking on the application of information security framework, it is important to have a high-level view as well as a detailed framework implementation specification. The high-level view gives a solution to understand the overall area of information system management while the individual level is needed to implement it in a real situation. However, to implement the framework successfully, the overall area understanding is a must. As well, it is important to consider a wide area as possible to introduce all potential stakeholders. Therefore, we add two more characteristics for the comparison of ISM frameworks: framework presentation in high-level abstraction concepts (C6) and different type of stakeholder presentation in the framework (C7). C6 is meet if the framework provides an underlying architecture of information security management framework which can be used for information security management area understanding. While "four Ps of Service Design" (Clinch, 2009) should have an analog in the ISM framework to meet C7.

We evaluated all overviewed ISM frameworks according to the chosen characteristics (does it apply (+) to the framework fully, partially (+-), or not apply at all (-)) and the results are presented in Table 1.1.

The results showed most of the analyzed solutions are internal level (organizational or information security system) ISM frameworks. This proves the idea there is a lack of ISM framework which would consider the versatility of nowadays enterprise, organization or system as relationships between different stakeholders are ignored.

During the comparison of analyzed information security management frameworks we noted some of the information security management frameworks could apply to a particular part of the organization, e.g., to the operational level, while others are intended to be used to the entire organization but in very abstract approach, not considering integration, partnership, external communication. In most cases it is high abstraction level frameworks, despites on the application area.

Table 1.1. A summary of Information security management frameworks' comparison results

Author	Framework	Purpose	C 1	C 2	C 3	C 4	C 5	C 6	C 7
1	2	3	4	5	6	7	8	9	10
M.M. Eloff1 et. al (Eloff, 2000)	Hierarchical framework for various approaches	Aims to unite and integrate issues of certification, benchmarking, guidelines, codes of practice, and IS management approaches widely accepted in the international arena.	+	-	+	-	+	+	-
Denis Trček (Trèek, 2003)	An integral framework for information systems security management	A layered, multi-plane approach based on the identification of threats to e-business assets, focuses on physical security and human interactions. Technological, organizational, and legislative perspectives are addressed.	+	+	-	+	+	-	+-
Bradley et. al (Bradley et al., 2004)	An open framework for enterprise security management	Aims to turn the black art of enterprise security management into a reproducible, automatable science.	-	-	+	-	-	-	-
John Sherwood et. al (Sherwood, 2005)	Sherwood Applied Business Security Architecture (SABSA)	Designed for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives.	+	+	+	-	+	+	-
Manuel Suter (Suter, 2007)	Generic National Framework for Critical Information Infrastructure Protection	Provides concrete solutions to meet country-specific needs in protecting critical information infrastructure by concentrating on top priorities, and cooperation between various stakeholders, flexibility and adaptability.	-	+	+	-	+	-	+
Shuyuan Mary Ho (Ho, 2008)	Coordinated defense framework	Aims to protect information as assets through the use of technologies, policy, and best management practices for defending against coordinated attacks.	+	-	+	-	+	+	+

End of Table 1.1

1	2	3	4	5	6	7	8	9	10
Qingxiong Ma et. al (Ma et al., 2009)	An integrated framework for ISM	Intended to serve as a common ground for integrating all types of information security functions. It helps answer questions on how to react to information security issues.	-	+	-	+	-	+	-
Kenneth J. Knapp et. al (Knapp et al., 2009)	An organizational- level process model	The purpose is to provide a more complete, practice based framework that informs organizations and researchers concerning the interactions of key processes and influences that form an effective information security policy process.	+	+	+	-	-	-	-
Government of South Australia (Government of South Australia, 2014)	Information security management framework (ISMF)	Among many objectives of the ISMF, the main is to support the attainment and realization of three information security objectives across Government: Confidentiality, Integrity, and Availability of information.	+	+	+	-	+	+	+

The balance between abstract level presentation and implementation step definition in achieved in Sherwood Applied Business Security Architecture (SABSA) model by John Sherwood, Andrew Clark and David Lynas (Sherwood et al., 2005) and Information security management framework (ISMF) by the Government of South Australia (Government of South Australia, 2014). These frameworks present a main architecture of the framework as well as provide guidelines for framework implementation. The difference between those two frameworks is application area as SABSA is organization oriented, while ISMF is government oriented framework. This makes ISMF harder to apply in small or even medium size organizations. Meanwhile, SABSA framework does not involve all 4 P's from ITIL (Clinch, 2009), which means it does not present enough wide organization security management area.

In overall, it can be said that analyzed ISM frameworks do not meet all depicted characteristics. Frameworks consider theoretical and conceptual approaches for managing information security, and there is a lack of attention, committed to ensuring the unimpeded and resilient process of ISM as some important stakeholders are not considered.

1.4. Research on Information Security Management in Lithuania

In 2015 National audit office in Lithuania released a comprehensive report on cybersecurity environment in Lithuania (Valstybės kontrolė, 2015). In this audit report, cybersecurity is viewed in a broader sense than in the Law on Cyber Security (The Law of the Republic of Lithuania on Cyber Security, 2014), and includes certain elements (security of electronic information, application, network, internet and other information infrastructure) covered by the standards of the International Organization for Standardization (ISO) and the recommendations of the North Atlantic Treaty Organization's (NATO) Cooperative Cyber Defense Centre of Excellence. As the report states, "up to 2015, development in the field of cybersecurity was based on legal acts that did not clearly define the institutions responsible for shaping and implementing cybersecurity policy, the duties and responsibilities of the parties involved in cybersecurity, or organizational and technical requirements for cybersecurity and measures for ensuring cybersecurity. At the end of 2014, essential changes were made to cybersecurity regulation: The Law on Cyber Security6 was passed, detailing how to set up, manage and control the national cybersecurity system and defining cybersecurity terms and other related concepts." The purpose of the performed audit was to assess whether cybersecurity is being ensured in Lithuania, whether an effective cybersecurity system has been set up and cyber security is ensured in public establishments.

In the report National audit office came up with the conclusions, that (i) in Lithuania, the areas of cybersecurity and electronic information security are governed by separate laws, however, implementing them is not an easy task, and the general public security level in these areas has so far not seen significant improvement; (ii) The implementation of technical and organizational measures for cybersecurity and electronic information security in the public sector is insufficient, and establishments are not adequately prepared to react to potential cyber threats.

Information security management in Lithuania was analyzed in-depth by S. Jastiuginas. In 2012 an article “Integral Information Security Management Model for Lithuanian State Institutions” was published (Jastiuginas, 2012). In the article, the author asserts, that for a long time the technological solutions of research problems have dominated, but lately more relevant have become the human, economic and other issues, and there is a need for a more managerial approach. The article discusses the empirical study as a theoretical integral information security management model that could be applied in practice.

In his works (Matulevičius et al., 2010; Altuhhova et al., 2012; Pullonen et al., 2017; Matulevičius, 2017) R.Matulevicius demonstrate results of a comprehensive analysis of business process modeling regarding information security requirements. The author proposes PE-BPMN – privacy enhanced ex

tensions to the BPMN language for capturing data leakages. It should be noted, that models proposed are related to the software development over the new approaches of information security management.

Other information security scientists in Lithuania develop significant researches that are targeted at the security of software development as well:

- R. Rainys researches we tied up to computer network infrastructure (Rainys, 2006; Kajackas et al., 2011);
- N. Goranin proposed a genetic algorithm based model for estimating the propagation rates of known and perspective Internet worms after their propagation reaches the satiation phase (Goranin et al. 2008);
- S. Ramanauskaite proposes a composite denial of service attack model that combines bandwidth exhaustion, filtering, and memory depletion models for a more realistic representation of similar cyber attacks (Ramanauskaitė et al. 2015);
- J. Janulevicius performed analysis of virtualization and risk assessment (Janulevičius et al., 2017);
- Several scientists under M.K. Ragulskis leadership performed an in-depth analysis of cryptography. Research results were published in several articles (Ragulskis et al., 2007; Palevičius et al., 2015; Petrauskienė et al., 2014).

Summarizing, it can be stated, that among Lithuanian researchers, there is a significant interest and absorption of the information security topic. Though no new approaches or solutions for information security management were spotted.

1.5. Conclusions of the First Chapter and Formulation of the Objectives of the Thesis

The first chapter of this thesis provides an overview of information security management principles and existing research in this area. More significant concentration is dedicated to the analysis of existing information security management frameworks to define the missing elements. The following conclusions have been drawn:

1. The systemic analysis of scientific papers in the field of information security management revealed the majority of the papers in the period from 1998 till 2016 were written on the topic of risks and solutions in organizational level. The importance of this topic in scientific society shows the importance of this problem and a variety of different issues as well as solutions;
2. Existing information security management frameworks were compared according to 7 criteria. The comparison proved there is no one superior framework, able to cover all information security management related

areas. Therefore, a new, more holistic information security management framework is needed to concentrate all SME needed information security management relevant information;

3. Analysis of information security management framework revealed there is no information security management framework, where all main stakeholders would be included. The lack of broader information security management framework perspective does not allow a more realistic understanding of the situation.

Based on the conclusions, the following tasks are formulated to achieve the goal:

1. To design a new information security management framework which will combine high-level processes and stakeholders of ISM;
2. To improve the applicability of proposed information security management framework, by providing a list of associated tools to automate or simplify the framework usage in SME;
3. To evaluate the proposed ISM framework and tools as information security management improvement solution in small and medium enterprise.

2

Proposed Information Security Management Framework

In this chapter, the new information security management framework is presented. The Information security management framework defines and extends stakeholders' categories based on existing categories, by considering missing and influencing the ISM process categories. The construction of the proposed ISM framework is based on military C2, PDCA, and other paradigms. While for more straightforward adoption of this framework, a list of questions is presented close to the framework. Each question in this questionary is dedicated to analyzing a specific area of the framework, and a list of tools is given for each question to help to answer the question or to improve the situation. All idea of the framework, as well as its details, is described in this chapter. However, we were not able to find a tool for modeling or evaluation the security of enterprise management security; therefore, a need for information flows security modeling tool was identified in this chapter too.

Analysis presented in this Chapter was published in (Kauspadiene et al., 2017).

2.1. Idea of Information Security Management Framework

The second generation (Solms, Information security management: The second generation, 1996) ISM framework must consider the nature of nowadays enterprise. Today business has multiple partners, uses collaborative systems, outsourcing, and other third parties, which requires a broader view into organization security management. S. B. Maynard et. al (Maynard et al., 2011) identifies 9 stakeholder categories in organization security policy development while European security Trends and Threats In Society (ETTIS) (European security trends and threats in society, 2012) uses the broader concepts of security and identifies 7 stakeholder categories in global security area. We used a classification of 7 stakeholder categories (see Table 2.1) to define high-level stakeholder categories, which acts in today's enterprise and have to be considered to ensure organizations security.

Table 2.1. High-level Information security management framework stakeholder categories and its relation to organization oriented and global security oriented stakeholder taxonomies (invented by authors)

Stakeholders Category	Description	Interest/ Responsibilities	S. B. Maynard Category (Maynard, Ruighaver, & Ahmad, 2011)	ETTIS Category (European security trends and threats in society, 2012)
1	2	3	4	5
Corporate governance	Ensuring the security of critical infrastructure	Critical infrastructure security	Business Unit Representatives	Think tanks
Legislative bodies	Ensures Cyberspace monitoring	Cyber space monitoring	Legal & Regulatory	Government
Professionals	Ensures the management of information security in a system level	Information security management	ICT Specialists; Security Specialists	Industry
IT Enterprises	Enterprises, that provides physical infrastructure	Physical infrastructure		

End of Table 2.2

1	2	3	4	5
Developers Academia	Software development Prepare expertise human resource for performing the processes of information security management	Software Human resources	Executive Executive Management; Human Resources	Academia/ research institutions
External parties	Collaborates with the organization, by changing different information, tools, services, etc.	Information and resource exchange	Public Relations; User Community; External Representatives	Civil Society Organisations; The media; The public

Most ISM frameworks have no list of default stakeholders and require identification of stakeholders as every situation can be unique and require a different type of stakeholders to include. However, this approach is stakeholder identification knowledge and practice dependent. If one or more important stakeholders would be missed, the final security management result can be crucial as this is a base for other information security management elements. Our proposed approach has 7 top level stakeholder categories, which can be divided into smaller, more specific ones. Therefore, the stakeholder identification, specification process starts from these high-level categories to think of and leads to lower probability to miss some important stakeholders.

The proposed framework has needed information security management components too. In Fig. 2.1, essential elements in performing information security management are shown. It is a matter-of-course that the continuous and resilient processes are the gist of information security management performance.

Information security management processes are performed by professionals – an expertise human element, e.g., CISO (Chief Information Security Officer), that are prepared by academia and science institutions. This is the core of the proposed framework as presents the organization level. The organization has multiple processes (internal as well as external), which are the engine of the company. The organization enables a command to manage and installs a control to perform monitoring of these processes. For continuous development, best-practice-based processes optimization should be organized. However, all innovations and optimizations have to be audited and confirmed by certain control to meet

organization needs, regulatory compliance, and security requirements. All the production (or services the organization provide) is dependent on organization, processes and optimization elements, while command and control (C2) denotes the set of organizational and technical attributes and processes by which an enterprise marshals and employs human, physical, and information resources to solve problems and accomplish tasks (Vassiliou, M., 2015). Military system C2 should be applied for the monitoring and management of the processes (see Figure 6). This is required as the human factor is the weakest link of any security system, and the biggest attention in security management should be given to the processes, performed by people. Cyber warfare command and control system demonstrates that defense in-depth can be taken to a new level that is active and anticipatory rather than passive and reactive (Howes et al., 2004).

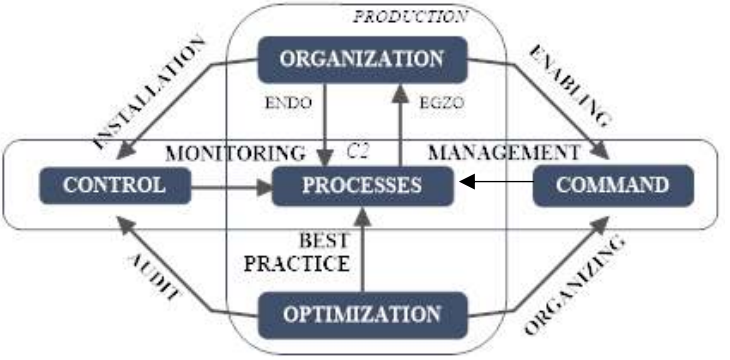


Fig. 2.1. Core elements (organization level) of HISMF (invented by authors)

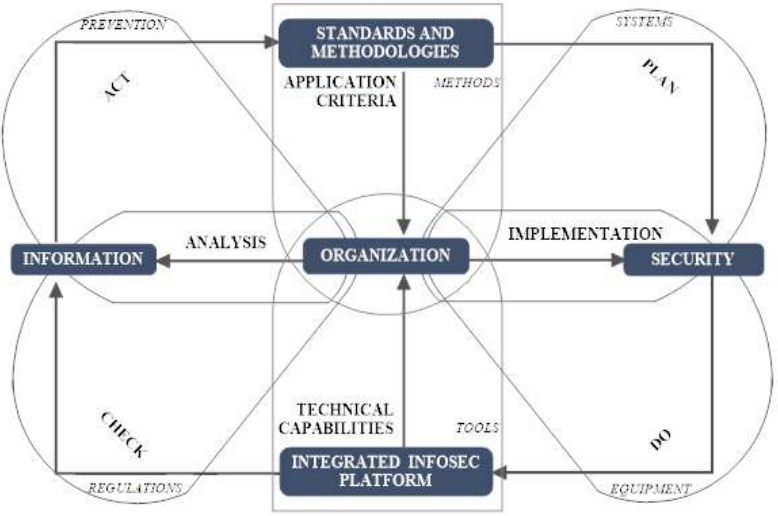


Fig. 2.2. Main components of organization security level (invented by authors)

The Deming cycle Plan-do-check-act (PDCA) is another approach which was integrated as a must in the framework (see Fig. 2.2). Based on application criteria, specific standards and methodologies should be applied to the ISM of the organization (Methods section, Fig. 2.2). According to security standards and technologies, security actions are planned and later integrated into the information security platform. The information security platform is a set of physical tools used for information security implementation. Usually, the information security platform depends on organizations technical capabilities and professionals, which are capable of using those tools correctly and of obtaining clear evidence on the efficiency of implemented security tools. This includes an analysis of organization information, its compliance to specific controls, and acting according to a particular situation, defined in standards and methodologies.

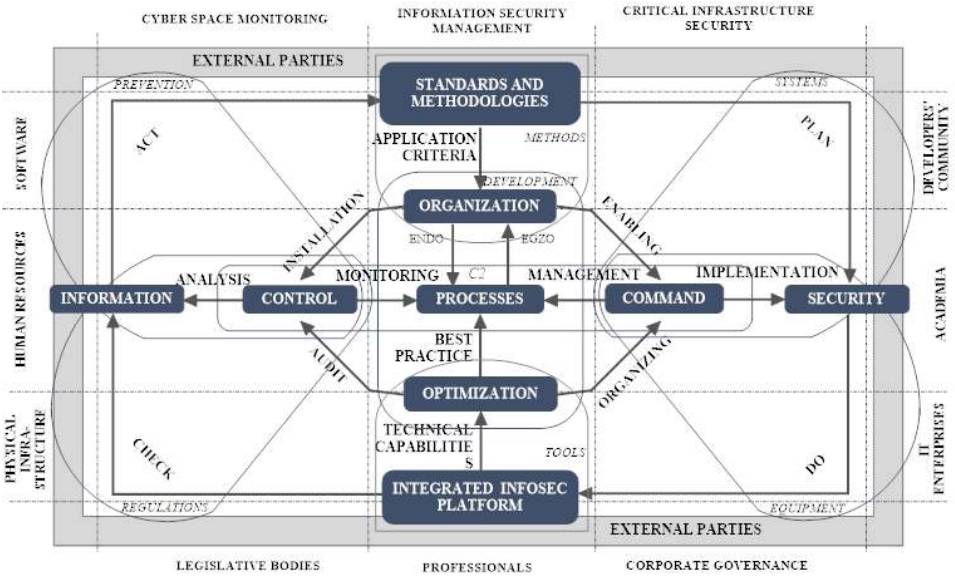


Fig. 2.3. High-level self-sustaining Information Security Management Framework (invented by authors)

To understand the relations between components of organization security level and ISM shareholders and responsibilities or functions they perform (see Table 2.1), four additional sections are identified (Fig. 2.3): (1) *prevention* is done by cyber space monitoring in the software level, according regulations, issued by the legislative bodies, and involves control and information elements, as the control of information plays one of the major roles in IS prevention, weather it is data leakage, fraud, etc.; (2) *regulations* are issued by legislative bodies and implemented at the cyber space monitoring and physical infrastructure levels, and involves control and information elements due to ensure processes compliance to

national as well as international law (personal data protection, audit procedures, laws of cyber space, etc.); (3) *systems* (at the software level provided by the developers community) and (4) *equipment* (at the hardware – physical infrastructure , provided by IT enterprises) serves to the corporate government by assuring the security of critical infrastructure, whereas the security is implemented under the commands given by organization.

When the organization is growing, the continuous improvement loop – PDCA cycle – turns around bringing new informational security management challenges that influence stakeholders' demands. To provide more specific guidance, we mapped the PDCA cycle to security level as well as associated all elements of the HISMF to particular top-level stakeholder category or its responsibility (Fig. 2.3). As external parties can be of very different type and purpose they can act in different responsibility areas, however, they should be treated as external level and separated from the organizational or even security level. Therefore, partners are linked to the elements of standards and methodology, security, integrated security platform, and information.

Self-responsive cyber security network, generated by the High-level information security management framework, is based on five resilience principles (Vries, 2010): self-merging, robustness, viability, flexibility, and interoperability. Instructional design of self-sustainable components of high-level information security management framework is arranged to form a self-organizing system. Self-refreshingness on demand, based upon distributed stakeholders' initiative, enables the system to self-awareness.

The high-level information security management framework represents a broader approach to collaborative information security network defense. This framework represents security processes demystification paradigm, based upon embed systems participate development. Four sections of the model correspond to a viable, resilient cyber security system that is based upon the inter-linked participate network. Cybersecurity demand is fulfilled in this system as a co-working crowd source-based IT system integration pattern in complex self-repellent environment. Various challenges, as the provision of skills and competencies, are conglomerated as general PDCA model acts upon the supervision of framework stakeholders' superiority. Superior forces of self-referencing development of technological capabilities are fulfilled by using foremost open-source tools of self-referring standards that are proclaimed as best practice-based knowledge assets.

The framework provides a new approach to organization informational security management challenge and can be suitable for any organization. Emerging organization growth is considered in high-level information security management framework – processes are controlled on demand using C2 paradigm, utilizing the PCDA cycle collaborate stakeholders grid efforts.

2.2. Guidelines for Application of Proposed Framework

The proposed ISM framework defines important requirements to ensure security. This is very useful when the enterprise is newly established, and its structure, policies might be changed. As well the proposed framework concentrates all needed information into one framework; therefore, it is suitable for SME as not enough resources can be assigned to gather all required information from different or very detailed sources. Meanwhile, if existing SME has its structure and management policies, it might be necessary to evaluate how close the enterprise is to the proposed framework. Therefore, a questionary was developed to serve as a checklist both for newly designed ISM structure as well as evaluating the current situation.

For the high-level information security management framework readiness evaluation self-assessment sheet based on methodology, developed by information technology promotion agency (Japan), is presented. This self-assessment sheet is one component of the overall cyber security picture. This self-assessment cannot reveal all types of information security weaknesses, and additional means of determining an organization's security management situation should be used. However, it is dedicated to highlighting the need for change in the ISM.

The user of this self-assessment sheet must go through all questions (see Table 2.2.) in the questionary and answer by selecting the answer "Yes," "No," "Partially" or "N/a" (not applicable). The answer "Yes" indicated the area, covered within the questionary is suitable in the SME, while other responses indicated the area should be inspected additionally. As well existing tools are listed to each question to suggest the answer or take some additional actions to change the situation.

As mentioned above – the self-assessment sheet is not dedicated to evaluating the security level. It is more oriented to identification of areas, which require more in-depth analysis. The self-assessment sheet should be used as a checklist for information security management as the questions, and elements will show whether the SME is covering the area and if they are not, they will have a set of tools, dedicated to doing so.

For each question, a tool for answer deriving or situation modification was selected. The tools will help the person to derive objective answers rather than based on personal opinion. However, one additional problem was noticed – there are no tools for evaluation of SME management security (there are tools for process modeling in terms of cost, time and other criteria; however, no security measures are indicated).

Table 2.2. Proposed self-assessment sheet, used as a checklist in information security management process

No	Question	Yes	No	Partly	N/a	Tools
General						
1.	Does organization install clearly documented control and command enabling mechanisms?					Controllers checklist for data protection self assessment (Information Commissioner's Office, 2018)
2.	Does organization monitor all processes?					SOLVE (Conventus, 2018)
3.	Does organization execute audits on control mechanisms?					NMAP (NMAP, 2018)
4.	Does organization apply best security practices and standards?					ENISA (Manso et al., 2015)
5.	Does organization optimize management and operational processes?					**Not found**
Management						
6.	Does organization apply PDCA cycle for ISM?					PDCA Checklist (HIMMS, 2018)
7.	Does organization have clear security regulations?					ISO/IEC 27001 for SMEs (Valdevit et al., 2009)
8.	Does organization apply prevention mechanisms?					Information Security Risk Assessment Checklist (Argi Business Insurance Services)
9.	Does risk analysis is executed in the organization?					CORAS (Fredriksen et al., 2002)
Technical						
10.	Does organization have enough technical capabilities to operate?					NetworkAlliance (NetworkAlliance, 2018)
11.	Does organization ensure the IT (software, network, etc.) security?					CySeMoL EAAT (Rabbani, 2016)
12.	Does organization uses needed physical infrastructure?					Information Security Physical & Environmental Protection Standard (State of Minnessota, 2010)

Typically, an expert is used to evaluate the situation and propose some improvements. This makes the optimization of management processes complicated. Therefore, a simplified tool or tools for SME management security modeling would be valuable to increase the SME security level.

2.3. Conclusions of the Second Chapter

1. The proposed information security management framework provides an evolutionary approach to organization informational security management challenge and can be suitable for any organization, particularly for SMEs, as none of the existing and analyzed frameworks meet the features, that are necessary for nowadays organization ensures its security. Therefore, all needed knowledge in one framework can reduce the time, needed to find and gather it from different sources.
2. The proposed framework is adapted to cover emerging organization growth as processes are controlled on demand using the Command and Control paradigm, utilizing the Plan-Do-Check-Act cycle collaborate stakeholders grid efforts.
3. In the framework, there are defined stakeholders of a whole system of Information security management. Stakeholders are: Legislative bodies (ensure cyberspace monitoring), Corporate governance (ensure the security of critical infrastructure), Universities (provision of expertise human resource), IT enterprises (provides physical infrastructure), Professionals (management of information security in a system-level) and Developers' community (software development), External parties (all external communications). These stakeholder categories ensure a wide area of information security management will be analyzed by leaving no space for stakeholders influence no estimation.
4. The High-level information security management framework can serve practitioners as guidelines for the development of an overall information security plan or program in their organizations as associated tools are provided to make sure its smooth implementation in SME.
5. High-level information security management framework distinguishes from existing solutions by its integration of the important information security management paradigms and the defined stakeholders' list and its interactions.

3

Information Security Evaluation Models for Small and Medium Enterprise

To execute ISM, some tools can be useful as they allow the automation of some complex tasks or works as decision support systems to get more suitable decisions. In this chapter, existing information security evaluation and/or modeling tools are analyzed, and a lack of solutions in strategy and organization perspectives is missing. Based on the tool analysis and previous analysis of existing ISM frameworks, a list of models, dedicated to model and evaluate information security level in organization perspective and structure aspect are presented. The new models are proposed to cover the most important areas of ISM and are dedicated to getting the data leakage, data availability, and data integrity levels for different information flows, objects in the organization. The models are based on probability theory and consider the enterprise management structure, hardware, and software related metrics as well as human error factors. While hardware and software associated metrics are used in multiple tools, human based factors are poorly analyzed in information security modeling and evaluation tools.

The analysis and research presented in this chapter was published in (Kauspadiene L., 2018).

3.1. Analysis of Information Security Evaluation Tools

Enterprise analysis and modeling have tools developed to optimize enterprise operating properties and give advantages compared to competitors. Enterprise modeling covers an extensive area and enables to "use multiple, interrelated views to describe the properties of an enterprise system and its surrounding environment" (Atkinson, 2015). Ulrich Frank (Frank, 2014) states that multi-perspective enterprise modeling has three perspectives – strategy, organization, information system. They can be modeled in four different aspects – resource, structure, process, goal (see Fig. 3.1). Combining these perspectives and aspects produces 12 different enterprise modeling views.

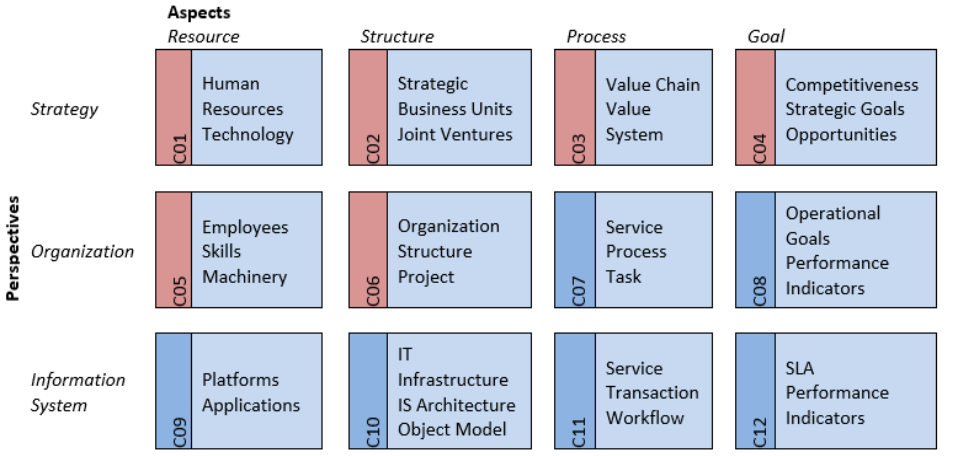


Fig. 3.1. High level enterprise security modeling perspectives and aspects (U. Frank, 2014) (red notated views are lacking models in terms of security while blue notated views already have such models)

U. Frank's model is not a limit to the scope of enterprise modeling views. Previously, security was considered to be a separate modeling area. However, modern tendencies indicate that a precise security evaluation is interdisciplinary. Therefore integrating (Ekstedt, & Sommestad, 2009) it as a part of enterprise modeling is a more promising approach, as enterprises heavily rely and sometimes are based on IT. Existing security models are used for enterprise modeling in the perspective of information systems. As one of the examples to illustrate this comes to a new approach to use attack–defense stochastic game Petri nets (Wang et al., 2013) to model enterprise network to analyze its security issues. Therefore, it

covers resource (C09) and structure (C10) aspects of information system perspective in enterprise modeling. Petri nets provide security related metrics for more in-depth analysis; therefore, risk assessment models (Aa-gedal, Den Braber, Dimitrakos, Gran, Raptis, & Stolen, 2002) can be used to get risk assessment results. Another approach – the Cyber Security Modeling Language (CySeMoL) (Sommestad, Ekstedt, & Holm, 2013) is designed for enterprise level system architecture analysis. Using attack trees (Holm, Shahzad, Buschle, & Ekstedt, 2015) to describe the attack scenarios defines the risk probability for each component in the designed model. Combining these features with visualization possibilities (Ekstedt, Johnson, Lagerstrom, Gorton, Nydren, & Shahzad, 2015) simplifies the analysis of the security situation as well as the presentation of the situation to the non-IT executive staff. Moreover, the approach enables automated model creation based on scanning (Buschle, Holm, Sommestad, Ekstedt, & Shahzad, 2011) the scan logs of infrastructure security software products. Various security models exist for modeling enterprise from the perspective of information systems. As the IT usage in enterprise evolves, new security models, including cloud computing (Kazim, & Evans, 2016) are developed to meet the needs of an enterprise. However, organizational and strategic perspectives of enterprise modeling in terms of security are not as advanced.

UML notation has several extensions for security oriented process modeling: UMLsec (Jurgens, 2002) adds a security related notation to UML diagrams; however, it does not provide with the process security level metrics. Moreover, it is strictly related to the security of an information system. The development of a more detailed process security analysis for the UMLsec requires the usage of additional components. In this case, BPMN (Rodriguez, Fernandez-Medina, & Piattini, 2007; Altuhhov, Matulevicius, Ahmen, 2013) can be a favorable solution.

In terms of the role assignment and management process, another extension – SecureUML (Lodderstedt, Basin, & Doser, 2002) exists. It provides a well known tool for RBAC implementation. Moreover, additional models for rode design (Pistoia, Fink, Flynn, & Yahav, 2007), privacy ensuring in role assignment (He, & Anton, 2003) are useful for the enterprise modeling as well.

However, there is a lack of alignment between structures and processes of information systems and organizations (Danesh, Loucopoulos, & Yu, 2015). The enterprise strategy and structure does not address security issues with enough focus. P. Michelberger et al. (Michelberger, & Labodi, 2012) proposes a holistic and process centered enterprise security model; however, there are no suitable tools to model all components of the framework. Different aspects of IT security at different levels of abstraction, including the entire lifecycle of IT security systems (Goldstein, & Frank, 2016) have to be considered for deep modeling of security in enterprise analysis.

Infowatch global data leakage report (Global data leakage report 2015) specifies that the number of data breaches shows an annual increase. Recent research data stress the importance of human behavior within the enterprise for enterprise security (Evans, Maglaras, He, & Janicke, 2016). However, statistical comparison of years 2016 and 2017 (Infowatch 2017) show the increase of accidental data leaks by 36.9%. This means that almost half of data leakages occur with loyal employees and no external attacks. Data leakage occurs due to non-existent data monitoring, data leakage prevention systems (Wuchner, & Pretschner, 2012) and insufficient security policies (Data Leakage Worldwide: The Effectiveness of Security Policies, 2014).

This thesis proposes a model for enterprise management structure in terms of information security (confidentiality, availability, and integrity). The model takes into account the enterprise management, as well as data flow environment properties. The model is oriented towards the management instead that technical features of the enterprise, therefore covers the view, which is missing in enterprise security modeling.

3.2. Proposed Information Flow Security Evaluation Model

A typical information flow security analysis is performed at the level of implementation of hardware and software. The human factor is ignored in most cases. However, in practice, human error is one of the weakest links in the enterprise security (Streeter, 2013). Typically, the foundation of an enterprise structure is designed according to business needs with no attention to its security metrics. The structure might be modified later, according to requirements of implementation and continual improvement security standards and best practices (e.g., ISO 27001 and 27002, NIST 800-53, PCI DSS, etc.). Meanwhile, the presence of enterprise data security models would allow designing an enterprise with initial security in mind, thus allowing analysis and monitoring of the current structure.

Bell-LaPadula model (Bell, & LaPadula, 1973) is the most known security model, defining the rules for data confidentiality. Although there are arguments about the security of Bell-LaPadula model (McLean, 1985), it is supported by military organizations, used as the base for improved, up to date security models (Balamurugan, Shivitha, Monisha, & Saranya, 2015). It is based on a principle to assign different security levels to objects and subjects, appended by the policy for subject to write data to higher or the same security level objects while reading lower or the same security level objects. Although this model can be adapted to vertical hierarchy management structures, modern enterprises tend to have more complex management and information flow structures. This complicates the adaptation of the Bell-La Padula model.

The security levels of our proposed model are represented by the concept of "subordination flow." It defines the governable nodes of the enterprise and the ones with the duty to provide information. The subordination flow has to be provided according to the management policies of the enterprise.

Using the subordination allows the definition of the difference in security levels of the governable node compared to the superior node. The relative security level does not require predefined security classes, therefore allowing the modeling of situations when two departments of the enterprise have control over each other in different areas. An example of the model notation with two-directional subordination flows is presented Fig. 3.2. In this case, the government requires specific accountability from the enterprise; the head of the enterprise dedicates the task to the Finance department (one person in this example); the head of the enterprise defines the strategy of the enterprise and presents it to the management department; the management department is the center node, which coordinates the work between enterprise clients, designers, programmers and IT administrator; clients contact the management department (no specific person) with initial requirements, while management department responds to a particular client by providing the project details, price, and other questions; there is no subordination flow between the client and the management department; the management department commands the IT administrator to get certain IT services for the client; management department shares new project ideas with design and programming departments; when a responsible person from the design and programming department is assigned to execute the project, these persons communicate with the appointed manager from the management department to get more details and present the designed products; the programmer has a right to contact the project designer and to require additional design elements; the programmers can request specific IT services from the IT administrator to implement the fully functioning project so the IT administrator may send login information for the project IT services etc.

The description of the analyzed small website development enterprise management structure and information flows requires a long explanation. It can become even more complex when dealing with a medium or big enterprise. Meanwhile, the notation used in Fig. 3.3 provides the elements (departments and positions, persons in the enterprise) and basic subordination and information flow directions as well as the type of the flow (dedicated to one person in the department or all persons in the department). Even more details are planned to be provided by an interactive tool for each of the node and the edge.

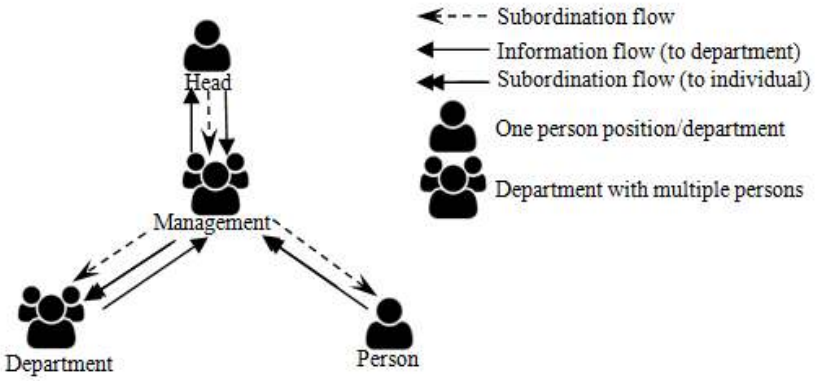


Fig. 3.2. Example of management structure in a small enterprise

The meta-model of the enterprise management structure is provided in Fig. 3.3. It consists of four main classes:

1. ManagementNode object indicates an element of the enterprise management structure. It can be an individual or a department. Depending on the type of the ManagementNode, additional information is required for specification of the number of persons in the department, person's position in the enterprise, etc.;
2. SubordinationFlow connects two ManagementNodes and provides information on which management node is superior and which is governable;
3. InformationObject defines the information object, which will be sent or managed by the enterprise. The InformationObject object is associated with SubordinationFlow object to define by which command the information could be sent. If there is no SubordinationFlow objects for the InformationObject object, the model assumes there is no policy, which specifies the initiator of the necessity to provide information flow. Each InformationObject object can be composed of multiple other InformationObject objects. This illustrates situations where information can be composed, filtered, generated or just stored as it is;
4. InformationFlow object defines the transfer of information from one ManagementNode to another. During the transfer, some information has to be sent; therefore, one of InformationObject objects from the sending ManagementNode objects have to be specified. The data leak depends on the transfer environment. The model defines three main types of transfer environments: DirectCommunicationData that represents data transfer during a vocal conversation; DigitalData that represents data transfer using network communication; and PlysicalData that represents data transfer when information is written to some external device or printed, varying depending on the situation. The specification of InformationFlow

types is necessary as each type of transferring environment has its characteristics. They include data format, protocol, delivery service, communication environment publicity, etc.

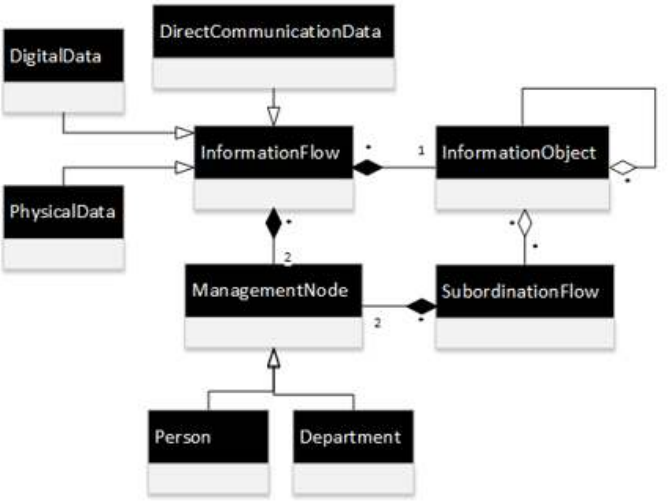


Fig. 3.3. Basic meta-model structure for enterprise management structure modeling

The meta-model allows tracing of information flow from one node to another. The visual model notation does not provide the information on Information Object operations or information flow. However, meta-model analysis can provide the flow path and information flow structure (composition or share data of different information flows).

The best way to analyze security risks is to analyze information confidentiality, availability, and integrity separately. This separation of different aspects can be used for various type organizations. For example, some organizations might collect publicly available data and publish it to the public. This kind of organizations requires information availability and integrity to be ensured, while the data confidentiality is not important (at least not for all data).

3.3. Estimation of Data Leakage Probability

The most intuitive metric to express data leakage is data leakage probability. The data leakage probability may vary for different nodes on the enterprise. This is caused by the individual characteristics of each information transfer, including different departments and employee, the number of subjects the information is shared with, etc. When the information flow path is known, the probabilities of data leakage in each of the nodes $P_{Cn}(n_i)$ can be defined, evaluating each transfer between enterprise nodes $P_{Ct}(c_i)$. The probability of at least one leakage to happen

$P_C(f)$ can be evaluated using equation 3.1. Evaluation of a leakage in the information flow path means that the data confidentiality is compromised if at least one person with no privileges to read the data gets access to it.

$$P_C(f) = 1 - \left(\prod_{i=1}^{N}(1 - P_{Cn}(n_i))\right) \cdot \left(\prod_{i=1}^{M}\left(1 - P_{Ct}(c_i)\right)\right). \quad (3.1)$$

In Eq. (1) there $P_C(f)$ is the probability of information flow f to be leaked in at least one of nodes or transfers; N – number of nodes in the information flow path; $P_{Cn}(n_i)$ – the probability of the node i to leak data; M – number of transfers in the information flow path; $P_{Ct}(c_i)$– the probability to leak data during the data transfer i.

3.3.1. Estimation of Probability to Leak Data During the Data Transfer

The probability of data leakage during the data transfer is estimated according to the technical data. Based on the data transfer technologies, existing vulnerabilities are identified. For each of these vulnerabilities the confidentiality impact C and likelihood L can be estimated and multiplied. In this version we use simplified data leakage probability for data transfer estimation. This method relies on National Vulnerability Database (National Vulnerability Database, 2018) (NVD) for vulnerability identification and uses modified base score value BS of Common Vulnerability Scoring System v3.0 (Common Vulnerability Scoring System v3.0, 2018) (CVSS). To get the probability of data leakage during the data transfer base score BS is divided by 10 to get the probability of the vulnerability and calculate the probability of at least one vulnerability to be exposed to the channel (see equation 3.2). This probability is multiplied by probability of the organIization to be attacked from the outside P_r(r) and probability of the channel to be accessible to an external attacker $P_a(a_i)$. The probability that the organization is be attacked from outside $P_r(r)$ is based on statistical data. For example, 55% of large enterprises and 33% of small enterprises were attacked by an unauthorized outsider in 2014 (Information security breaches survey 2014). Meanwhile the probability that channel i is be accessible to an external attacker $P_a(a_i)$ is estimated by modeling the certain enterprise IT architecture.

$$P_{Ct}(c_i) = 1 - \left(\prod_{j=1}^{K}\left(1 - \frac{BS_j}{10}\right)\right) \cdot P_r(r) \cdot P_a(a_i). \quad (3.2)$$

In Eq. (3.2), there BS_j is modified CVSS base score for vulnerability j; K – the number of vulnerabilities for transfer channel i; $P_r(r)$ – attack probability against this type of enterprise; $P_a(a_i)$ – channel i accessibility by external attacker.

The same method and metric values as CVSS v3.0 is used for the modified base score estimation. The only difference is in base impact subscore ISC_{Base} estimation – rather than using the probability of at least one of confidentiality, integrity and availability to occur (see equation 3.3), only confidentiality impact value is used (see equation 4).

$$ISC_{Base} = 1 - \left(\left(1 - IMP_{conf}\right) \cdot \left(1 - IMP_{Integ}\right) \cdot \left(1 - IMP_{Avail}\right)\right). \quad (3.3)$$

$$ISC_{Base} = IMP_{conf}. \quad (3.4)$$

In Eq. (3.3) and (3.4), there IMP_{conf} is confidentiality impact value; IMP_{Integ} is integrity impact value; IMP_{Avail} is availability impact value.

3.3.2. Estimation of Probability to Leak Data by Enterprise Node

The estimation of data leakage probability at an enterprise node, be it person, department or a group of persons, relies on human factors rather than only IT specifications. Five main threats are taken into account for enterprise node data leakage probability estimation. Each threat is associated with data leakage likelihood values *nl*. Therefore, enterprise node data leakage probability is equal to the probability of occurrence of at least one of human error (refer to equation 3.5).

$$P_{Cn}(n_i) = 1 - \left(\prod_{j=1}^{\tau}\left(1 - nl_j \cdot conf\right)\right). \quad (3.5)$$

In Eq. (3.5), there nl_j is data leakage likelihood value for threat j; *conf* – employee confidentiality level coefficient for node i; τ – the number of relevant threats for node i.

Equation 3.5 facilitates threats, relevant to the node. The list of possibly relevant threats is specified in Table 3.1. According to Infowatch Global Data Leakage Report 2015 (Global data leakage report 2015) data leakage depends on person's position in the enterprise. Therefore, the data leakage likelihood value *nl* is modified to illustrate the change of confidentiality level of different positions of the enterprise. Five enterprise positions are analyzed (see Table 3.2). They have their confidentiality level coefficient *cof* and should be associated for each enterprise structure nodes.

Probabilities and coefficients in Table 3.1 and Table 3.2 are provided as examples and should be defined and updated periodically by statistical or expert evaluation data in global, national or enterprise sector level.

Table 3.1. List of human factor errors: threats and data leakage likelihood values for data leakage probability estimation of the enterprise management structure node

Threat	Model situation	Data leak likelihood, *nl*
Person uses IT to store or process information and the data can be leaked because of IT vulnerabilities.	Node properties define what IT is used to process and store, as well as specify the information flow.	Calculated according to modified CVSS score (see Chapter 3.3.1) for applicable NVD data.
Person has secret information and leaks data accidently or on purpose.	Node stores one or more information objects.	0.020 (Thommesen, & Andersen, 2012)
Person confusingly sends secret data to a lower security level person or department.	Node stores multiple information objects and sends it to one or more different nodes.*	0.016 (Thommesen, & Andersen, 2012)
	Node stores one or more information objects and sends different information to multiple nodes.*	
Person confusingly sends the data to a wrong to specific employee in a department.	Node sends information to one person in a multiperson department.	0.006
Unauthorized person sends data. This shows accountability problems and the possibility for confidential information to be shared.	Node sends information with no associated subordination flow.	0.050

* does not apply if all receiving nodes issued the subordination flow for all information objects the sending node owns. In this case the receiver gets wrong information, however the data is not leaked as it is sent to the same person with a right to access it.

Table 3.2. Data leak likelihood correction coefficients for different type enterprise structure nodes

Node type	Position/Department type	Confidentiality level coefficient *cof*
Individual	Employee	1.05
	Contractor	1.02
	System administrator	1.00
	Executive	0.99
Department	Hierarchical structure	1.00
	Flat structure	1.02

3.4. Availability Evaluation Model

While methods for automated security risk evaluation based on computer infrastructure exist, the automated security risk evaluation based on information management structure and human behavior is still missing. To fulfill this gap, we propose a method, which analyzes the information management scheme and derives the probabilistic data availability metric by estimating security needs at the computerized information flow management nodes.

Data availability depends on the number of possible data sources. If there are multiple data sources and one cause is unavailable, it is possible to use other ones. This means that the overall data availability can be calculated as a probability that at least one data source is available at the moment.

To get data for the availability estimation, the visual notation is a handful tool, allowing a clear data flow presentation. UML (Larman, 2000) or BPMN (Chinosi et al., 2012) are one of the most used tools in such cases, and they can be used in this model too. However, in the future, this model should be combined with confidentiality and integrity evaluation models where enterprise hierarchy plays an important role. As BPMN is oriented to present business process flow rather than business management structure, the standard BPMN is not suitable for this solution; meanwhile, UML is more engineering oriented and would need additional enterprise based notation. The enterprise management structure based notation is proper and preferred comparing to UML to adopt this model in business areas, with no need of security or information technology specialist – to draw enterprise hierarchy and information flows for business area person is easier comparing to drawing detailed business process scheme.

For this model, we use notation, presented in Fig. 3.2. It allows the definition of an enterprise hierarchy, by using subordination flows. As well we can define one person or group of persons. This is very important for confidentiality; however, it plays an essential role in availability evaluation too. Also, each member

of the group has data copy, so the availability is improved compared to the situation when one person has the data on his supervision.

The definition of enterprise information management structure is just the first step in availability evaluation. As this diagram is the hierarchy and information transfer direction oriented, it does not allow the definition of separate information flows. Therefore, the second step is to define information objects in the model. The user defines each information object, by selecting information flows it contains, its order and by defining properties for each of the information flow.

Each information flow in the information object has to be detailed by providing such information as:

1. Transfer type – defines the transfer environment. The list of possible environments can vary. It is important as the data availability in each environment is different. Accordingly, each transfer environment is associated with the according to the probability of data availability $P_{At}()$;
2. Storage by the receiver – the amount of time the receiver stores the information. In some cases, the receiver resends the information, and no storage is done. In such cases, the receiver can cause the delay; however, it will not increase the availability as the copy of the information will not be stored by him or her;
3. Usage by the receiver – defines can the receiver change the information. Modification of received information enables deleting important parts of the information, while storage without modification ensures that the initial information is available. The type of actions the receiver can execute on received information influences its availability, therefore each type of actions has an associated data availability;
4. Receiver's availability $P_{An}()$ – the receiver availability throughout the time. If one person stores the information and the person is unavailable, the information will be unavailable too. So, the parameter defines the probability of the receiver's availability to provide information all the time;
5. Receiver's storage availability $P_{As}()$ – defines the receiver's computer resistance to denial of service or data unavailability. This parameter should be calculated by other tools, designed to evaluate computers or computer infrastructures availability.

In the second step, the user defines all information flows for each information object. This includes modification of the object; therefore, the probability of data availability is calculated for each version of the information object. Thus, the third step divides the information object into information object versions. This is done according to Usage by receiver property – if the user can modify the information object; from this point, we assume it as a new version of the object.

The information processing sequence plays a vital role in terms of required incoming data. If a node needs specific information to finish its tasks, generate new information, the delay or absence on needed incoming flow stops the new information generation process; therefore, the further information is unavailable at the moment when incoming data is delayed. So, if we divide information object into M versions, probability of each information object versions depends on the availability of the previous version.

In the fourth step, we analyze the availability of each version of the information object. The probability is calculated as the probability of all needed previous versions available (*PAv 1*()*)* and the probability that the version is available in at least one of nodes which stores the version of an information object *(PAN*()*)*. The *PAv 1*() can be calculated as availability production of all L needed information object versions. As the first version of the information object is original and there are no previous versions, the availability of the initial version of the information object is equal to (3.6).

$$P_{Av}(f) = P_{Av-1}(f) \cdot P_{AN}(f) = \left(\prod_{i=1}^{L} P_{Av-1}(i)\right) \cdot \left(1 - \prod_{j=1}^{K}(1 - P_{At}(j) \cdot P_{An}(j) \cdot P_{As}(j))\right). \quad (3.6)$$

As each information object version is stored in *K* nodes, the P_{AN}() is calculated as a probability at least in one of those nodes we will be able to get the version of the information object. The information availability in the node depends on nodes ability to get data or availability of transfer environment P_{At}(), availability of the node itself P_{An}() and availability of nodes storage P_{As}*()*. All three parameters are important for data availability in the node as at least one of those stages the data will be unavailable, the access to the data will not be possible.

As the availability of each version of information object P_{Av}() is dependent on the availability of previous versions $P_{Av\text{-}1}$() the sequence of P_{Av}() calculation have to be executed starting from the oldest versions to the newest ones. This generates the availability of information object for each version. The availability of the information flow is equal to the availability of the last version. Meanwhile the data availability of the entire enterprise is equal to the lowest availability between all information flows in the enterprise. The abstract scheme of all availability evaluation steps is presented in Fig. 3.4.

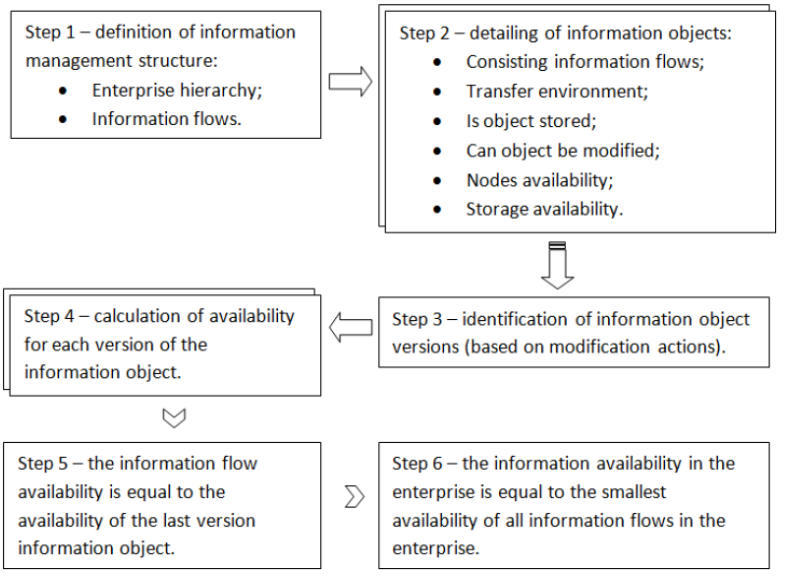


Fig. 3.4. Abstract scheme of the steps to evaluate enterprise availability based on its information management structure

The application of this method is uncomplicated if information transferring environment, node and node's storage (usually personal computer) availability is known. All the availabilities can be unique for each enterprise as well can vary for a different node in the information management structure. We propose to use EAAT or another similar tool in parallel for security analysis of computer infrastructure in the enterprise. The results of this analysis can be used as metrics for transfer $P_{At}()$ and node storage $P_{As}()$ availability estimation, while the node's availability $P_{An}()$ can be calculated according to employee contract conditions.

3.5. Integrity Evaluation Model

By analyzing existing literature, real world examples, and generating different situations, a list of factors influencing information integrity was derived:

- Format of the information object. Some file formats are dedicated for editing while others are difficult to change. The easier to change the information, the bigger the probability it will be changed (accidentally or no);
- The number of persons, possible to access and change the information. Each person who can access the information might change the information object, damage, or delete it;
- Information transfer channel. Information might be altered by its users or third parties during the data transfer or getting access to the

storage. Therefore, it is essential how safe is the transfer channel from the sender to the receiver. This is a more technical aspect; however, it should be integrated into integrity estimation calculation;

- Security of information storage. This is another technical element, which defines how secure the information is while it is stored in different locations or the organization. If the computer where the employer stores the information is compromised, third parties can change the data and reduce the integrity of the information object;
- Human factors. The integrity of the information object can be reduced by unsuitable employees work with it. If the employee does not know how to work with a specific system, is stressed, not concentrated, etc., he or she can accidentally damage the information object;
- Logging and backup system usage. The bigger number of information object copies exist, the bigger probability to trace the modification of information object or reconstruction of original data.

All these mentioned factors and more specific situations can be divided into three main categories: information storage environment; information transfer environment; human factors. The first two can be obtained by modeling and evaluating the organizations IT infrastructure (by using CySeMoL EAAT tool or other), while the third one can by estimated be analyzing statistical data on human error accidents or experimentally the human error resistance in different situations.

For information integrity estimation we will use those three summarized metrics: integrity corruption probability during transfer from node *a* to node *b* $P_{It(a,\,b)}$, integrity corruption probability while storage in node *a* $P_{Is(a)}$, integrity corruption probability by its user (human factors) in node *a* $P_{Ih(a)}$. In order to understand the occurrences of these probabilities in the information flow, an example situation is presented in Fig. 3.5.

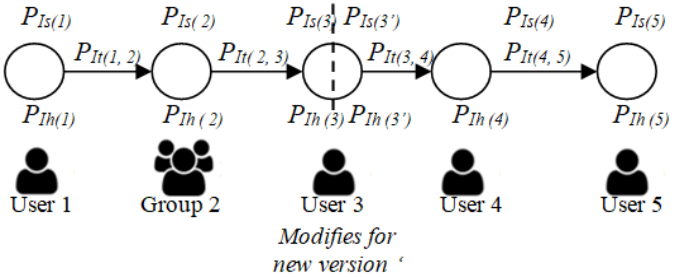


Fig. 3.5. Abstract scheme of information flow with noted integrity corrupting probabilities and modification for new version point

The example in Fig. 3.5 shows situation when information object is created by User 1 and sent to Group 2. Group 2 send it to User 3, which modifies (legally as a part of the process) the information object. From this point the information object was modified and User 3 stores both unmodified and modified versions of the information object while for further actions modified object is sent to User 4 and User 5 consequently. Because of the required modification in the information flow the flow is divided into two – one for each version of the information object. Therefore the first version of the information object is influenced by probabilities $P_{Is(1)}$, $P_{Is(2)}$, $P_{Is(3)}$, $P_{Ih(1)}$, $P_{Ih(2)}$, $P_{Ih(3)}$, $P_{It(1,\,2)}$, $P_{It(2,\,3)}$ while the second by probabilities $P_{Is(3')}$, $P_{Is(4)}$, $P_{Is(5)}$, $P_{Ih(3')}$, $P_{Ih(4)}$, $P_{Ih(5)}$, $P_{It(3,\,4)}$, $P_{It(4,\,5)}$.

All the probabilities are independent; therefore, we can calculate the information object version integrity as probability as in all nodes of the version the integrity will be kept (3.7)

$$P_{If}(f) = \prod_{i=n+1}^{m}\left(1 - P_{It(i-1,i)}\right) \cdot \prod_{i=n}^{m}\left(1 - P_{Is(\,i)}\right) \cdot \prod_{i=n}^{m}\left(1 - P_{Ih(\,i)}\right). \qquad (3.7)$$

There $P_{If(f)}$ is the versions information flow f integrity. While n is the node from with the version's information flow starts and m is the node, where the information of this version flow end. So we have to go through all probabilities of this specific version a and multiply all inverted transfer $P_{It(a,\,b)}$, storage $P_{Is(a)}$ and human error $P_{Ih(a)}$ occurrence probabilities.

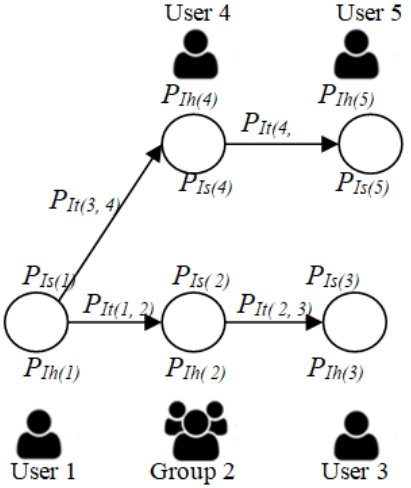


Fig. 3.6. Abstract scheme of information flow with fork, where multiple copies of the same version is processed in different paths

However, there might be situations (see Fig. 3.6) when one information object is send to multiple destinations and a fork of information flow is done. In

situations like this the versions is accessible in multiple information paths, therefore should be calculated separately (probabilities $P_{Is(1)}$, $P_{Is(2)}$, $P_{Is(3)}$, $P_{Ih(1)}$, $P_{Ih(2)}$, $P_{Ih(3)}$, $P_{It(1,\,2)}$, $P_{It(2,\,3)}$ will be used for one path and probabilities $P_{Is(1)}$, $P_{Is(4)}$, $P_{Is(5)}$, $P_{Ih(1)}$, $P_{Ih(4)}$, $P_{Ih(5)}$, $P_{It(1,4)}$, $P_{It(4,\,5)}$ for another). The integrity of this information object version $P_{Iv}(f)$ will be equal to probability that it is unchanged in at least one of the information flows $P_{If}(f)$ of the version (3.8) as we can get it from the source which has unchanged information.

$$P_{Iv}(f) = 1 - \prod_{i=1}^{k}\left(1 - P_{If(i)}\right). \tag{3.8}$$

There $P_{Iv}(f)$ is the versions f integrity. While k is the number of different paths of the information flow (for this specific version), where integrity of each information flows $P_{If}(f)$ is used to get the integrity of the version.

By using this formula (3.8) we can calculate the integrity of each version of the information object. In order to calculate the integrity of overall information object we should calculate what is the probability the information object will not be changed in any of its versions. If integrity is corrupted in at least one version this means the integrity of the information object is corrupted too. While the versions of information object is dependent on each other, the integrity probabilities of each version are independent, therefore we can calculate the overall information objects integrity $P_{Ii(o)}$ for object o as shown in (3.9).

$$P_{Ii}(o) = \prod_{j=1}^{V} P_{Iv}(f). \tag{3.9}$$

Transfer $P_{It()}$ and storage $P_{Is()}$ integrity corruption occurrence probabilities can be estimated from existing IT infrastructure estimation tools. User can model specific situations and analyze the security risk for each of the nodes. Meanwhile the most complicated part of the model is estimation of human error occurrence probabilities $P_{Ih()}$. While there are no clear statistics on integrity corruption probabilities for different SME positions or other employees' properties we suggest to use "Human Error Probabilities (HEPs) for generic tasks and Performance Shaping Factors (PSFs) selected for railway operations" (Thommesen, & Andersen, 2012). You can find different situations and average human errors in those situations. By linking the provided situations to the usual stress level in the organization, some orientation metrics can be transferred and used as human error influenced integrity corruption probabilities.

3.6. Conclusions of the Third Chapter

1. The analysis of ISM tools revealed there are no solutions for resource and structure aspects in an organization perspective while strategy perspective is not implemented in information security tools at all. Only 50% of enterprise security modeling views are covered by modeling tools. The most important aspect for information security management is C06: organizational perspective with structure view as most information security standards and frameworks mention the importance of human factors and information flows; however, clear methods for its evaluation do no exists. Yet this view is not covered by any tool; therefore, a toolset for information security management cannot be full.
2. To reflect different security criteria in the organization separate models for information confidentiality, integrity, and availability were proposed. All these models rely on information flow and according to security corruption possibilities during the information flow process. By considering separate probabilities in each node and each transfer the overall information object data leakage, availability, and integrity can be estimated.
3. The information object can be modified; therefore, the models consider the legal modification fact and calculates the probability for each version and only then derives the overall probability for the total information object. Therefore, the person who models the situation has to take into account not only the management structure of the organization but the information flows and user privileges as well.
4. The proposed model operated even probabilities; therefore, the security level is expressed as probability it will stay secure or as an inverted probability – the system security will be damaged. The quantitative expression is more suitable for comparison and can be used for risk management too.

4

Validation of Proposed Models and Framework

The proposed information security level estimation models were proposed in the previous Chapter, and in this Chapter, they are validated by analyzing some selected situations and how it correlates to experts' opinions. All situations reflected an SME which work in web development and had the same management nodes, however the management scheme varied, by presenting different information flow schemes. All three models were applied to these situations and compared with information security management experts. Experts used the ranking of all proposed situations; therefore, we were able to compare the ranking with modeling results and achieved a high correlation between experts ranking and modeling results.

The proposed ISM framework and its leading models are developed to simplify the ISM process in SME. Therefore, the main criteria for its suitability should be a real application in real life SME. Thus, in this Chapter, some examples of SME are presented too. Those SMEs applies the proposed tools, and according to the usage properties and the final conclusions on the suitability of proposed solutions can be evaluated.

Described research and its results, described in this Chapter were published (Kauspadiene et al., 2018 and Kauspadiene et al., 2019).

4.1. Validation of Information Flow Security Evaluation Models

4.1.1. Selected Situations and Properties for Experimentation

For validation of the proposed model, we execute an experiment where different management versions of the same enterprise are analyzed. The usage of different management versions of the same organization allows comparison of management influence, while the nodes stay the same.

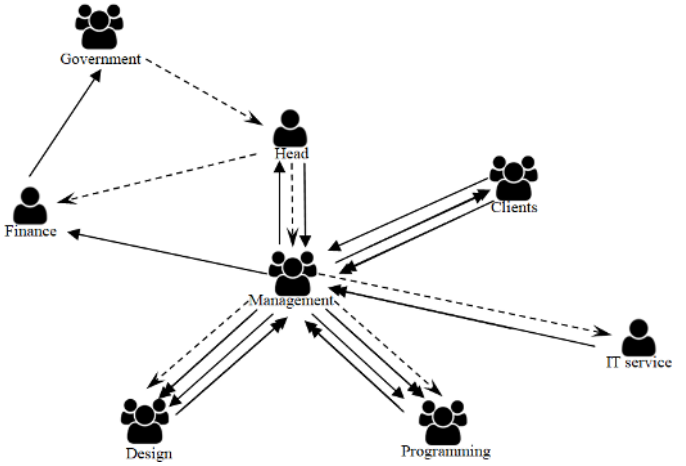


Fig. 4.1. Hierarchal enterprise management scheme with departments

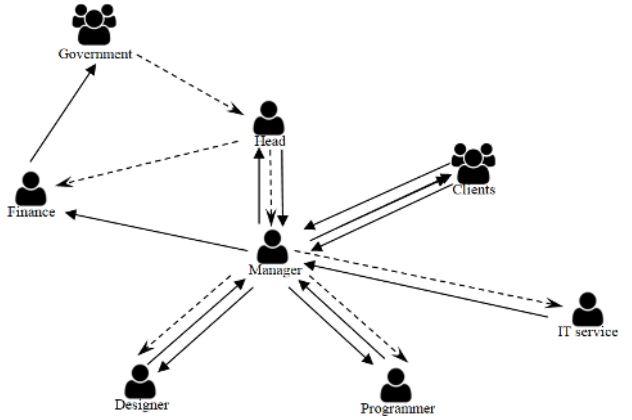


Fig. 4.2. Hierarchal enterprise management scheme with no departments

Multiple enterprise management structure (EMS) variations of one company were analyzed to validate the proposed model:

- Hierarchical (traditional hierarchy) EMS has tree structure subordination flow, where each person/department has one superior node only:
  - With departments, where multiple employees work in the same position (see Fig. 4.1);
  - With a single person in one position and forming no departments in the enterprise (see Fig. 4.2);
- Flatter EMS removes layers within the organization and enables communication and collaboration within different layer persons/departments.
  - With departments, where multiple employees work in the same position (see Fig. 4.3);
  - With a single person in one position and forming no departments in the enterprise (see Fig. 4.4).

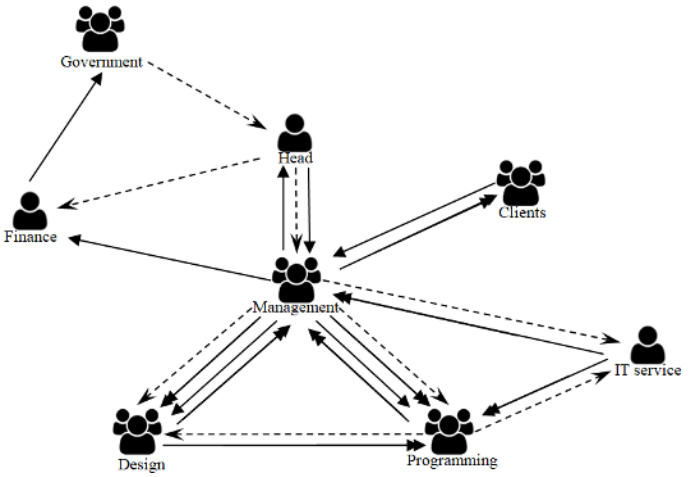


Fig. 4.3. Flatter enterprise management scheme with departments

The properties of each node and information flow are defined in a similar manner. However, the node type changes, although the values of matching properties and vulnerabilities are set to be the same. Similar settings allow more accurate comparison of enterprise architecture.

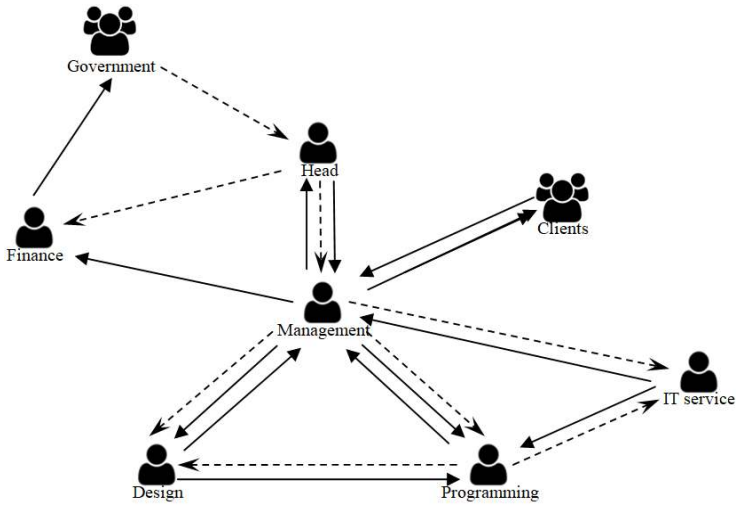


Fig. 4.4. Flatter enterprise management scheme with no departments

To make the analyzed situations even more similar in the sense of parameters, the same 8 main information flow groups are analyzed:

1. Organization strategy – initiated by the leading authority, passed to the management and shared with clients;
2. Activity report – parts generated by management, passed to the leading authority and the finance department. The finance department processes it and sends it to the government;
3. Project idea – client generated project ideas are shared with the management; management shares it with design and programming;
4. Initial project price – design and programming department generates parts of it, send it to management, management processes it according to organization strategy, and sends to the client;
5. Detailed project requirements – client generates the requirements and sends them to the management, management shares parts of it with design and programming;
6. User server account login data – IT service generates logins and sends to the programmer (directly or through management);
7. Developed system design – designer generates the system design and sends it to the programmer (directly or through the management), programmer integrates it into the project source code and sends to the management, which presents it to the client;
8. Developed system source code – programmer takes the designed system design and uses server login data to implement it, then sends the project

source code to the management, where the source code is presented to the client.

For better presentation, schemes of all 8 information flows are presented in Fig. 4.5–Fig. 4.16. Dotted areas define iterative processes.

Organization strategy is very simple, consists of three nodes, connected linearly (see Fig. 4.5). The organization strategy information flow is identical for both hierarchical and flatter enterprise management schemes.

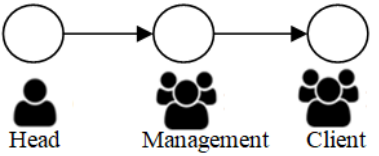


Fig. 4.5. Information flow of Organization strategy in Hierarchical and Flatter enterprise management scheme

Activity report (see Fig. 4.6) has two alternative paths as well Finance node is modify the information object by generating another version.

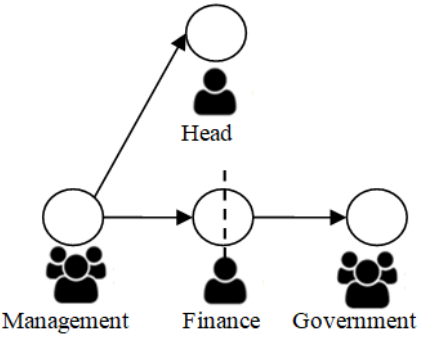


Fig. 4.6. Information flow of Activity report in Hierarchical and Flatter enterprise management scheme

Project idea information flow is more complicated and divided into two parts – price arrangement and project development (see Fig. 4.7 and Fig. 4.8). These parts can be executed multiple times.

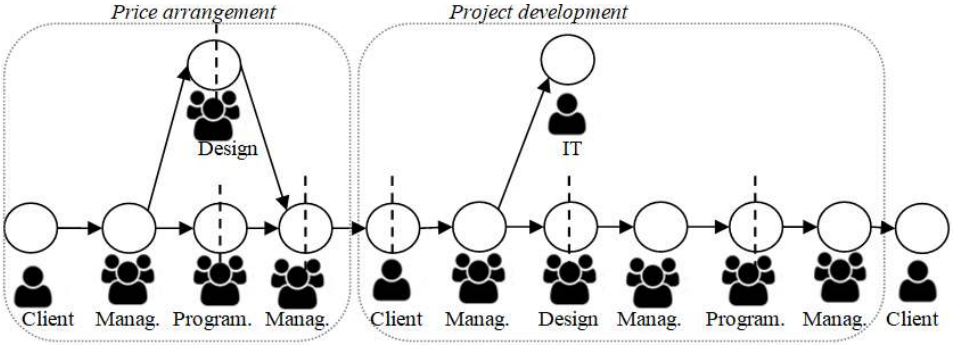


Fig. 4.7. Information flow of Project idea in Hierarchical enterprise management scheme

The difference between hierarchical and flatter enterprise management schemes (see Fig. 4.7 and Fig. 4.8) are in project development only, when information to IT is sent in different moment.

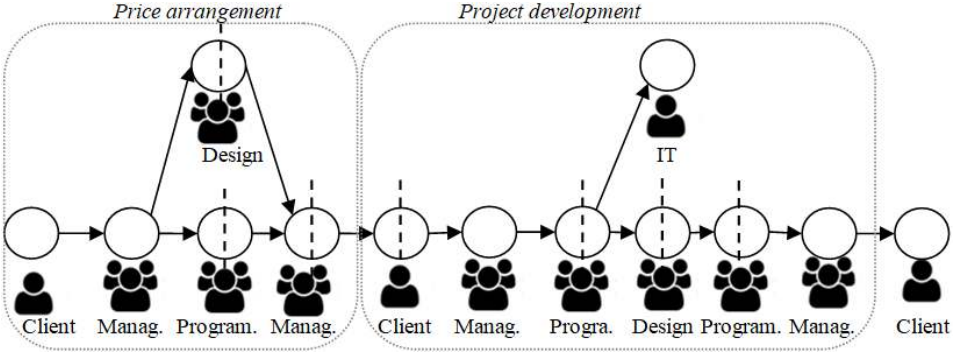


Fig. 4.8. Information flow of Project idea in Fatter enterprise management scheme

Initial project price information flow is different as management gets information from two nodes and only then can proceed by creating another version of the information object (see Fig. 4.9).

Project requirements are part of the project idea, so it repeats the project development part (see Fig. 4.10 and 4.11). As mentioned above, the difference between hierarchical and flatter enterprise management schemes are the place to send information to the IT node.

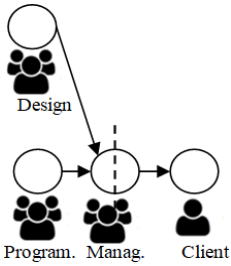


Fig. 4.9. Information flow of Initial project price in Hierarchical and Fatter enterprise management scheme

As well the number of information object versions is different, as in flatter enterprise management scheme programmer and designer changes it and send the modified version. Meanwhile in hierarchical enterprise management structure the management is responsible to collect all information and combine it to one new version.

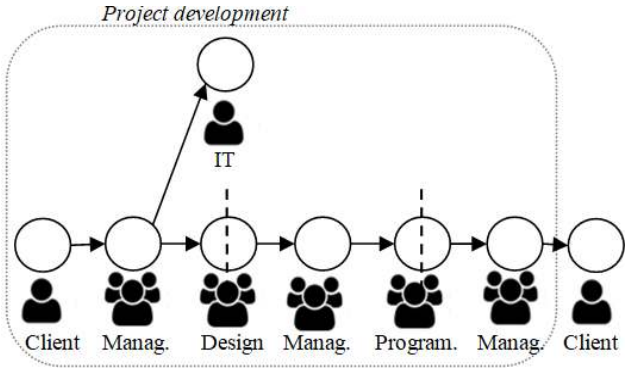


Fig. 4.10. Information flow of Project requirements in Hierarchical enterprise management scheme

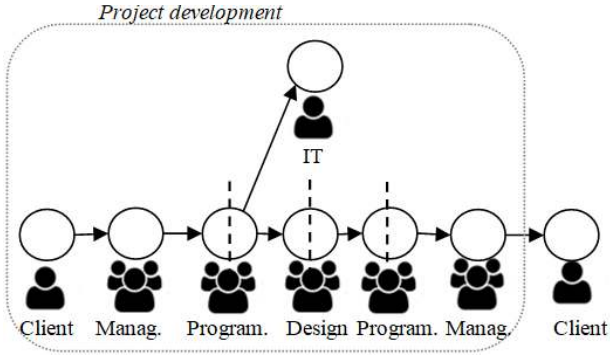


Fig. 4.11. Information flow of Project requirements in Fatter enterprise management scheme

The rest information flows are linear and differs according to the list of nodes in the flow or/and modifications in some nodes (see Fig. 4.12–Fig. 4.16).

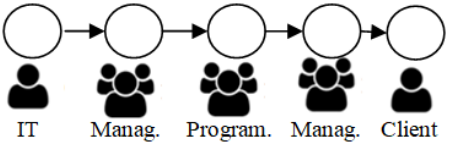


Fig. 4.12. Information flow of Login data in Hierarchical enterprise management scheme

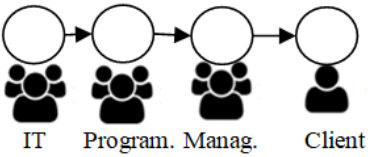


Fig. 4.13. Information flow of Login data in Flatter enterprise management scheme

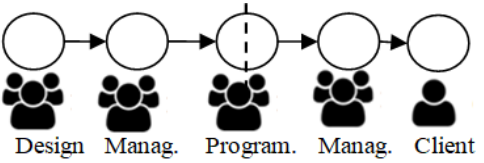


Fig. 4.14. Information flow of Project design in Hierarchical enterprise management scheme

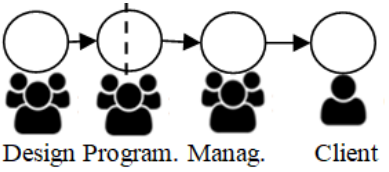


Fig. 4.15. Information flow of Project design in Fatter enterprise management scheme

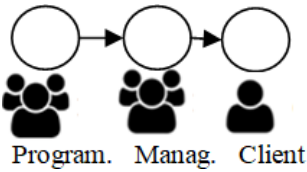


Fig. 4.16. Information flow of Project source in Hierarchical and Flatter enterprise management scheme

To analyze the situation, all information transfers within the enterprise are done by using the local network and specialized communication and order management systems. Therefore, the transfer environment confidentiality, availability, and integrity among enterprise employees are 0.99. Meanwhile, the client sends the information via the Internet, and its values in our case are 0.98. All employees of the enterprise use computers for order information storage and its confidentiality, availability, and integrity is 0.99; meanwhile, the values for client's computer is 0.95 as it's a personal computer with no specific security protection tools.

For confidentiality evaluation, the coefficients of Table 3.2 are used. Meanwhile, the confidentiality of enterprise computers which stores the information is 0.97 (calculated according to existing threats in computers and computer network) the human confidentiality is 0.98 (estimated based on human error possibility, which is 2% in this kind of tasks). As well we assume there is a 1.6% possibility the information flow will be sent to the different receiver if the sender works with different receivers/departments. There is a 0.6% possibility a person will send the data to the wrong person in a group of persons. 7% possibility some data leakage will occur if the information is sent to unmonitored object (when the receiver is in lower subordination flow level).

The availability of enterprise employees and client is as follows:

- Head – 0.7 as the head is busy with other tasks, as well travels a lot;
- Management. Design, Programming groups and Finance – 0.9 as there are multiple persons they can stand in for each other; however, they must participate in other activities too, therefore might be unavailable in some cases;
- Management, Design, Programming individual person – 0.8 as there are one person for each position which is responsible for all projects at the same time;
- Governance – 0.99 as it is a separate organization, which ensures it will be available 99% of needed time;
- IT – 0.95 as there is only one person, which always is in place to look after the equipment and services, however sometimes he is ill as well he

has huge number of tasks to execute and cannot serve all requests at one time. However, he uses information technologies to work from distance;
- Client – 0.6 as he has other responsibilities and this order is not his first priority.

For availability evaluation each dashed line in Fig. 4.5–Fig. 4.16 presents where the information flow is modified, so from this point forward a new version is in action.

For integrity evaluation, the enterprise computers availability is 0.98 (calculated according to existing threats in computers and computer network), client's computer – 0.95. The human error possibility for impropriate data modification or corruption is 2% (estimated based on human error possibility for this kind of tasks) if an individual is working with the information and 1% if group is working (more chances to make an error but at the same time more persons can notice the error and correct it).

4.1.2. Experiment Execution Process

In order to validate the results of proposed models some data for comparison was required. The probability estimation for security level comparison is not new; however, we were not able to find a model, which would take into account enterprise management structure and would derive the data leakage probability. The closest solution is Enterprise Architecture Analysis Tool, based on attack trees and CySeMoL (Holm, Shahzad, Buschle, & Ekstedt, 2015). However, this tool allows modeling of information technology infrastructure, while human based factors are not included. There is only very fragmented data on SME security management level for specific situations therefore it is impossible to compare our models calculated and existing results. Therefore, in order to validate the results of our experiment, we used expert evaluation.

Experts were chosen from the information security area. 15 persons were selected for the first meeting to evaluate their suitability to participate in this experiment as information security management experts. Multiple criteria were applied for expert selection:

- At least 3 years experience in information security area;
- Understanding of information security management principles (participants were asked to answer some questions related to information security standards and best practices);
- Experience in risk management (at least understanding how it is done, what methods and tools can be used for it).

Only 8 persons meet all three criteria and were chosen to participate in the experiment as information security management experts.

The description of example enterprise, examined information flows were provided and variations of the cases were explained. Each expert had a freedom to use any tools or methods for evaluation of all provided situations. They had a period of 1 week (7 days) to rank (or provide some metric which can be used for ranking different situations) all information flows according to confidentiality, integrity and availability. Each expert ranked/evaluated 32 situations – 8 information flows in each of 4 different EMS situations.

Two of experts did not provide any data and refused to continue the participation in the experiment. Therefore, results from 6 experts were used for model validation. All experts used ranking or a personally chosen risk metrics for each situation. Each expert has his own risk evaluation methodology and metrics; therefore, they were not forced to use a different, maybe unknown system. Because of ranking, rather than risk measurement metric was used by some expert, the validation aimed to prove the correlation between experts' opinion and modeling results rather than get the accuracy of modeling results. There is no unified and very clear quantitative metrics or scales for security risk measurement. While in many situations High, Medium and Low risk levels are used, each person can have his own understanding on the threshold for each of these categories. Therefore, it is important to evaluate does the trendline is the same between experts' opinion and modeling results. If clear relationship will be noticed, the next step can be segmentation of modeled values to be mapped to experts used metric.

Half of the experts (3 out of 6) ranked all situations while other half presented marks or categories (defining the risk) for each situation. The expert had to explain the grading scale (minimum and maximum values) and later the scale ranges were used to normalize the results for data comparison.

The described situations were modeled by using the proposed models. At the same time expert opinion was used to rank or evaluate the situations. The comparison of model results to expert opinion and existing rules of other models allowed validation of the proposed models as different situations have different risk values and can be compared between to find out the better or worse case.

4.1.3. Data Leakage Evaluation Results and their Analysis

After modeling all four enterprise structures, data leakage probabilities for each of these 8 information flows were estimated. The results are presented in Table 4.1. Comparing the average data leakage probability for each type of analyzed enterprise structures has revealed a tendency of the individual based structure to be more suitable for data confidentiality. The difference is 1% and meets the rule – the more persons know the secret information, the bigger the risk of data leakage.

Table 4.1. Data leakage probability for each of the information flows of the analyzed enterprise structures.

Information flow	Data leakage probability			
	Hierarchical structure		Flatter structure	
	With departments	With no departments	With departments	With no departments
Organization strategy	0.236	0.230	0.236	0.230
Activity report	0.254	0.261	0.253	0.261
Project idea	0.408	0.390	0.417	0.402
Initial project price	0.310	0.290	0.321	0.304
Detailed project requirements	0.370	0.352	0.380	0.364
User server account login data	0.226	0.210	0.151	0.141
Developed system design	0.331	0.311	0.321	0.304
Developed system source code	0.286	0.266	0.296	0.278
Average	0.303	0.289	0.297	0.285

Comparison of data leakage probability in hierarchical and flatter structure enterprises showed no direct correlation. In some cases, information flow data leakage probability is lower when using hierarchical enterprise structure, in some cases it is the opposite.

Data leakage probability mostly depends on the number of nodes and connections between them. In analyzed scenario the flatter enterprise structure allowed minimization of information flow shared nodes, therefore the data leakage probability was lower. This tendency is most obvious in "User server account login data" information flow: in this hierarchical structure 3 nodes know the information and 2 data transfers are needed, while in flatter enterprise structure only 2 nodes know the information and only 1 data transferring was required to share it. A significant change in the node and its connection number influences the difference of data leakage probability in hierarchical and flatter enterprise structure for this information flow is 7.5%.

For proposed model result validation, all four enterprise structure models and defined information flows were presented to 6 experts in the field of organization risk management. The comparison of expert ranking and modeled information flow data leakage probability is presented in Fig. 4.17.

Despite the fact that the experts used different ranking scales (one expert ranked the situations sequentially from 1 to 32, two used the same rank for multiple situations, therefore the scales were from 1 to 18 or from 1 to 7 only, two

experts evaluated all situations according to scale High, Medium, Low and one expert evaluated all situations based on 10-point scale).

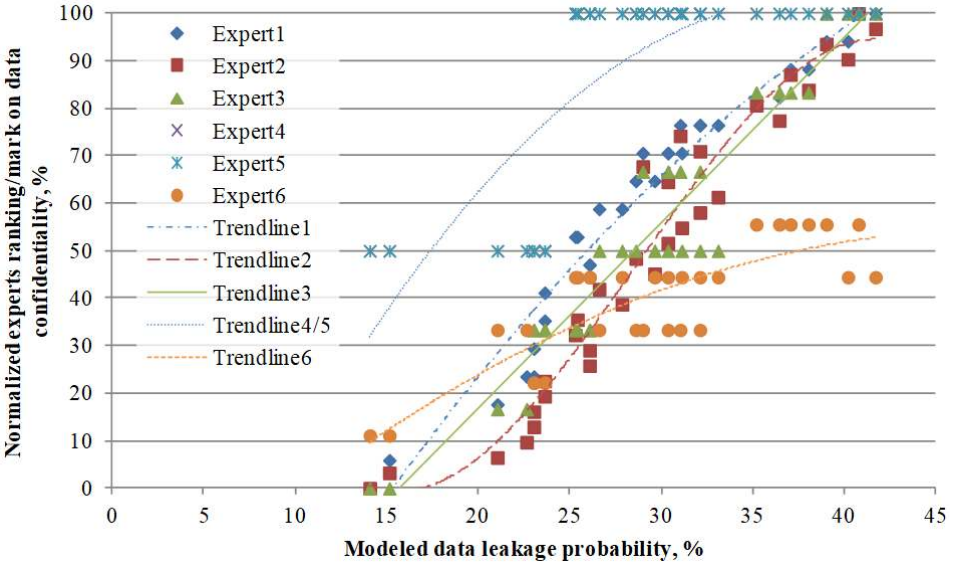


Fig. 4.17. Relationship between modeled information flow data leakage probabilities and normalized expert rankings

The comparison between modeled data leakage probability and situation confidentiality ranking cannot provide the accuracy of the data leakage probability. However, the precision of the data is considered to be good, as the correlation coefficients between modeled values and experts ranking/marks are high (see Table 4.2).

Table 4.2. Experts data analysis for data leakage experiment

Metrics	Expert1	Expert2	Expert3	Expert4	Expert5	Expert6
1	2	3	4	5	6	7
Evaluation method	Ranking	Ranking	Ranking	Evaluation	Evaluation	Evaluation
Scale	1–18	1–32	1–7	High (3), Medium (2), Low (1)		1–10
Min. value	1	1	1	Low	Low	2
Max. value	18	32	7	Medium	Medium	6

End of Table 4.2

1		2	3	4	5	6	7
Correlation to modeled values		0.97	0.96	0.97	0.72	0.72	0.82
Linear trendline	x	64.40	129.38	23.43	4.55	4.55	13.29
	C	–7.59	–21.47	–2.69	1.42	1.42	0.60
Max. difference between linear trendine and experts value		12%	19%	15%	16%	16%	11%
Polynomial (2) trendline	x^2	–93.53	80.72	15.31	–23.85	–23.85	– 34.53
	x	118.62	82.59	14.56	18.37	18.37	33.30
	C	–15.01	–15.08	–1.48	–0.48	–0.48	–2.14
Max. difference between polynomial trendine and experts value		13%	20%	15%	18%	18%	10%
Polynomial (3) trendline	x^3	–1118	–3392	–11	–281	–281	–128
	x^2	841.22	2916	24.44	211.02	211.02	72.50
	x	–127.9	–665.3	12.15	–43.56	–43.56	5.08
	C	5.279	46.47	-1.278	4.622	4.622	0.185
Max. difference between polynomial (3) trendine and experts value		10%	18%	15%	15%	15%	11%

Comparison between experts' opinion and modeling results show high correlation (0.72–0.97). However analysis of 2nd and 3rd order polynomial trendlines showed some experts' opinion comparison to modeled results can be expressed with smaller variation by using polynomial rather than line. The maximum difference between experts' opinion and modeled value can be reduced up to 2% by using 2nd or 3rd order polynomial. This shows the experts' opinion and modeled values have different value distributions, however the difference is not drastic.

4.1.4. Data Availability Evaluation Results and their Analysis

Data of availability modeling results is presented in Table 4.3. In a given situation the Project idea and Initial project price are one of the most vulnerable as its availability is the lowest. Analysis of factors which influence these results showed it is related to the need of different data from different sources in order to proceed. In situations when different data is needed to precede the node is dependent on multiple sources, while in linear transfer the node requires only one version and can get it from multiple sources too.

The importance of multiple copies of the same version can be noted from the results too. User server account login data has one version only and is stored by 3 or 4 different nodes. Therefore, the availability of User server account login data is the highest among other information flows and do not decrease less than 0.99.

Table 4.3. Data availability probability for each of the information flows of the analyzed enterprise structures

Information flow	Data availability			
	Hierarchical structure		Flatter structure	
	With departments	With no departments	With departments	With no departments
Organization strategy	0.981	0.967	0.981	0.967
Activity report	0.982	0.973	0.982	0.973
Project idea	0.927	0.838	0.905	0.782
Initial project price	0.912	0.810	0.912	0.810
Detailed project requirements	0.989	0.963	0.965	0.899
User server account login data	0.999	0.998	0.999	0.998
Developed system design	0.990	0.965	0.975	0.926
Developed system source code	0.992	0.977	0.992	0.977
Average	0.972	0.937	0.964	0.917

Analysis of EMS influence on data availability showed the Hierarchical EMS leads comparing to Flatter. The difference is not significant (averagely 1%) and mostly is related to the number of versions – the Flatter EMS increases the number of versions (for project idea and requirements), therefore smaller number of nodes has the same version and it is more difficult to get the data.

In the initial parameters position with one employee had 10% smaller availability comparing to position with multiple employees (as they can cover each other). This influenced the information flow availability and reaches 10% for

project idea and initial price. However, the average information flow availability difference between multiple employee departments and individual person departments is 5%.

By analyzing the experts ranking for all 32 situations, opinions of two experts are different comparing to other experts and our modeling results (Fig. 4.18). One expert ranked Initial project price and User server account login data as information flows whose availability is the lowest while the Organization strategy and Project idea has the biggest availability. As the information flow is very different for two highest and two lowest rankings the expert was asked to explain the criteria used for situation ranking.

The expert answers revealed he based his ranking on personal experience and time period needed to get certain type of information (the answer of the expert was: "The company's strategy is publicly stored in the web and everyone knows the basic idea of a project they are working with therefore you can get the information quickly. Meanwhile no one wants to share the server's logins or the price of the project. This kind of data is not meant for sharing; therefore, it takes more time to find a person who knows it and is willing to share it.").

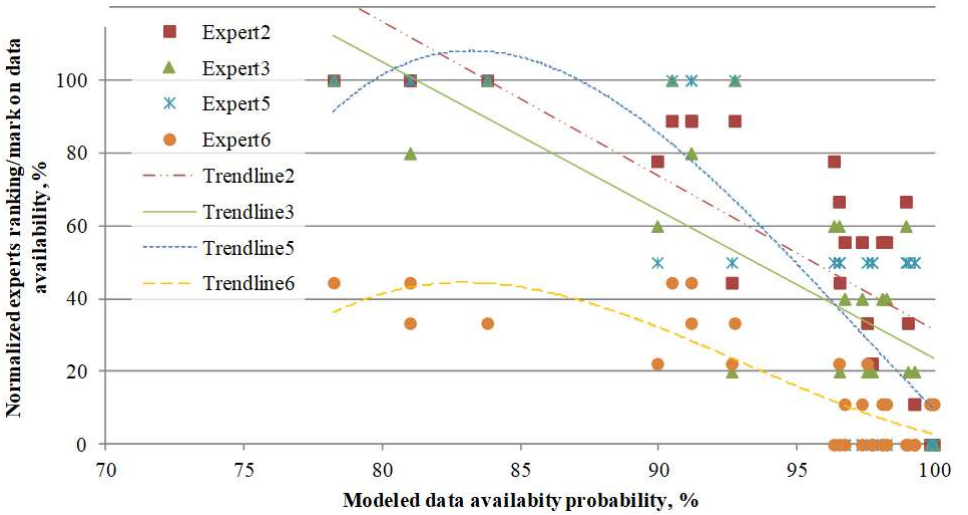


Fig. 4.18. Relationship between modeled information flow data availability probabilities and normalized expert rankings

This ranking was very content based and very related to data confidentiality rather than availability only. Our model does not take into account what kind of data it is and analyzes the information flow rather than confidentiality of the information flow and this is done consciously as availability should not be confused with confidentiality. However, in order to reflect the different type of data, the node's storage availability value can be adjusted.

Another user ranked all situations the same – Low availability risk. The same value for all situations is not suitable for comparison. Therefore, opinion of these two experts was eliminated from the validation experiment.

The other four experts took into account the availability should be evaluated for the person who has right to access the information therefore it is not confused with confidentiality. The ranking scale is different for all experts but the correlation between modeled values and expert ranking is high (see We can notice some differences however the main trend between those four experts and our model results are similar.

The same ranking/evaluation scales were used by experts as in data leakage experiment. In this experiment opinion of two experts is not very useful and might be misleading (one expert was not able to evaluate availability only and mixed it with confidentiality, while the second expert ranked all situations with the same rank – Low risk).

The correlation between the rest four experts and modeled data availability values are not as high as for data leakage, however the values varies from –0.75 till –0.80 which is high and show strong relation (see Table 4.4).

Table 4.4. Experts data analysis for data availability experiment

Metrics		Expert1	Expert2	Expert3	Expert4	Expert5	Expert6
1		2	3	4	5	6	7
Evaluation method		Ranking	Ranking	Ranking	Evaluation	Evaluation	Evaluation
Scale		1–18	1–32	1–7	High (3), Medium (2), Low (1)		1–10
Min. value		1	1	1	Low	Low	2
Max. value		18	32	7	Low	High	5
Correlation to modeled values		–0.06	–0.78	–0.78	N/A	–0.75	–0.80
Linear trendline	x	N/A	–38.16	–20.40	N/A	–9.90	–19.05
	C		41.96	22.57		11.25	20.42
Max. difference between linear trendine and experts value			9%	34%		31%	19%

End of Table 4.4

1		2	3	4	5	6	7
Polynomial (2) trendline	x^2	N/A	–318.7	–152.2	N/A	–59.4	–87.4
	x		537.3	254.4		97.4	138.7
	C		–216.0	–100.6		–36.8	–50.3
Max. difference between polynomial (2) trendine and experts value			11%	35%		24%	15%
Polynomial (3) trendline	x^3	N/A	–3089	–951	N/A	287	950
	x^2		8032	2419		–834	–2654
	x		–6961	–2054		793	2444
	C		2019	587.8		–244	–738
Max. difference between polynomial (3) trendine and experts value			11%	36%		23%	15%

Linear and polynomial (2^{nd} and and 3^{rd} order) trendlines were analyzed for each expert. The maximum differences between trendline based experts' values and real experts' rankings/marks were calculated. In half cases (for experts 2 and 3) the linear trendline is capable to get a smaller maximum difference while for other half (experts 5 and 6) the 3^{rd} order polynomial trendline produces smaller maximum difference as the value distribution has a have tails (see Table 4.4).

4.1.5. Data Integrity Evaluation Results and their Analysis

Results of modeled situations (see Table 4.5) showed the information flow integrity is closely related to the length of in sequence transferred data. The bigger integrity was achieved in small processes with up to 4 nodes and 3 information transfers – Activity report, Organization strategy, Developed system source code.

Another important factor – forking of information flow. Activity report has the same number of nodes and transfers comparing to Developed system design in Fatter EMS, however the integrity of the second one is approximately 10% lower. This is influenced by the fact the information flow is forked in Activity report case therefore the probability to change the information flow in all duplicated information objects is significantly smaller. If multiple versions of the same

document exist, there will be a possibility to check whether the information object is changed or not. At the same time backup copies of the information object will help to recover the original version and changes in the object.

Table 4.5. Data integrity probability for each of the information flows of the analyzed enterprise structures

Information flow	Data integrity			
	Hierarchical structure		Flatter structure	
	With departments	With no departments	With departments	With no departments
Organization strategy	0.842	0.833	0.842	0.833
Activity report	0.917	0.916	0.917	0.916
Project idea	0.564	0.499	0.509	0.447
Initial project price	0.769	0.731	0.769	0.731
Detailed project requirements	0.670	0.629	0.670	0.629
User server account login data	0.776	0.753	0.808	0.792
Developed system design	0.746	0.723	0.817	0.793
Developed system source code	0.886	0.868	0.886	0.868
Average	0.842	0.833	0.842	0.833

The smallest integrity is calculated for Project idea as it is the longest information flow, multiple versions exist, information is sent to client multiple times. All these criteria reduce the integrity to less than 50%. This value should be a big concern to the enterprise as even usage of multiple employees in the same position to control each other increases the integrity up to 5%.

Observing how similar the results are to expert's opinion a very strong correlation can be examined (see Fig. 4.19 and Table 4.6). This proves the main tendencies between different information flows in this situation can be captured analogue as experts' opinion.

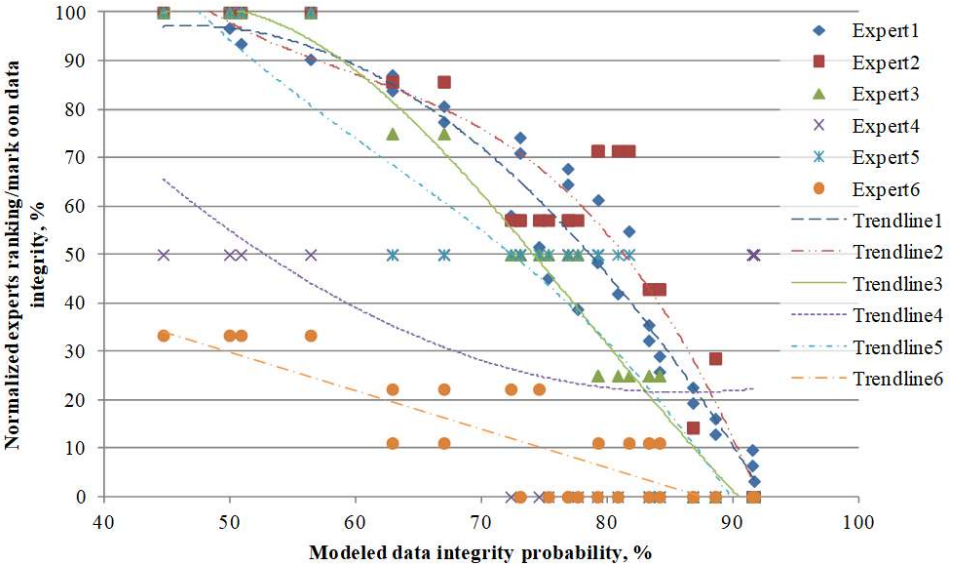


Fig. 4.19. Relationship between modeled information flow data integrity probabilities and expert rankings

Table 4.6. Experts data analysis for data integrity experiment

Metrics		Expert1	Expert2	Expert3	Expert4	Expert5	Expert6
1		2	3	4	5	6	7
Evaluation method		Ranking	Ranking	Ranking	Evaluation	Evaluation	Evaluation
Scale		1–18	1–32	1–7	High (3), Medium (2), Low (1)		1–10
Min. value		1	1	1	Low	Low	1
Max. value		18	32	7	Medium	High	4
Correlation to modeled values		–0.93	–0.89	–0.97	–0.40	–0.91	–0.83
Linear trendline	x	–68.59	–15.27	–10.15	–1.59	–4.77	–7.12
	C	68.69	16.43	10.35	2.77	5.38	7.23
Max. difference between linear trendine and experts value		19%	29%	27%	7%	17%	11%

End of Table 4.6

1		2	3	4	5	6	7
Polynomial (2) trendline	x^2	–143.1	–37.41	–11.39	5.12	–4.21	10.08
	x	133.61	37.59	5.94	–8.83	1.18	–21.37
	C	0.04	1.53	4.88	5.23	3.36	12.07
Max. difference between polynomial (2) trendine and experts value		14%	59%	15%	6%	16%	13%
Polynomial (3) trendline	x^3	–68.63	–115.4	45.41	102.78	–18.25	50.5
	x^2	1.47	205.62	–107.1	-211.43	34.25	–96.32
	x	34.69	–128.7	71.39	139.32	–25.13	51.42
	C	21.81	35.2	–9.58	–27.5	9.17	–4.01
Max. difference between polynomial (3) trendine and experts value		14%	23%	15%	8%	15%	13%

Analyzing the difference between modeled data integrity value and trendline based experts ranking/mark the linear trendline produces the smallest difference for expert 6, 2nd order polynomial trendline – for expert 1 and 4, while 3rd order polynomial trendline produces the smallest maximum difference for experts 2, 3 and 5 (see Table 4.6).

4.1.6. Summary of Information Security Evaluation Results

Also, we can notice the errors in ranking occurred in the range between 70% and 80% for the first expert and between 80% and 90% for the second expert as there were multiple situations with similar availability values. Therefore, it was easier for experts to rank more different situations rather than different with similar integrity values.

The ranges of different security components (confidentiality, integrity and availability) can be noticed in Fig. 4.20, where all these values are presented according to the probability of calculated overall security. All three components have a clear linear dependency, while the slope of confidentiality and availability is very similar (0.38 for confidentiality and 0.32 for availability) the slope for integrity is much higher (0.95). This shows the integrity values are more scattered

and have a bigger values ranges, while confidentiality and integrity are not as varied in our situation and have more similar values.

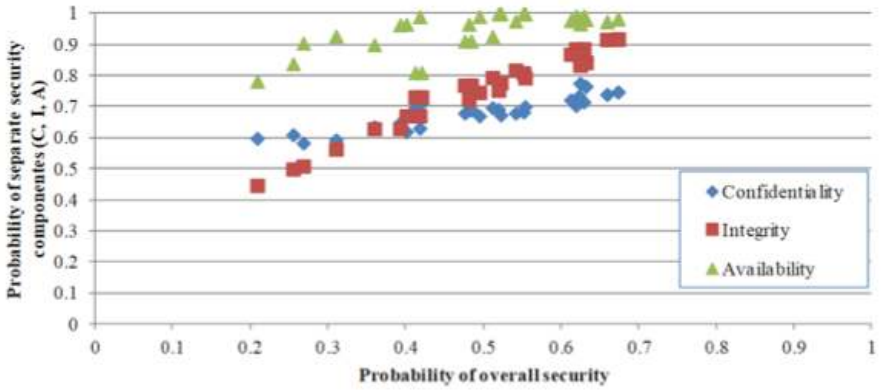


Fig. 4.20. Relation between modeled data confidentiality, integrity and availability values, ordered according to calculated overall security values

The overall security should be reflected as probability the enterprise information will be confidential, available and keep the integrity. It can be calculated as product of inverted data leakage probability, data availability probability and data availability probability. In these experiments it varies between 21% and 76%.

4.2. Validation of Information Security Management Framework

Validation and evaluation of proposed information security management framework is a complicated task as there are no clear methodologies of how it should be done. To reflect both theoretical and practical benefits of the proposed information security management framework the validation is divided into two parts: proposed ISMF comparison with other ISMF in the sense of framework fullness; experiment with enterprise presenters to evaluate reaction and benefits of proposed ISMF.

4.2.1. Multi-criteria analysis of Information Security Management Frameworks

The proposed framework partly was compared with existing frameworks during the analysis of existing frameworks (see Table 1.1), when requirements for a new one were derived. However, the previous comparison reflected properties of

analyzed ISMF and was not analyzing the fullness of ISMF. All existing ISMF comparisons basically are the same – relies on multiple criteria, however, all criteria have the same weight:

1. HITRUST – Health Information Trust Alliance (HITRUST, 2014) presents a brochure "Comparing the CSF, ISO/IEC 27001 and NIST SP 800-53: Why Choosing the CSF is the Best Choice" where 12 factors are used to compare three analogues. The comparison is done in binary values by defining is the factor included in the analyzed framework or no;
2. O. Rebollo et al. (Rebollo et al., 2011) presented a comparative analysis of information security governance frameworks. The research aims to guarantee an objective comparison through a set of comparative criteria to highlight the strengths and weaknesses of each framework. Criteria for the comparison were selected from an analysis of existing information security governance papers, including both governance and management aspects. Meanwhile, the comparison is executed by defining values of each criterion, and no weights or importance factors are defined in the comparison;
3. M. Alnuem et al. (Alnuem et al., 2015) executed a comparison study of information security risk management frameworks in cloud computing. The paper discussed how information security risk management is related to the cloud computing environment and presents seven different information security risk management frameworks that cover all of cloud service models and deployment models. Meanwhile, the comparison of mentioned frameworks was executed by summarizing framework information and classifying the frameworks according to coverage area of the framework.

A source where information security management frameworks would be evaluated according to clearly defined and weighted factors do not exist. However, it is clear the comparison is a multi-criteria problem and should involve multi-criteria decision making to select the best ISM framework. The weights of ISMF can be used for the optimization of newly developed ISMF. While in this thesis, the multi-criteria analysis will be used not to optimize the framework, but to find the best one. Therefore, a simple aim function is used – the sum of all criteria weight and value products.

From the linguistic analysis of the aim of this research, there can be noted two main evaluation areas: ISM framework applicability in small and medium enterprise and at the same time the ISM framework must serve as a needed knowledge database for information security management. As these two criteria (applicability in SME and content of the ISM framework) are too abstract, they must be detailed. Therefore, we selected the analytical hierarchy process (AHP) methodology (Saaty, 1980) to be applied. AHP implements the hierarchical

criteria structure, which will be very handy in our situation. It is a multi-criteria decision making technique and will represent the nature of multi-purpose security nature. AHP enables to combine a consensus of the expert group by weighing the criteria and sub-criteria (Baudry, 2018). The construction of the method is based on three steps: definition of the criteria structure; comparative evaluation of the substitutes and the criteria; synthesis of the priorities. AHP combines subjective assessments based on qualitative criteria and objective assessments based on quantitative criteria analytically (Saaty et al. 2015). According to A. Mardani et al. research results (Mardani et al. 2015), this is the most popular decision making technique during the period from 2000 till 2014 in scientific papers as more than 30% of all 393 analyzed decision making related papers were using this technique.

As mentioned above, we instinctively have the top-level criteria: applicability in SME and content of the ISM framework. In order to leave no place for unfair second level criteria selection we need a source which could serve as a reference model. In case of criteria "content of the ISM framework" the most intuitive is usage of security standard as a reference model. The most known and used information security management standard is ISO/IEC 27001 (ISO, 2013). This standard specifies a management system that is intended to bring information security under management control and gives specific requirements. Organizations that meet the requirements of this standard may be certified by an accredited certification body following successful completion of an audit. The current version of this standard has 114 controls in 14 domains:

1. A.5: Information security policies (2 controls);
2. A.6: Organization of information security (7 controls);
3. A.7: Human resource security (6 controls that are applied before, during, or after employment);
4. A.8: Asset management (10 controls);
5. A.9: Access control (14 controls);
6. A.10: Cryptography (2 controls);
7. A.11: Physical and environmental security (15 controls);
8. A.12: Operations security (14 controls);
9. A.13: Communications security (7 controls);
10. A.14: System acquisition, development and maintenance (13 controls);
11. A.15: Supplier relationships (5 controls);
12. A.16: Information security incident management (7 controls);
13. A.17: Information security aspects of business continuity management (4 controls);
14. A.18: Compliance (with internal requirements, such as policies, and with external requirements, such as laws) (8 controls).

These 14 control domains define the main areas of ISM framework content therefore we will use it a second level criteria as first level criteria "content of the ISM framework" sub-criteria.

Criteria for "ISM framework applicability in small and medium enterprise" does not have a clear reference model. There are no standards related to framework applicability in small and medium enterprise. Meanwhile the research papers are more concentrated on enterprise factors rather than the framework. For example, the S. C. Eze et al. (Eze et al., 2018) research "Key success factors influencing SME managers' information behavior on emerging ICT (EICT) adoption decision making in UK SMEs" derived 16 key success factors influencing small business managers' information behavior on emerging information and communication technologies. However, the factors defined the SME or its employee's properties rather than the properties of EICT. Therefore, for the ISM framework applicability in small and medium enterprise we proposed some second level criteria by ourselves. It is very basic in order to be adaptable for different type or purpose ISM frameworks and defines the ISM framework properties, influencing its easy integration into SME. The second level criteria are:

Guidelines. In order to adapt the ISM framework its content has to be understood correctly by the SME. Therefore, the presentation of ISM framework has to be taken into account. Guidelines include clear documentation of the ISM framework. It might include some examples, visualizations or even trainings in order to help understanding and integrating the framework. It is important to all type of enterprise; however, it is very important to SME as it is lacking resources to analyze the ISM framework for a longer time, it must be as clear as possible from the first introduction to it.

Community. Even if the ISM framework is fully acquired, some SME specific situations might be tricky and require additional consultations. Therefore, it is important to have a community, which could help in discussion requiring situations. Big enterprises might buy additional training or consultations, meanwhile SME are lacking of resources therefore publicly available and free of charge solutions are desired. The community might be defined by the popularity of the ISM framework as it leads to the bigger number of persons, able to share their experience. Forums or live help systems for the ISM framework information sharing might help and define the community possibilities.

Tools. Information security management might be done by using human resources only, however specified tools might simplify the information security management process. Therefore, an ISM framework with dedicated or recommended tools leads to more modern information security management. The purpose of ISM framework dedicated or recommended tools might vary from logging to modeling, situation evaluation or even decision support. SME would be able to

adapt the tools and reduce the cost of manual information security management processes.

In total there are 2 first level criteria and 17 second level criteria in our proposed analytic hierarchy process (see 0). All criteria have descriptions in order to understand what should be taken into account in order to evaluate it.

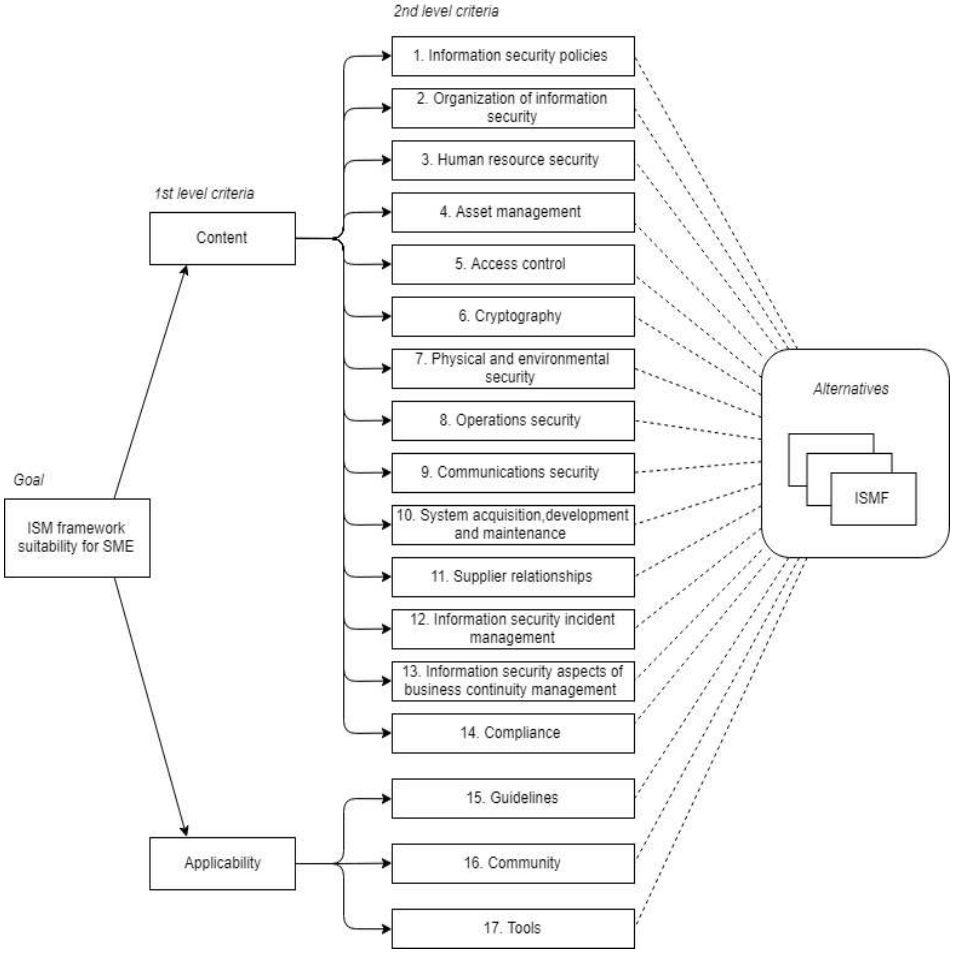


Fig. 4.21. Proposed AHP structure for evaluation of information security management framework suitability for usage in small and medium enterprise

The proposed analytic hierarchy process will be used for estimation of its weights and evaluating the information security management framework quality and suitability to be applied in small and medium enterprise.

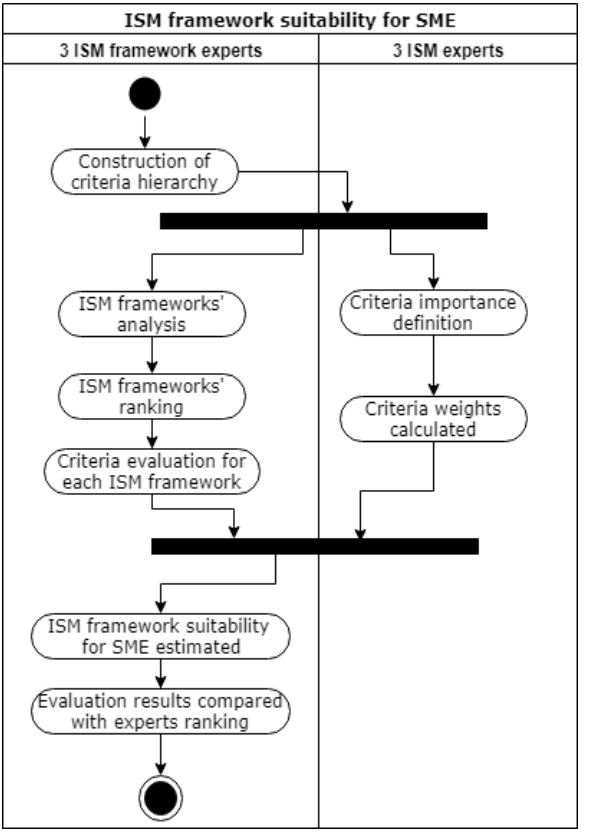


Fig. 4.22. Process of the research: criteria hierarchy definition, criteria weight estimation, ISM framework ranking and evaluation according to defined criteria and their weights, MCDM result comparison to experts ranking

Criteria definition is important for alternative comparison, however in multicriteria decision making the importance, weight for each of the criteria has to be estimated. We use the standard methods of AHP technique: define the structure; evaluation the substitutes and criteria; synthesize the priorities. In order to eliminate the unconscious bias two groups of experts were used and the MCDM results were compared to ISM frameworks experts ranking (see Fig. 4.22): as experts of ISM frameworks we prepare the hierarchy of criteria; external information

security management experts evaluate the weights of the criteria; we rank the compared ISM frameworks according to our own believes for its suitability to be applied in SME; we estimate the values of second level criteria for each of compared ISM frameworks; the ISM framework ranking is compared to MCDM result for its validation.

In criteria definition process three information security management experts participated. These three ISM experts have at least 5 years of experience in information security management and currently work in this area. Each ISM expert individually executed the pairwise comparisons of the same level sibling criteria. Traditionally AHP uses nine-point intensity of importance scale. We proposed an alternative solution to define the pairwise importance – dividing the 100% influence between two criteria. ISM expert is able to adjust the values interactively (see. Fig. 4.23) by assuming how the influence of those two criteria should be divided in percentages.

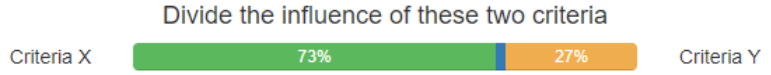


Fig. 4.23. User interface example for executing the pairwise comparison by ISM experts

If the set of criteria are $C = \{ C_i | \, i = 1, 2, \ldots, n\}$, the results of the pairwise comparison of n criteria will be summarized in an evaluation matrix A of size n x n. Every element a_{ij} ($i, j = 1, 2, \ldots, n$) in matrix A is the quotient of weights of the criteria (4.1).

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}, a_{ii} = 1, a_{ji} = \frac{1}{a_{ij}}, a_{ij} \neq 1 . \quad (4.1)$$

As ISM expert opinion is expressed as value from 0 to 100, we transform these values into evaluation matrix values. For transformation from 100% scale to AHP nine-point scale we use an equation 4.2.

$$a_{ij} = \begin{cases} \frac{1}{Z(x_{ij})}, & x_{ij} < 50 \\ Z(50 - x_{ij}), & x_{ij} \geq 50. \end{cases} \quad (4.2)$$

there a_{ij} is a value of matrix A for criteria i and j; x_{ij} is ISM experts proposed influence value for criteria i comparing to criteria j; $Z(x)$ is a scale transformation function, presented in equation 4.3.

$$Z(x) = 1 + \frac{8x}{50}. \quad (4.3)$$

As we used three ISM experts opinion, the evaluation matrix *A* is formed based on the average value of these three ISM experts. The ISM experts were acting individually, however their criteria importance marks in 100-scale were quite similar: maximum difference between opinions of two ISM experts was 15%; standard deviation does not reach more than 9%. The average ISM experts mark was transformed to nine-point system, the evaluation matrix was filled and Eigenvectors were calculated (see Table 4.7). For 1st level criteria one weight is obtained, while for 2nd level criteria local weight is known as well as global weight which is calculated as product of 1st level (parent) and local weight.

Table 4.7. Criteria weights (Eigenvectors), calculated according to ISM experts pairwise evaluation

Criteria		**Weight**	
		Local	Global
ISM framework content		0.817	
	Information security policies	0.115	0.094
	Organization of information security	0.099	0.081
	Human resource security	0.126	0.103
	Asset management	0.054	0.044
	Access control	0.115	0.094
	Cryptography	0.023	0.019
	Physical and environmental security	0.043	0.035
	Operations security	0.095	0.078
	Communications security	0.071	0.058
	System acquisition, development and maintenance	0.051	0.042
	Supplier relationships	0.020	0.016
	Information security incident management	0.103	0.084
	Information security aspects of business continuity management	0.051	0.042
	Compliance	0.033	0.027
Applicability in SME		0.183	
	Guidelines	0.522	0.096
	Community	0.157	0.026
	Tools	0.321	0.059

The ISM experts' criteria pairwise comparison leaded to no intransitive judgments (three-way cycles). This fact shows the ISM experts have a clear understanding of the overall importance of all sibling criteria. The overall dissonance (Chen, 2011) is more than 0 for ISM frameworks content criteria as it has a big number of 2nd level criteria. However the dissonance value is equal to 0.098 and does not require changes.

For ISM frameworks' evaluation we selected 5 alternatives. These five frameworks were analyzed by three ISM framework experts and ranked from the best to the worst. All three ISM framework experts worked together and in discussion derived a consensus, one ranking. The analyzed ISM frameworks were ranked in this order:

1. Holistic information security management framework (Kauspadiene et al., 2017);
2. SABSA framework (Sherwook et al., 2009);
3. An organizational level process model in Information security policy framework (Knapp et al., 2009);
4. Framework for information systems security management based on layered multi-panes (Trcek, 2006);
5. M. M. Eloff and S. H. von Solms hierarchical framework (Eloff et al., 2000).

The ISM framework ranking was done in the beginning to make sure there is no preconception. The ISM framework evaluation criteria were defined after the ranking, so ISM framework experts used its own criteria to evaluate the ISM framework suitability for SME.

After the ISM framework evaluation criteria were defined, a list of criteria and their description was provided for the three ISM framework experts and they had to evaluate all five ISM frameworks according to all seventeen 2nd level criteria. For criteria evaluation ISM framework experts were discussing and deriving a consensus mark. The mark had to be expressed in an interactive system (example provided in Fig. 4.24), using linguistic values. The ISM framework expert opinions expressed in linguistic values are translated into the scale values exhibited in Table 4.8.

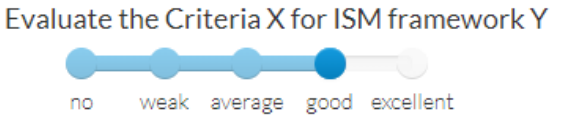


Fig. 4.24. User interface example for executing the defined information security management framework criteria evaluation by framework experts

Table 4.8. Linguistic values and scale values for information security management framework criteria meeting

Linguistic value:	no	weak	average	good	excellent
Scale value:	0.00	0.25	0.50	0.75	1.00

The results of the ISM framework evaluation are presented in Table 4.9. and 0. Both ISM framework experts proposed score values (score) as well as the values, multiplied by the weight of the criteria (weighted score) are presented and summed in the end of the table. According to the sum, ranking was presented. The results prove the ranking according to the sum of not weighted scores do not meet the ranking of ISM framework experts' opinion (the first and the second ISM framework had the same sum of not weighted scores, while the ranking was different by the ISM framework experts; the ranking of the third and the fourth ISM framework according to not weighted scores and ISM framework experts opinion are opposite). Meanwhile the sum of weighted scores is well aligned with the ISM framework experts ranking.

Table 4.9. Results of information security management framework score

2nd level criteria	HISMF	SABSA	Knapp	Trcek	Eloff
1	2	3	4	5	6
Information security policies	1.00	1.00	1.00	1.00	0.00
Organization of information security	1.00	0.50	1.00	0.75	0.50
Human resource security	1.00	0.75	0.50	0.50	0.00
Asset management	0.50	1.00	0.00	1.00	0.00
Access control	0.50	0.75	0.00	0.50	0.00
Cryptography	0.00	0.00	0.00	1.00	0.00
Physical and environmental security	0.50	1.00	0.50	1.00	0.00
Operations security	1.00	1.00	0.75	0.50	0.50
Communications security	1.00	1.00	0.50	0.00	0.00
System acquisition, development and maintenance	1.00	0.75	0.25	0.50	0.50
Supplier relationships	0.50	0.00	0.75	0.00	0.00
Information security incident management	0.00	0.00	0.50	0.00	0.00

End of Table 4.9

1	2	3	4	5	6
Information security aspects of business continuity management	0.75	1.00	1.00	0.50	0.00
Compliance	0.75	0.75	0.75	0.50	1.00
Guidelines	0.50	0.75	0.50	0.50	0.50
Community	0.25	1.00	0.25	0.25	0.25
Tools	1.00	0.00	0.00	0.00	0.00
Sum:	11.25	11.25	8.25	8.50	3.25
Ranking:	1–2	1–2	4	3	5

Analysis of compared ISM framework suitability for small and medium enterprise showed none of the ISM frameworks fully meets the criteria. The maximum quality and applicability value is 71%. This means all of the frameworks have place to improve

Table 4.10. Results of information security management framework weighted score

2nd level criteria	HISMF	SABSA	Knapp	Trcek	Eloff
1	2	3	4	5	6
Information security policies	0.094	0.094	0.094	0.094	0.000
Organization of information security	0.081	0.040	0.081	0.061	0.040
Human resource security	0.103	0.077	0.051	0.051	0.000
Asset management	0.022	0.044	0.000	0.044	0.000
Access control	0.047	0.070	0.000	0.047	0.000
Cryptography	0.000	0.000	0.000	0.019	0.000
Physical and environmental security	0.018	0.035	0.018	0.035	0.000
Operations security	0.078	0.078	0.058	0.039	0.039
Communications security	0.058	0.058	0.029	0.000	0.000
System acquisition, development and maintenance	0.042	0.031	0.010	0.021	0.021
Supplier relationships	0.008	0.000	0.012	0.000	0.000
Information security incident management	0.000	0.000	0.042	0.000	0.000

End of Table 4.10

1	2	3	4	5	6
Information security aspects of business continuity management	0.031	0.042	0.042	0.021	0.000
Compliance	0.020	0.020	0.020	0.013	0.027
Guidelines	0.048	0.072	0.048	0.048	0.048
Community	0.007	0.029	0.007	0.007	0.007
Tools	0.059	0.000	0.000	0.000	0.000
Sum:	**0.716**	**0.690**	**0.512**	**0.500**	**0.182**
Ranking:	**1**	**2**	**3**	**4**	**5**

The coverage and applicability score of other analyzed ISMF varies from 18% to 69% (see Table 4.10) and do not reach the score our proposed ISMF reached (72%). This prove our proposed ISMF covers a wider area of ISM comparing to other existing ISMF.

4.2.2. Information Security Management Framework Introduction to Enterprise

To examine the practical value of this dissertation, a discussion with SME presenters was executed. The discussion aimed to evaluate do presenters of SME understand the proposed ISMF, do they understand how the ISFM should be applied in the SME. Practical application of the proposed ISMF was not executed because of multiple reasons: the process is time and resource consuming, and there were no SME willing to do it for experimental purposes; proposed ISMF application in SME could not be made by thesis author (in order to save SME resources) as SME has security sensitive data and were not willing to let unknown person inside to the enterprise with policy changing actions.

In this discussion, persons from the IT field and different enterprises were asked to participate. There was no filter to make sure the person is responsible for the ISM in the enterprise as this would limit the number of possible candidates because of the lack of persons in this position in SME. However, the IT background was required to ensure the person will be able to understand the basics of ISM.

The experiment was executed in the premises of Vilnius Gediminas Technical University. All participants arrived and spend from 2 to 6 hours in person with experiment executor. During the meeting, some talks, tasks had to be done

by the participant. The experiment with persons who agreed to participate in the experiment consisted of several steps:

1. Experiment executor provided a short list of questions to the participant to log its relevance to ISM and specifics of the enterprise, the person is working in;
2. Later the person was asked to list the main security management weaknesses and countermeasures, which could be used to fix the situation in his or her organization;
3. Experiment executor introduced the participant with the proposed ISM framework. It was an oral presentation with some additional visual materials. The presentation lasted about 10 minutes. Any questions the participant had regarding the framework were answered during the presentation as well;
4. The participant was asked to try to adapt the framework to its enterprise. The adaptation was more like a discussion, bidirectional question and answer session. The participant was able to use any tools, take notes or ask the experiment executor to demonstrate some situations by selected tools. This phase was not logged because of high occupation of the experiment executor;
5. The participant was asked to answer the same questions as in phase 2 in order to analyze the difference of ISM understanding in the specific enterprise;
6. The experiment ended with an open question for the participant to summarize the experience of this experiment.

This scheme of the experiment was selected to measure the perception of the ISM framework for non-security experts to apply it for information security management and improvement in the SME. To utilize existing examples, an ensure similarity between analyzed enterprises, all enterprises were selected to work in the web development sector.

It is worth noting the experiment was executed in Lithuania and Lithuanian language was used in the experiment.

Five persons of different enterprises participated in the experiment. The size of enterprise they work varies from 2 persons to up to 300 (answers were 2, 10, 12, ~200, ~ 300). According to the European Commission, the company of 2 persons should be treated as micro, while the enterprise with more than 250 employees is too big for the medium-size enterprise. However, we left those two cases to see is it applicable for micro companies also. The two biggest enterprises have a position for ISM. The head of the rest three enterprises states the security assurance is part of the IT administrators work. Meanwhile, the rest two persons say there is no person in the company, whose responsibility would be to take care security questions and issues. According to it – medium enterprise in Lithuania

understands the importance of security management and has positions for it. Meanwhile, small and micro enterprises do not have enough resources for them.

The second phase of the experiment was dedicated to gathering initial thoughts on enterprise security. As the primary research trend in the security area is hardware/software security, we expected similar results from enterprise presenters too. However, one person only mentioned threats related to hardware and software vulnerabilities (see Table 4.11). It is interesting the enterprise owners only mention the lack of resources as the main threat to security. The opinion the lack of resources is the foremost important remains even after the introduction to the ISM framework, however before the experiment, they noted the need of money; meanwhile, after the experiment they mention the lack of time, additional work.

Analyzing the changes of opinion on main threats before and after the experiment, it is noted that the person, who stated the hardware/software vulnerabilities are the most important, now thinks the security policies and stakeholders are the most important. The stakeholders were not mentioned as a threat before the experiment; meanwhile, after the experiment, two persons say it in the second place. This is interesting as the ISM framework adds communication with stakeholder as one of the components, which have to be considered in ISM.

The two presenters of the biggest enterprises in the experiment stayed with the same opinion – the security policies are the main component in enterprise security. From these results, it seems the medium or bigger enterprise has no benefits from the ISM framework as they stay with the same opinion.

Table 4.11. Framework usability experiments summarized data

Enterprise data			Answers on main threats in the enterprise	
Number of employees	Position of enterprise presenter	Is there IS department?	Before the framework usage	After the framework usage
2	Owner, programmer	No	Lack of resources	Lack of resources, specifics of the enterprise
10	Programmer	No	Hardware/ software	Security policies, stakeholders
12	Owner, designer	No	Lack of resources	Lack of resources, stakeholders
~200	Programmer	Yes	Security policies	Security policies
~300	Quality assurance engineer	Yes	Security policies	Security policies

However, the enterprises were the two persons work, has a department, responsible for security assurance in the enterprise. The ISM is executed in these enterprises; therefore, the persons are introduced with the security management process in the enterprise. This means the proposed ISMF is capable even within a short period to reflect the same main ideas of ISM as departments, responsible for ISM in the enterprise.

As well the fact persons from bigger enterprises stay with the same opinion does not mean the introduction with the proposed ISM frameworks was useless. Both persons from the biggest enterprises in the discussion are not responsible for the ISM in the enterprise; however, both were interested in different tools, which allows security modeling. Those two persons were not sure what should be the initial values of the model, how to apply it, but valued the ability to measure the influence of enterprise process and IT infrastructure parameters and mentioned this could be used as reasoning tool during the personnel teaching (in the security area).

The presenters of small and micro enterprise mentioned the framework and tools are useful for security level incensement in the enterprise, however, would like to have even more automated systems, with recommendations how exactly the current situation should be improved.

4.3. Conclusions of the Fourth Chapter

1. The comparison of experts ranking and modeling results revealed high correlation (up to 0.97) between experts ranking and ranking, obtained by ordering modeling results. This proves the proposed model is suitable to be used in practice in order to replace experts ranking.
2. In executed experiments the cumulative enterprise security level varies between 21% and 76% for different situations. The range size is wider and similar to integrity values (it ranges between 47% and 92%) as the range of values for data leakage and availability is 19–21%. This fact shows the most sensitive security component is integrity for this enterprise.
3. The executed experiments are not enough to prove the precision of proposed models as there are no unified measures and experts used ranking. However, the models are accuracy as in all except one expert's evaluation had a very close ranking. This show the proposed models can be used for comparison on multiple situations in order to define the better one according to the data confidentiality, availability or integrity.

4. Analysis of a person's opinion on main security threats in his or her enterprise showed the proposed ISM frameworks and usage of recommended tools allows understanding of security policies importance.

General Conclusions

1. The analysis of existing tools and frameworks revealed the lack of solutions, dedicated to SME. Existing solutions concentrate on some specific areas of information security or require an in-depth analysis of provided recommendations and management guidelines. Therefore, it would be difficult to adapt existing solutions in SME for a person with insufficient knowledge in information security.
2. The newly proposed information security management framework consolidates main principles of information security insurance as well add a bigger concentration to different type stakeholders. The attention to stakeholders' existence ensures the information security will reflect the total information security level rather than the situation of isolated from outside communication enterprise while integrated PDCA cycles assure sustainable information technology security in the enterprise.
3. The proposed models for information security estimation (data leakage, data integrity, and data availability) are based on probability theory and its results in analyzed situations closely correlate (up to 0.97) to experts ranking. Experts provided situations rankings and not metrics for security level estimation; therefore, experiment result confirms the accuracy of these models.
4. Proposed analytic hierarchy process in multi-criteria decision making defines weights for information security management framework evaluation criteria

which usage is more suitable for ISM framework ranking than not weighted sum of criteria values.

5. Proposed multi-criteria evaluation method defines a quantitative score of ISM framework suitability to be applied in small and medium enterprise. According to the score, the newly proposed ISM framework outperforms other frameworks (our framework reaches 72%, while the next best fullness is 69% only).

References

Aagedal, J. O., Den Braber, F., Dimitrakos, T., Gran, B. A., Raptis, D., & Stolen, K. (2002). Model-based risk assessment to improve enterprise security. In *Enterprise Distributed Object Computing Conference*, 2002. EDOC'02. 51–62.

Alnuem, M., Alrumaih, H. & Al-Alshaikh, H. (2015). A comparison study of information security risk management frameworks in cloud computing. *Cloud computing*, 103–109.

Altuhhova O., Matulevičius R., Ahmed N. (2012). Towards definition of secure business processes. *International Conference on Advanced Information Systems Engineering*. Springer, Berlin, Heidelberg.

Appling, U. M. L. (2000). Patterns: An introduction to Object–Oriented Analysis and Design and Unified Process, Craig Larman.

Argi-Business Insurance Services. Information Security Risk Assessment Checklist <https://www.abisonline.com/media/cms/RM_Information_Secrity_Risk_Assesm_8B24CD022B2A3.pdf >

Arora, A., Hall, D., Piato, C. A., Ramsey, D., & Telang, R. (2004). Measuring the risk-based value of IT security solutions. *IT professional*, 6(6), 35–42.

Atkinson, C. (2015). Tutorial: Towards Orthographic Enterprise Architecture Modeling. In *Enterprise Distributed Object Computing Workshop* (EDOCW), 164–164. IEEE.

Baer, W. S., & Parkinson, A. (2007). Cyberinsurance in it security management. *IEEE Security & Privacy*, 5(3).

Balamurugan, B., Shivitha, N. G., Monisha, V., & Saranya, V. (2015, February). A Honey Bee behaviour inspired novel Attribute-based access control using enhanced Bell-Lapadula model in cloud computing. In *Innovation Information in Computing Technologies* (ICIICT), 1–6.

Baudry, G., Macharis, C. & Vallée, T. (2018). Range-based Multi-Actor Multi-Criteria Analysis: A combined method of Multi-Actor Multi-Criteria Analysis and Monte Carlo simulation to support participatory decision making under uncertainty. *European Journal of Operational Research*, 264(1), 257–269.

Bell, D. E., & LaPadula, L. J. (1973). Secure computer systems: Mathematical foundations (No. MTR-2547-VOL-1). MITRE CORP BEDFORD MA.

Bjorck, F. (2004). Institutional theory: A new perspective for research into IS/IT security in organisations. *In System Sciences*, 2004. *Proceedings of the 37th Annual Hawaii International Conference on. IEEE.*

Borgman, B., Mubarak, S., & Choo, K. K. R. (2015). Cyber security readiness in the South Australian Government. *Computer Standards & Interfaces*, 37, 1–8.

Botta, D., Werlinger, R., Gagné, A., Beznosov, K., Iverson, L., Fels, S., & Fisher, B. (2007). Towards understanding IT security professionals and their tools. *In Proceedings of the 3rd symposium on Usable privacy and security*, 100–111. ACM.

Bradley, D., & Josang, A. (2004). Mesmerize: an open framework for enterprise security management. *In Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation-Volume* 32, 37–42. Australian Computer Society, Inc..

Buschle, M., Holm, H., Sommestad, T., Ekstedt, M., & Shahzad, K. (2011). A Tool for automatic Enterprise Architecture modeling. *In Forum at the Conference on Advanced Information Systems Engineering* (CAiSE), 1–15. Springer, Berlin, Heidelberg.

Cezar, A., Cavusoglu, H., & Raghunathan, S. (2017). Sourcing information security operations: The role of risk interdependency and competitive externality in outsourcing decisions. *Production and Operations Management*, 26(5), 860–879.

Chinosi, M., & Trombetta, A. (2012). BPMN: An introduction to the standard. *Computer Standards & Interfaces*, 34(1), 124–134.

Chorppath, A. K., & Alpcan, T. (2012). Risk management for it security: When theory meets practice. *In New Technologies, Mobility and Security* (NTMS), 1–5. IEEE.

Common Vulnerability Scoring System v3.0: Specification Document, retrieved from https://www.first.org/cvss/specification-document.

Conventus. SOLVE: More Context. More Relevance. More Detail. 2018 <https://www.conventus.com/solve/>

Danesh, M. H., Loucopoulos, P., & Yu, E. (2015). Dynamic capabilities for sustainable enterprise IT–a modeling framework. In *International Conference on Conceptual Modeling*, 358–366. Springer International Publishing.

Data Leakage Worldwide: The Effectiveness of Security Policies (2014). Retrieved from http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-503131.html

Ekstedt, M., & Sommestad, T. (2009). Enterprise architecture models for cyber security analysis. In *Power Systems Conference and Exposition*, 2009. PSCE'09. IEEE/PES, 1–6. IEEE.

Ekstedt, M., Johnson, P., Lagerström, R., Gorton, D., Nydrén, J., & Shahzad, K. (2015). Securi cad by foreseeti: A cad tool for enterprise cyber security management. In *Enterprise Distributed Object Computing Workshop* (EDOCW), 2015 IEEE 19th International, 152–155. IEEE.

Eloff, J. H., & Eloff, M. (2003). Information security management: a new paradigm. In *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology*, 130–136. South African Institute for Computer Scientists and Information Technologists.

Eloff, M. M., & von Solms, S. H. (2000). Information security management: a hierarchical framework for various approaches. *Computers & Security*, 19(3), 243–256.

Ernawati, T., & Nugroho, D. R. (2012, September). IT risk management framework based on ISO 31000: 2009. In *System Engineering and Technology* (ICSET), 1–8. IEEE.

Ernest Chang, S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3), 345–361.

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, 9(17), 4667–4679.

Eze, S.C. Olatunji, S., Chinedu-Eze, V.C. & Bello, A.O. (2018). Key success factors influencing SME managers' information behaviour on emerging ICT (EICT) adoption decision-making in UK SMEs. *The Bottom Line*, 31(3/4), 250–275.

Faessler M., Morgan M.. (2011). Improving security in risk management. *Jornal of international peace operations*, Volume 7, No. 2.

Farn, K. J., Lin, S. K., & Fung, A. R. W. (2004). A study on information security management system evaluation—assets, threat and vulnerability. *Computer Standards & Interfaces*, 26(6), 501–513.

Fenz, S., & Ekelhart, A. (2011). Verification, validation, and evaluation in information security risk management. *IEEE Security & Privacy*, 9(2), 58–65.

Frank, U. (2014). Multi-perspective enterprise modeling: foundational concepts, prospects and future research challenges. *Software & Systems Modeling*, 13(3), 941–962.

Fredriksen R. et al. (2002). The CORAS framework for a model-based risk management process. *International Conference on Computer Safety, Reliability, and Security*. Springer, Berlin, Heidelberg.

Gilaninia, S., Mousavian, S. J., Taheri, O., Nikzad, H., Mousavi, H., & Seighalani, F. Z. (2012). Information Security Management on performance of Information Systems Management. *Journal of Basic and Applied Scientific Research*, J. Basic. Appl. Sci. Res, 2(3), 2582–2588.

Global data leakage report 2014 (2014). Retrieved from https://infowatch.com/report2014.

Global data leakage report 2015 (2015). Retrieved from https://infowatch.com/report2015.

Goldstein, A., & Frank, U. (2016). Components of a multi-perspective modeling method for designing and managing IT security systems. *Information Systems and e-Business Management*, 14(1), 101–140.

Goranin N., Čenys A. (2008). Genetic algorithm based internet worm propagation strategy modeling. *Information Technology and Control* 37.2.

Gurpreet Dhillon, James Backhouse. Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal* 11.2 (2001): 127–153.

Hawkey, K., Muldner, K., & Beznosov, K. (2008). Searching for the right fit: balancing IT security management model trade-offs. *IEEE Internet Computing*, 12(3).

He, Q., & Antón, A. I. (2003, June). A framework for modeling privacy requirements in role engineering. In *Proc. of REFSQ* (Vol. 3, pp. 137–146).

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, 20(4), 373–384.

Herrmann, M. (2009). Security strategy: From soup to nuts. *Information Security Journal: A Global Perspective*, 18(1), 26–32.

HIMSS Management Engineering & Process Improvement (ME-PI) Community. PDCA (Plan, Do, Check, Act) Checklist. <https://s3.amazonaws.com/rdcms-himss/files/production/public/HIMSSorg/Content/files/PDCAChecklist.pdf >

HITRUST – Health Information trust Alliance (2014). *Comparing the CSF, ISO/IEC 27001 and NIST SP 800-53: Why Choosing the CSF is the Best Choice*. Retrieved from https://hitrustalliance.net/documents/csf_rmf_related/CSFComparisonWhitpaper.pdf

Hohan, A., Pirnea, I. C., & Weber, G. (2014). Case study on implementing an information security management framework in green energy production plant. In *The 3rd International Conference on Quality and Innovation in Engineering and Management*. Cluj-Napoca, Romania (pp. 1–5).

Holm, H., Shahzad, K., Buschle, M., & Ekstedt, M. (2015). P2 CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language. *IEEE Transactions on Dependable and Secure Computing*, 12(6), 626–639.

Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say? *Computers & Security*, 21(5), 402–409.

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, 11(5), 243–248.

Howes, N. R., Mezzino, M., & Sarkesain, J. (2004). *On cyber warfare command and control systems*. MISSILE DEFENSE AGENCY WASHINGTON DC.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information security technical report*, 13(4), 247–255.

Hussain, M., Zaidan, A. A., Zidan, B. B., Iqbal, S., Ahmed, M. M., Albahri, O. S., & Albahri, A. S. (2018). Conceptual framework for the security of mobile health applications on android platform. *Telematics and Informatics*, 35(5), 1335–1354.

Information Commissioner's Office. Controllers checklist, 2018 <https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/controllers-check-list/>

Information security breaches survey 2014, Technical report (2014). Retrieved from https://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf.

Infowatch. Global data leakage report, 2017 <https://infowatch.com/sites/default/files/report/Global_Data_Leak_Report_2017_ENG.pdf >

Jaferian, P., Hawkey, K., Sotirakopoulos, A., Velez-Rojas, M., & Beznosov, K. (2014). Heuristics for evaluating IT security management tools. *Human–Computer Interaction*, 29(4), 311–350.

Janulevičius, J. et al. (2017). Enterprise architecture modeling based on cloud computing security ontology as a reference model. *Electrical, Electronic and Information Sciences* (eStream).

Jastiuginas, S. (2012). Integralaus informacijos saugumo valdymo modelio taikymas Lietuvos valstybės institucijoms. *Informacijos mokslai*, 61.

Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, 28(5), 413–422.

Jouini, M., & Rabai, L. B. A. (2019). A security framework for secure cloud computing environments. In *Cloud Security: Concepts, Methodologies, Tools, and Applications* (pp. 249–263). IGI Global.

Jung, Y., & Chung, M. (2010). Adaptive security management model in the cloud computing environment. In *Advanced Communication Technology* (ICACT), Vol. 2, pp. 1664–1669.

Jürjens, J. (2002). UMLsec: Extending UML for secure systems development. «UML» 2002—*The Unified Modeling Language*, 1–9.

Kajackas A., & Rainys R. (2011). Estimation of critical components of internet infrastructure. *Elektronika ir elektrotechnika*, 110.4, 35–38.

Kalinin, M. O. (2010, September). Permanent protection of information systems with method of automated security and integrity control. In *Proceedings of the 3rd international conference on Security of information and networks* (pp. 118–123). ACM.

Kazim, M., & Evans, D. (2016). Threat Modeling for Services in Cloud. In Service-Oriented System Engineering (SOSE), *2016 IEEE Symposium* (pp. 66–72).

Kiang, A., & Lee D. (2018). System and method for enhanced security and management mechanisms for enterprise administrators in a cloud-based environment. U.S. Patent No. 9,959,420. 1 May 2018.

Kitchenham, B. (2007). Empirical paradigm–the role of experiments. In *Empirical Software Engineering Issues. Critical Assessment and Future Directions* (pp. 25–32). Springer, Berlin, Heidelberg.

Kitchenham, B., Pretorius, R., Budgen, D., Brereton, O. P., Turner, M., Niazi, M., & Linkman, S. (2010). Systematic literature reviews in software engineering–a tertiary study. *Information and Software Technology*, 52(8), 792–805.

Knapp, K. J., Morris Jr, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, 28(7), 493–508.

Ko, E., Kim, T., & Kim, H. (2018). Management platform of threats information in IoT environment. *Journal of Ambient Intelligence and Humanized Computing*, 9(4), 1167–1176.

Lodderstedt, T., Basin, D., & Doser, J. (2002). SecureUML: A UML-based modeling language for model-driven security. «UML» 2002—*The Unified Modeling Language*, 426–441.

Ma, Q., Schmidt, M. B., & Pearson, J. M. (2009). An integrated framework for information security management. *Review of Business*, 30(1), 58.

Malcolmson, J. (2009, October). What is security culture? Does it differ in content from general organisational culture? In *43rd Annual 2009 International Carnahan Conference on Security Technology*.

Manso, C., et al. (2015). *Information security and privacy standards for SMEs.*

Mesquida, A. L., Mas, A., Amengual, E., & Calvo-Manzano, J. A. (2012). IT Service Management Process Improvement based on ISO/IEC 15504: A systematic review. *Information and Software Technology*, 54(3), 239–247.

Mardani, A., Jusoh, A., Zavadskas, E. K., Khalifah, Z. & Nor, K. M. (2015). Application of multiple-criteria decision-making techniques and approaches to evaluating of service quality: a systematic review of the literature. *Journal of Business Economics and Management* 16(5): 1034–1068.

Matulevičius, R. et al. (2010). Comparing quality of security models: a case study. *Local Proceedings of the 14th East-European Conference on Advances in Database and Information Systems*. University of Novi sad, Serbia.

Matulevičius, R. (2017). Security Risk-Oriented BPMN. *Fundamentals of Secure System Modelling*. Springer, Cham, 63–76.

Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E., & Wieringa, R. (2018). An integrated conceptual model for information system security risk management supported by enterprise architecture management. *Software & Systems Modeling*, 1–28.

Maynard, S. B., Ruighaver, A. B., & Ahmad, A. (2011). *Stakeholders in security policy development.*

McGee, A. R., Bastry, F. A., Chandrashekhar, U., Vasireddy, S. R., & Flynn, L. A. (2007). Using the Bell Labs security framework to enhance the ISO 17799/27001 information security management system. *Bell Labs Technical Journal*, 12(3), 39–54.

McLean, J. (1985). A comment on the 'basic security theorem'of Bell and LaPadula. *Information Processing Letters*, 20(2), 67–70.

Michelberger Jr, P., & Lábodi, C. (2012). *After Information Security–Before a Paradigm Change (A Complex Enterprise Security Model).* Acta Polytechnica Hungarica, 9(4), 101.

Mingaleva, Z. & Kapuskina, T. (2009). Institutional aspects of information security in Russian economy. World Academy of Science, Engineering and Technology. *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering,* 3(10), 1843–1849.

Monfelt, Y., Pilemalm, S., Hallberg, J., & Yngström, L. (2011). The 14-layered framework for including social and organizational aspects in security management. *Information Management & Computer Security*, 19(2), 124–133.

Morgan, J. (2015). The 5 Types Of Organizational Structures: Part 2, 'Flatter' Organizations. Retrieved from http://www.forbes.com/sites/jacobmorgan/2015/07/08/ the-5-types-of-organizational-structures-part-2-flatter-organizations/#7519802bca71.

Morimoto, S. (2009). Application of COBIT to security management in information systems development. In *Frontier of Computer Science and Technology*, 2009. FCST'09, 625–630.

Mubarak, S. (2016). Developing a theory-based information security management framework for human service organizations. *Journal of Information, Communication and Ethics in Society*, 14(3), 254–271.

Myler, E., & Broadbent, G. (2006). ISO 17799: Standard for security. *Information Management*, 40(6), 43.

National Vulnerability Database, retrieved from https://nvd.nist.gov/home.cfm.

NetworkAlliance. Understanding Technology Costs (2018) <http://networkalliance.com/understanding-technology-costs/ >

NMAP. Nmap Security Scanner, 2018 <https://nmap.org/ >

Organization Internationale de Normalisation (ISO). ISO 7498-2:1989 (1989). Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.

Palevicius P., Ragulskis M. (2015). Image communication scheme based on dynamic visual cryptography and computer generated holography. *Optics Communications* 335: 161–167.

Parkin, S., Van Moorsel, A., Inglesant, P., & Sasse, M. A. (2010, September). A stealth approach to usable security: helping IT security managers to identify workable security solutions. In *Proceedings of the 2010 New Security Paradigms Workshop*, 33–50.

Pavlov, G., Karakaneva, J. (2011). Information security management system in organizations. *Trakia journal of sciences*, Vol. 9, No 4, 20–25,

Pistoia, M., Fink, S. J., Flynn, R. J., & Yahav, E. (2007, May). When role models have flaws: Static validation of enterprise security policies. In *Software Engineering*, 2007. ICSE 2007, 478–488.

Pullonen, P. Matulevičius, R., Bogdanov, D. (2017). PE-BPMN: Privacy-Enhanced Business Process Model and Notation. *International Conference on Business Process Management*. Springer, Cham.

Rabbani, T. (2016). Empirical Testing of the CySeMoL Tool for Cyber Security Assessment–Case Study of Linux Server and MySQL.

Radanliev, P., De Roure, D., Nurse, J. R., Nicolescu, R., Huth, M., Cannady, S., & Montalvo, R. M. (2018). Integration of cyber security frameworks, models and approaches for building design principles for the internet-of-things in industry 4.0.

Ragulskis, M. Aleksa, A., Saunoriene, L. (2007). Improved algorithm for image encryption based on stochastic geometric moiré and its application. *Optics communications* 273.2, 370–378.

Rainys, R.. (2006). Network and Information Security. Assessments and Incidents Handling. *Elektronika ir Elektrotechnika* 70.6, 69–74.

Ramanauskaitė S. et al. (2015). Modelling influence of Botnet features on effectiveness of DDoS attacks. *Security and Communication Networks*, 8.12, 2090–2101.

Rebollo, O., Mellado, D., Sánchez, L. E. & Fernández-Medina, E. (2011). Comparative analysis of information security governance frameworks: a public sector approach. In *The Proceedings of the11th European Conference on eGovernment–ECEG*, 482–490.

Rhee, H. S., Ryu, Y. U., & Kim, C. T. (2012). Unrealistic optimism on information security management. computers & security, 31(2), 221–232.

Rodríguez, A., Fernández-Medina, E., & Piattini, M. (2007). A BPMN extension for the modeling of security requirements in business processes. *IEICE transactions on information and systems*, 90(4), 745–752.

Saaty, T. L. (1980). *The analytic hierarchy process: Planning, priority setting, resources allocation.* New York, NY: McGraw.

Saaty, T. L., Ozdemir, M. S. & Shang, J. S. (2015). The rationality of punishment–measuring the severity of crimes: an AHP-based orders-of-magnitude approach. *International Journal of Information Technology & Decision Making* 14(01): 5–16.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management*, 39(4), 60.

Sheikhpour, R., & Modiri, N. (2012). A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. *Indian Journal of Science and Technology*, 5(2), 2170–2176.

Shervin Erfani. United States Patent. No. US 6,542,993 B1. Security management system and method. 2003

Sherwood, J., Clark, A., & Lynas, D. (1995). Enterprise security architecture. SABSA, White paper, 2009.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, 46(5), 267–270.

Sommestad, T., Ekstedt, M., & Holm, H. (2013). The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. *IEEE Systems Journal*, 7(3), 363–373.

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, 48(7), 296–302.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, 503–522.

Spremić, M. (2012, June). Corporate IT Risk Management model: A holistic view at managing information system security risks. In Information Technology Interfaces (ITI), *Proceedings of the ITI 2012 34th International Conference on* (pp. 299–304) *IEEE*.

State of Minnesota. Enterprise Information Security Physical & Environmental Protection Standard, 2010 <https://mn.gov/mnit/images/SEC_S_Physical_Security_and_Environmental_Protection.pdf>

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. risk management guide for information technology systems.

Streeter, D. C. (2013). The effect of human error on modern security breaches. Strategic Informer: *Student Publication of the Strategic Intelligence Society*, 1(3), 2.

Suter, M. (2007, May). A Generic National Framework For Critical Information Infrastructure Protection. In *2nd WSIS Action Line C5 Facilitation Meeting* (pp. 1–24). International Telecommunication Union.

The Law of the Republic of Lithuania on Cyber Security, 11/12/2014, No. XII- 1428 <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee>

Thommesen, J., & Andersen, H. B. (2012). Human Error Probabilites (HEPs) for generic tasks and Performance Shaping Factors (PSFs) selected for railway operations. Department of Management Engineering, Technical University of Denmark.

Tohidi, H. (2011). The Role of Risk Management in IT systems of organizations. *Procedia Computer Science*, 3, 881–887.

Tracy, R. P. (2007). IT security management and business process automation: Challenges, approaches, and rewards. *Information Systems Security*, 16(2), 114–122.

Trcek, D. (2006). *Managing information systems security and privacy*. Springer Science & Business Media.

Trèek, D. (2003). An integral framework for information systems security management. *Computers & Security*, 22(4), 337–360.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: research and practice gaps. *Information Security Journal: A Global Perspective*, 17(5–6), 207–227.

Tsoumas, B., & Gritzalis, D. (2006, April). Towards an ontology-based security management. In 20th International Conference on Advanced Information Networking and Applications-Volume 1 (AINA'06), pp. 985–992.

Tweneboah-Koduah, S., & Buchanan, W. J. (2018). Security Risk Assessment of Critical Infrastructure Systems: A Comparative Study. *The Computer Journal*, 61(9), 1389–1406.

Valdevit, T., Mayer,N., Barafort, B. (2009). Tailoring ISO/IEC 27001 for SMEs: A guide to implement an information security management system in small settings. *European Conference on Software Process Improvement*. Springer, Berlin, Heidelberg.

Valstybės kontrolė. The cyber security environment in Lithuania. 9 December 2015, No. VA-P-90-4-16. < https://www.vkontrole.lt/failas.aspx?id=3504>

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), 476–486.

Vermeulen, C., & Von Solms, R. (2002). The information security management toolbox–taking the pain out of security management. *Information Management & Computer Security*, 10(3), 119–125.

Vilma Petrauskienė et al. (2014). Dynamic visual cryptography based on chaotic oscillations. *Communications in nonlinear science and numerical simulation*, 19.1, 112–120.

Von Solms, B. (2001). Corporate governance and information security. *Computers & Security*, 20(3), 215–218.

Von Solms, B. (2001). Information security – a multidimensional discipline. *Computers & Security*, 20(6), 504–508.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23(5), 371–376.

Von Solms, B., & Von Solms, R. (2005). From information security to… business security?. *Computers & Security*, 24(4), 271–273.

Von Solms, R. (1998). Information security management (2): guidelines to the management of information technology security (GMITS). *Information Management & Computer Security*, 6(5), 221–223.

Von Solms, R. (1998). Information security management (3): the code of practice for information security management (BS 7799). *Information Management & Computer Security*, 6(5), 224–225.

Von Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security*, 7(1), 50–58.

Von Solms, S. B. (2005). Information Security Governance–compliance management vs operational management. *Computers & Security*, 24(6), 443–447.

Wang, Y., Li, J., Meng, K., Lin, C., & Cheng, X. (2013). Modeling and security analysis of enterprise network using attack–defense stochastic game Petri nets. *Security and Communication Networks*, 6(1), 89–99.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, 17(1), 4–19.

Wheeler, T. L. (2008). Organization Security Metrics: Can Organizations Protect Themselves?. *Information Security Journal: A Global Perspective*, 17(5–6), 228–242.

Whitson, G. (2003). Computer security: theory, process and management. *Journal of computing sciences in colleges*, 18(6), 57–66.

Wüchner, T., & Pretschner, A. (2012). Data loss prevention based on data-driven usage control. In *Software Reliability Engineering* (ISSRE), 2012 IEEE 23rd International Symposium , 151–160. IEEE.

Zhang, J., Yuan, W. H., & Qi, W. J. (2011, June). Research on security management and control system of information system in IT governance. In *Computer Science and Service System* (CSSS), 2011, 668–673. IEEE.

The List of Scientific Publications by the Author on the Topic of the Dissertation

Papers in the Reviewed Scientific Journals

Kaušpadienė, L.; Ramanauskaitė, S.; Čenys, A. 2019. Information Security Management Framework Suitability Evaluation for Small and Medium Enterprise, *Technological and Economical Development of Economy*. ISSN: 2029-4913. eISSN: 2029-4921. DOI: 10.3846/tede.2019.10298. 2019, p. 1–19.

Kaušpadienė, L.; Ramanauskaitė, S.; Čenys, A.; Janulevičius, J.; Rastenis, J. 2018. Modeling of enterprise management structure for data leakage evaluation, *Information security journal: a global perspective*. London : Taylor & Francis Group. ISSN 1939-3555. eISSN 1939-3547. 2018, Vol. 27, no. 1, p. 1–13. DOI: 10.1080/19393555.2017.1423136. [Emerging Sources Citation Index (Web of Science)]

Kaušpadienė, L.; Čenys, A.; Goranin, N.; Tjoa, S.; Ramanauskaitė, S. 2017. High-level self-sustaining information security management framework, *Baltic journal of modern computing*. Ryga : University of Latvia. ISSN 2255-8942. eISSN 2255-8950. 2017, Vol. 5, no. 1, p. 107–123. DOI: 10.22364/bjmc.2017.5.1.07. [Emerging Sources Citation Index (Web of Science)]

Papers in other Editions

Ramanauskaitė, S.; Raslanaitė, J.; Kaušpadienė, L.; Čenys, A.. Information integrity estimation model for small and medium enterprise // 2018 IEEE. 6th workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), November 8–10, 2018 Vilnius, Lithuania : proceedings / edited by: Dalius Navakauskas, Andrejs Romanovs, Darius Plonis. New York : IEEE, 2018. ISBN 9781728120003. eISBN 9781728119991. p. 1–6. DOI: 10.1109/AIEEE.2018.8592443. [IEEE Xplore]

Summary in Lithuanian

Įvadas

Problemos formulavimas

Informacijos sauga yra vienas esminių kiekvienos įmonės ar organizacijos saugos aspektų. Visi įmonės duomenys turi būti prieinami sėkmingam operacijų vykdymui, paslaugų klientams teikimui. Įmonė privalo užtikrinti savo ir savo klientų duomenų konfidencialumą ir vientisumą. Šių funkcijų užtikrinimui didelės įmonės įsteigia atskirus departamentus. Tuo tarpu mažos ir vidutinės įmonės neturi tam pakankamai resursų, nors privalo kovoti su tomis pačiomis saugos grėsmėmis, kaip ir didelės.

Įmonėse visą informacinių technologijų priežiūrą ir valdymą atlieka informacinių technologijų padaliniai, arba, priklausomai nuo įmonės dydžio, tai gali daryti ir vos vienas asmuo. Informacijos saugos valdymui reikia specifinių žinių ir įgūdžių, tačiau vien jų nepakanka. Bet kokiu atveju, vien žmogiškųjų išteklių neužtenka, todėl papildomi įrankiai, skirti mažoms ir vidutinėms įmonėms, gali pagerinti situaciją, ir iš dalies automatizuoti procesus ar netgi veikti kaip informacijos saugos valdymo sprendimų priėmimo sistema. Tačiau sistema, padedanti smulkiam ir vidutiniam verslui spręsti informacijos saugos valdymo problemas kol kas neegzistuoja, nes nėra pakankamai plačių, informacijos saugos valdymo karkasų bei metodų, skirtų informacijos iš dalies automatizuotam saugos vertinimui.

Darbo aktualumas

Egzistuoja daug įvairių įrankių bei standartų, skirtų informacijos saugos reglamentavimui, rizikos vertinimui ir valdymui. Tačiau dauguma šių įrankių nėra pritaikyti mažoms ir vidutinėms įmonėms ir dengia tik dalį informacijos saugos valdymo procesų. Todėl pritaikyti šiuos įrankius praktikoje yra ganėtinai sudėtingas ir ištekliams imlus uždavinys. Tik iš dalies adaptuojamų informacijos saugos įrankių ar informacijos saugos valdymo sistemos netinkamas palaikymas ar apskritai jo nebuvimas gali baigtis padidėjusiu įmonės informacijos saugos pažeidžiamumu, sugadintais įmonės duomenimis ar paslaugomis, įmonės veiklos sutrikimu, žala įmonės klientams, partneriams, sistemoms, ir kt.

Suteikiant mažai ir vidutinei įmonei labai koncentruotus ir savalaikius informacijos saugos valdymo įrankius, įmonė gali atsilaikyti prieš naujausias saugos grėsmes ir užtikrinti įmonės informacijos saugumą net resursų informacijos saugos valdymui trūkumo atveju.

Tyrimų objektas

Darbo tyrimų objektas – informacijos saugos valdymo karkasai, kuriuos pajėgus taikyti mažas ir vidutinis verslas.

Darbo tikslas

Pagrindinis disertacijos tikslas yra pagerinti informacijos saugos valdymo karkasų ekosistemą, pasiūlant informacijos saugos valdymo karkasą, kuriame išplėsti suinteresuotų šalių ir mažam bei vidutiniam verslui pritaikytų įrankių sąrašai.

Darbo uždaviniai

Darbo tikslui pasiekti ir mokslinei problemai spręsti darbe iškelti šie uždaviniai:

1. Išanalizuoti egzistuojančius informacijos saugos valdymo karkasus;
2. Patobulinti esamus arba sukurti naują informacijos saugos valdymo karkasą, kuris apimtų aukšto lygmens procesus ir išorines suinteresuotas šalis;
3. Sudaryti pasiūlyto informacijos saugos valdymo karkaso įgyvendinimui reikiamus saugos vertinimo modelius, siekiant automatizuoti ir supaprastinti karkaso naudojimą mažoms ir vidutinėms įmonėms;
4. Įvertinti pasiūlyto informacijos saugos valdymo karkaso ir siūlomų įrankių tinkamumą mažo ir vidutinio verslo informacijos saugos valdymo tobulinimui.

Tyrimų metodika

Darbe taikomi lyginamosios analizės ir literatūros analizės metodai naudoti siekiant išanalizuoti informacijos saugos valdymą ir egzistuojančius informacijos saugos valdymo karkasus. Eksperimentinių tyrimų metodai naudojami pagrįsti pasiūlytų informacijos

saugos valdymo idėjų tinkamumą. Klasifikavimo ir statistikos metodai buvo naudojami tyrimų ir analizių rezultatų apdorojimui bei pateikimui.

Darbo mokslinis naujumas

Darbo mokslinis naujumas pagrįstas šiais rezultatais:

1. Sudarytas naujas informacijos saugos valdymo karkasas, susisteminantis esmines informacijos saugos valdymo praktikas bei apjungiantis visus suinteresuotų šalių tipus, siekiant užtikrinti informacijos saugos valdymą. Siūlomo karkaso pritaikomumas mažam ir vidutiniam verslui padidinamas pateikiant tam reikalingų įrankių sąrašą;
2. Parengti informacijos saugos įvertinimo modeliai, padedantys atvaizduoti informacijos srautų ir žmogiškųjų faktorių poveikį informacijos saugai. Šio modelio naudojimas leidžia įvertinant tiek techninės ir programinės įrangos, tiek informacijos srautų bei žmogiškojo faktoriaus įtaką informacijos saugos lygiui.

Darbo rezultatų praktinė reikšmė

Pasiūlytas informacijos saugos valdymo karkasas, kartu su naujai pasiūlytais ir jau egzistuojančiais įrankiais, reikalauja mažiau resursų, siekiant įvertinti ir sumodeliuoti mažos ir vidutinės įmonės informacijos saugos valdymą. Maža ir vidutinė įmonė, naudodama pasiūlytą karkasą ir įrankius gali sumažinti išlaidas informacijos saugos valdymui, nes nereikalingas ekspertinis vertinimas. Siūlomų įrankių pagalba maža ir vidutinė įmonė gali palaikyti pakankamą ar net didinti įmonės saugos lygį, nes naudodamasi įrankiais, o ne ekspertų vertinimu, gali paprasčiau modeliuoti skirtingas situacijas ir jas lyginti tarpusavyje.

Ginamieji teiginiai

1. Įvairių tipų suinteresuotų šalių įtraukimas į Informacijos saugos valdymo karkasą leidžia užtikrinti platesnę informacijos saugos valdymo sritį įmonėje ir padidinti saugos politikos svarbos suvokimą saugos užtikinimui;
2. Tikimybiniai metodai leidžia mažo ir vidutinio verslo atvejais nustatyti informacijos saugos lygį ir pakeisti ekspertų atliekamą informacijos saugos rizikų vertinimą, taip sumažinant Informacijos saugos valdymo kaštus;
3. Informacijos saugos valdymo karkasų tinkamumo taikyti mažame ir vidutiniame versle įvertinimui reikalinga daugiakriterinė analizė ir hierarchinis analizės procesas (*AHP*).

Darbo rezultatų aprobavimas

Disertacijos tema yra parengti trys moksliniai straipsniai mokslo žurnaluose, įtrauktuose į *Clarivate Analytics Web of Science* duomenų bazę. Vienas iš šių žurnalų turi citavimo

rodiklį, o du jo neturi. Disertacijos rezultatai buvo aprobuoti dviejose tarptautinėse konferencijose:

1. The 1st IEEE Workshop on Advances in Information, Electronic and Electrical Engineering AIEEE'13, Ryga, Latvija, Lapkričio 26–27, 2013;
2. IEEE International Conference, Hamburgas, Vokietija, Spalio 4, 2018.

Disertacijos struktūra

Disertaciją sudaro įvadas, keturi pagrindiniai skyriai, bendrosios išvados, literatūros šaltinių sąrašas, autoriaus publikacijų disertacijos tema sąrašas, santrauka lietuvių kalba. Darbo apimtis – 114 puslapių neskaitant priedų, tekste yra 37 paveikslai ir 11 lentelių. Rašant disertaciją buvo panaudota 141 literatūros šaltinis.

1. Informacijos saugos valdymas ir egzistuojantys informacijos saugos valdymo karkasai

Informacijos saugos valdymas apima įrankius, ryšius, sąveikas, dokumentaciją, duomenis, technologines ir kitas priemones, kurios padeda užtikrinti minimalų informacijos saugos rizikos lygmenį organizacijos vykstančių procesų tiek viduje, tiek išorėje, kartu užtikrinant veiklos nenutrūkstamumą. Išlaikant sisteminius ir savalaikius informacijos saugos valdymo procesus, organizacija yra pajėgi apsaugoti savo jautrius duomenis, sistemas nuo įsilaužimo, informacijos nutekėjimo ar kitų neigiamų faktorių, kaip, pvz., žmogiškų klaidų, tyčinių ar netyčinių veiksmų.

Disertacijoje dėmesys kreipiamas į tris pagrindinius informacijos saugos aspektus – konfidencialumas, vientisumas ir prieinamumas. *ISO/IEC 27000* informacijos saugos valdymo sistemų standartų grupė Konfidencialumą apibrėžia kaip "Informacija negali būti prieinama ar atskleidžiama autorizuotos prieigos neturintiems asmenims, organizacijoms ar procesams". Vientisumo principo laikymasis užtikrina, kad informacija nebus pakeista nesankcionuotu būdu, sugadinta arba visiškai prarasta. Galiausiai, Prieinamumo principas reiškia, kad informaciniai duomenys bet kada turi būti prieinami autorizuotiems asmenims.

Darbe buvo atlikta sisteminė literatūros analizė, iš dalies vadovaujantis B. Kitchenham (2007) pasiūlyta metodika. Literatūros šaltinių paieška buvo vykdoma skaitmeninėse bibliotekose, tokiose, kaip *ACM*, *InterScience*, *Google scholar*, *IEEE Explore*, *Inspec*, *ISI Web of Science*, *ScienceDirect*, *SpringerLink*. Disertacijoje literatūros apžvalgos dalyje ypatingas dėmesys buvo skirtas straipsniams, kuriuose pateikiami tam tikri konkretūs sprendimai/karkasai informacijos saugos valdymui. Iš viso buvo atlikta 80 straipsnių išsami analizė, pradedant 1998 ir baigiant 2016 metais. Vienas žymesnių autorių, itin daug dėmesio skyręs informacijos saugos valdymui – R. Von Solms. Mokslininkas analizavo ne tik informacijos saugos valdymo procesus, tačiau ir ruošė metodikas informacinių technologijų saugos sistemoms, vykdė įvairius standartų ir metodikų tyrimus. Apibendrinant literatūros straipsnių grupes pagal populiarumą, galima teigti, kad pirmąją vietą užima rizikų valdymo tema. Antroje vietoje – straipsniai, dedikuoti standartų ir metodologijų tyrimams. Trečioje vietoje lieka tyrimai, skirti

integruotų sistemų platformoms, informacinių sistemų koncepciniams modeliams, karkasams. Nuo 2014 m. nebuvo identifikuota iš esmės naujų informacijos saugos valdymo modelių, buvo analizuojamos tik tam tikros specifinės sritys.

Verslo poreikiams sukurtas ne vienas informacijos saugos valdymo modelis/karkasas. Karkasus siūlo mokslininkai, visuotinai pripažintos organizacijos, verslo kompanijos, vyriausybių institucijos, atsakingos už informacinius išteklius ir kt. Visi šie karkasai koncentruojasi į tam tikrą sritį, turi savus specifiškumus. Disertacijoje analizuojami ir tarpusavyje palyginami labiausiai su disertacijos tema susiję informacijos saugos valdymo karkasai. Vieni žymesnių – SABSA modelis, kurį pasiūlė John Sherwood, Andrew Clark ir David Lynas (Sherwood et al., 2005) bei Pietų Australijos Vyriausybės 2014 metais parengtas Informacijos saugos valdymo karkasas. Abu šie modeliai pateikia aiškią karkaso architektūrą bei įvardina konkrečius žingsnius jo diegimui organizacijoje. Tačiau nepaisant šių karkasų išsamumo, pirmasis nėra holistinis ir neapima *ITIL* standarto *4P* elementų (*People, Process, Products, Partners*), o antrasis yra orientuotas į valstybės įmones, todėl sunkiai pritaikomas mažose ir vidutinėse įmonėse.

Karkasų analizė parodė, kad daugiausia jie yra vieno lygmens – organizacijos arba informacijos saugos sistemų. Tai tik patvirtino iškeltą idėją, jog trūksta informacijos saugos valdymo karkaso, kuris atspindėtų šių dienų organizacijų įvairiapusiškumą. Dauguma modelių gali būti pritaikyti tik vienai ar keletui organizacijos dalių/lygmenų, kai tuo tarpu kiti, apimantys visą organizaciją, yra labai abstraktūs, neįvertina suinteresuotų šalių integracijos, partnerių ryšių, išorinės komunikacijos.

Apžvelgiant Lietuvos autorių, tyrinėjančių informacijos saugos valdymą, mokslinius darbus, galima išskirti S. Jastiugino, R. Matulevičiaus, A. Čenio, R. Rainio, N. Goranin, S. Ramanauskaitės darbus. Sisteminę valstybės informacinių sistemų saugos valdymo analizę-auditą atlieka Valstybės kontrolė.

Apibendrinant galima teigti, kad tyrimų rezultatuose informacijos saugos valdymo modeliai užima nemenką dalį, deja ne visi jie atspindi sritis, kurios turėtų būti įtrauktos organizuojant informacijos saugos valdymą. Vienas esminių elementų, kuris nėra atspindėtas – visų suinteresuotų grupių įtraukimas ir jų poveikio organizacijos informacijos saugos valdymui nustatymas.

2. Siūlomas informacijos saugos valdymo karkasas

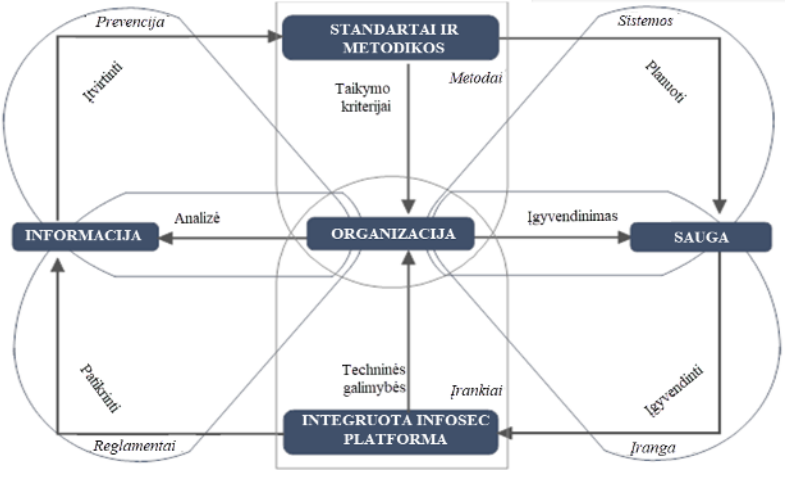
Šiame skyriuje pateikiamas naujas Informacijos saugos valdymo karkasas (ISMF). Šiame skyriuje pateikta analizė buvo publikuota 2017 m. (Kauspadiene et al., 2017).

Naujos kartos informacijos saugos valdymo metu būtina atsižvelgti į šiuolaikinių organizacijų specifiką, jų veiklos principus ir tai, kad jos turi daugybę partnerių, naudojasi bendradarbiavimo sistemomis ir platformomis, perka paslaugas iš trečiųjų šalių (angl. *out-sourcing*) ir kt. Visi šie aspektai reikalauja plataus požiūrio į informacijos saugos valdymą. Siekiant užtikrinti įmonės saugą, turi būti atsižvelgta į platų suinteresuotų šalių ratą. Pasiūlytame karkase naudojamos 7 suinteresuotų šalių kategorijos, neskirstant jų lygmenimis ar formomis: korporatyvinis valdymas, reguliaciniai mechanizmai, profesionalai, IT korporacijos, programuotojai, akademinė bendruomenė, išorės

elementai. Visos šios suinteresuotų šalių grupės gali būti padalintos į dar smulkesnes. Disertacijoje pateikiami jų aprašymai, interesų laukai, atsakomybės sritys. Pasiūlytas karkasas integruoja pagrindinius informacijos saugos valdymo elementus, kurie, kartu su sąsajomis pavaizduoti S2.1 paveiksle. Organizacijos procesų stebėsenai ir valdymui siūloma taikyti karinę doktriną C2 (*Command and Control*), o produkcijos ar paslaugų teikimo užtikrinimui ir nenutrūkstamumui siūloma nuolatos taikyti gerąsias praktikas.

S2.1 pav. Informacijos saugos valdymo karkaso pagrindiniai organizacinio lygmens elementai

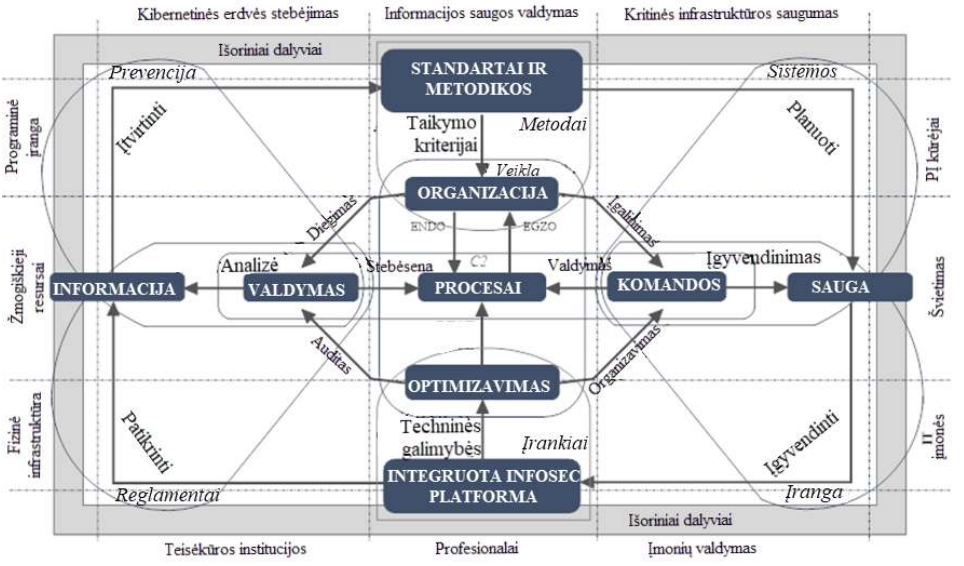
Karkaso veikimo patikimumo ir tęstinumo užtikrinimui buvo pasitelktas Demingo ciklas *Plan-Do-Check-Act*, kuris buvo integruotas į organizacijos saugos lygmenį. Ši integracija pavaizduota S2.2 paveiksle. Priklausomai nuo taikymo kriterijų, atitinkami standartai ir metodikos turi būti pritaikomi organizacijos informacijos saugos valdymui. Karkase pavaizduota informacijos saugos platforma apima fizinius įrankius, naudojamus informacijos saugos sistemos įdiegimui. Dažniausiai informacijos saugos platforma priklauso nuo organizacijos techninių galimybių bei profesionalų, kurie geba tuos įrankius tinkamai valdyti, kas apima ne tik jų kasdieninį valdymą, bet ir organizacijos informacijos srautų analizę, veikimo kontrolę, reagavimą į trikdžius ir kt.



S2.2 pav. Pagrindiniai organizacijos saugos lygmens komponentai

Norint tinkamai suprasti ryšius tarp organizacijos saugos lygmenų komponentų ir informacijos saugos valdymo suinteresuotų šalių bei jų atsakomybių ar funkcijų, kurias jie atlieka, buvo identifikuotos keturios papildomos dalys: (1) prevencija (kibernetinės erdvės stebėsena programinės įrangos lygmenyje; stebėsena vykdoma vadovaujantis teisės aktais ir susideda iš kontrolės ir informacijos elementų, nes tai yra esminės prevencijos komponentai, nusakantys duomenų nutekėjimą, pažeidžiamumą ir t.t.); (2) *reguliaciniai mechanizmai* (juos išleidžia vyriausybės, ministerijos ar kitos įsakymų leidimo galią turinčios organizacijos, o mechanizmų diegimas vykdomas kibernetinės erdvės stebėsenos ir fizinės infrastruktūros lygmenyse, įtraukiant kontrolės ir informacijos elementus tam, kad būtų užtikrintas procesų atitikimas nacionalinei ir tarptautinei teisei (asmens duomenų apsauga, audito procedūros, kibernetinę erdvę reglamentuojantys teisės aktai ir kt.); (3) *sistemos* (programuotojų bendruomenės kuriama programinė įranga); (4) *įranga* (IT korporacijų, gamintojų tiekiama techninė įranga techniniam lygmeniui tarnauja korporatyvinio valdymo aspektu, užtikrinant kritinės infrastruktūros saugą).

S2.3 paveiksle pateiktas karkasas – naujas požiūris, atliepiantis informacijos saugos valdymo procesuose kylančius iššūkius ir itin tinkantis mažoms ir vidutinėms įmonėms. Keturios karkaso dalys atliepia atsparią (angl. *resilient*) kibernetinės saugos sistemą, kuri paremta tarpusavyje susijusiais sąveikaujančiais tinklais. Pasiūlytas informacijos saugos valdymo karkasas yra puikus įrankis informacijos saugos specialistams ir kitiems praktikams ruošiant organizacijoms jų informacinės saugos planus ar programas.



S2.3 pav. Informacijos saugos valdymo karkasas

Pasiūlytas karkasas apibrėžia pagrindinius reikalavimus mažai ir vidutinei įmonei, jos informacijos saugai. Karkaso diegimo metodas labai patogus naudoti naujai kuriamoms ar įkurtoms įmonėms. Tuo tarpu įmonėms su jau nusistovėjusia politika,

valdymo struktūra, gali tekti atlikti vertinimą, siekiant nustatyti kiek procedūrų reikia atlikti, kad pilnai ar iš dalies įdiegtų karkasą savo organizacijoje. Šiuo tikslu buvo paruoštas klausimynas, leidžiantis įvertinti įmonės pasirengimą karkaso diegimui. Kiekvieno klausimo tiksliam ir išsamiam atsakymui buvo parinkti laisvai prieinami įrankiai, kurie padeda objektyviai pateikti atsakymą, išvengiant subjektyvių asmeninių nuomonių. Klausimui „Ar organizacija optimizuoja valdymo ir operacinio (kasdienės veiklos) lygmens procesus?“ nebuvo rasta tinkamų įrankių, todėl organizacija turėtų subjektyviai įvertinti savo pastangas ar jų trūkumą/nebuvimą šioje srityje. Siekiant išvengti subjektyvių vertinimų, kurie galėtų daryti įtaką MVĮ informacijos saugos valdymui, kyla poreikis plėtoti naujus informacijos saugos modelius, leidžiančius vertinti informacijos srautų įtaką bendrai įmonės ar organizacijos informacijos saugai.

3. Informacijos saugos vertinimo įrankiai, skirti mažam ir vidutiniam verslui

Trečiajame skyriuje pateikiama informacijos saugos įrankių vertinimo analizė bei pasiūlomi nauji modeliai. Daugiapakopis organizacijos modeliavimas turi tris aspektus (U. Frank, 2014) – strategija, organizacija, informacinė sistema. Jie gali būti modeliuojami dar keturiais skirtingais aspektais: resursai, struktūra, procesai, tikslai. Kombinuojant šiuos aspektus tarpusavyje galima gauti 12 skirtingų organizacijos modeliavimo būdų.

Anksčiau informacijos sauga buvo laikoma atskira modeliavimo sritimi. Tačiau naujausios tendencijos rodo, kad tikslus saugos vertinimas turi būti tarpdisciplininis. Todėl informacijos saugos integracija į organizacijos modeliavimą yra būtina, įvertinant tai, kad organizacijos yra labai, o kartais ir visiškai priklausomos nuo informacinių technologijų. Taip pat darbe apžvelgiami tokie įrankiai kaip *CySeMoL* (*Cyber Security Modeling Language*), *UML* plėtiniai (*UMLsec*, *SecureUML*), *Petri* tinklai ir kt. Atkreiptinas dėmesys, jog nepavyko identifikuoti įrankių leidžiančių modeliuoti organizacijos procesų ar valdymo struktūros saugumo lygmenis.

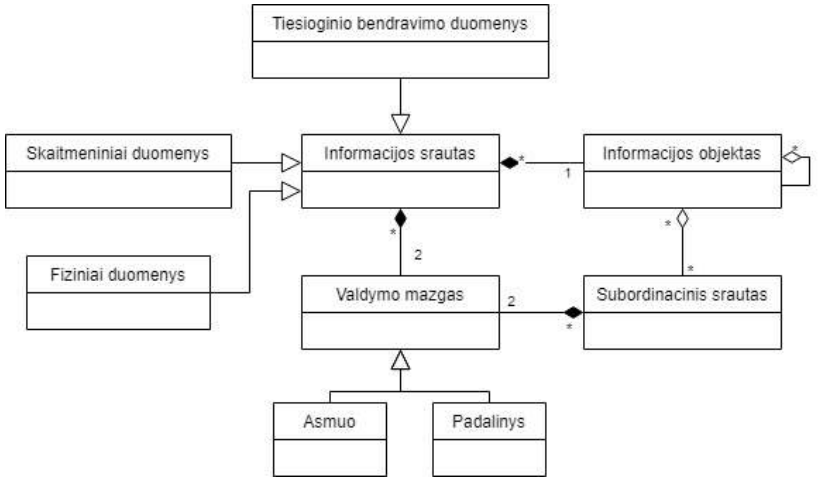
Darbe pasiūlyti organizacijos valdymo struktūros modeliai, atsižvelgiantys į informacijos saugą (konfidencialumas, prieinamumas, vientisumas). Modeliuose įvertinta tiek organizacijos vadyba, tiek informacijos srautai. Modeliai labiau yra orientuoti į vadybą nei į technines organizacijos savybes, todėl dengia tą modeliavimo dalį, kuri dažnai yra praleidžiama modeliuojant organizacijos informacijos saugą.

Pasiūlyti modeliai saugos lygio įvertinimui naudoja sąvoką „subordinaciniai srautai“. Jie nustato organizacijos valdymo mazgų, atsakingų už informacijos tiekimą, tarpusavio pavaldumą, kas iš dalies atitinka skirtingus saugos lygmenis.

Organizacijos valdymo struktūros meta modelis pateikiamas S3.1 paveiksle. Jį sudaro keturios pagrindinės klasės:

1. Valdymo mazgas (*ManagementNode*) – nurodo organizacijos valdymo struktūros elementą). Tai gali būti individas arba departamentas. Priklausomai nuo šio mazgo tipo, yra būtina papildoma informacija, specifikuojanti departamento žmonių skaičių, jų pozicijas organizacijoje ir kt.;

2. Subordinacinis srautas (*SubordinationFlow*) jungia du valdymo mazgus ir suteikia informaciją kuris valdymo mazgas yra tiekiantis informaciją, o kuris – valdantysis;
3. Informacijos objektas (*InformationObject*) apibrėžia objektą, kuris bus siunčiamas organizacijai arba bus jos valdomas. Šis objektas yra susietas su subordinaciniu srautu tam, kad būtų aišku, kokia komanda bus naudojama informacijos perdavimui;
4. Informacijos srauto (*InformationFlow*) objektas apsprendžia informacijos perdavimą iš vieno Valdymo mazgo į kitą. Šiame procese aplinka gali lemti informacijos nuotėkius.



S.3.1 pav. Organizacijos valdymo struktūros modeliavimo meta modelis

Šis meta modelis leidžia sekti informacijos srautus, keliaujančius nuo vieno mazgo prie kito ir taip vertinti kokios savybės kiekvieno veiksmo metu ar mazgo viduje gali keisti atitinkamą saugos komponento (*CIA*) reikšmę.

Darbe taip pat pateikti pasiūlyto modelio duomenų nutekėjimo tikimybės skaičiavimai duomenų perdavimo metu, per tam tikrą organizacijos mazgą (individą, jų grupę ar tam tikrą departamentą).

Toliau darbe pateikiamas prieinamumo įvertinimo modelis. Duomenų prieinamumas priklauso nuo galimų duomenų šaltinių. Jei yra keletas jų, nors ir vienas yra neprieinamas, galima naudotis kitu, kuris duotuoju momentu yra prieinamas. Tai reiškia, kad duomenų prieinamumas apskritai gali būti apskaičiuojamas kaip tikimybė, jog nors vienas duomenų šaltinis tam tikru momentu yra prieinamas. Pirmasis žingsnis vertinant prieinamumą yra organizacijos informacijos valdymo struktūros nustatymas. Sekantis žingsnis – nustatyti informacijos objektus. Vartotojas nustato kiekvieną informacijos objektą pagal jo informacijos srautus ir tam tikrus tų srautų parametrus. Trečiame žingsnyje informacijos objektas padalinamas į skirtingas versijas, ir čia informacijos apdorojimo seka atlieka pagrindinį vaidmenį. Padalinus informacijos objektą į keletą versijų, kiekvieno objekto

versijų duomenų prieinamumas priklauso nuo prieš tai buvusios versijos prieinamumo. Galiausiai ketvirtame žingsnyje analizuojamas kiekvienos objekto versijos prieinamumas.

Formuojant vientisumo vertinimo modelį buvo išskirti trys jį lemiantys veiksniai: informacijos saugojimo aplinka, informacijos perdavimo aplinka ir žmogiškieji veiksniai. Darbe pateikti du atvejai – linijinis informacijos perdavimas bei išsišakojantis informacijos srauto tekėjimas. Abiem atvejais itin jautrus yra žmogiškojo faktoriaus elementas, tuo tarpu informacijos saugojimas ir perdavimas orientuojamas į organizacijos IT infrastruktūrą naudojant CySeMoL EAAT ar kurį kitą įrankį.

4. Siūlomų modelių ir karkaso validavimo rezultatai

Ankstesniame skyriuje buvo pasiūlyti informacijos saugos lygmens apskaičiavimo modeliai, o šis skyrius yra skirtas jų validavimui analizuojant tam tikras situacijas bei pateikiant ekspertines nuomones.

Modelių validavimui buvo atliktas eksperimentas, kurio rezultatais remiantis buvo analizuojami vienos organizacijos skirtingi valdymo būdai – hierarchinis (tradicinis), kuomet informacija didžiąja dalimi perduodama vertikaliais kanalais, ir horizontalus, kuomet informacija dažniausiai perduodama tinkliniu būdu. Iš viso eksperimentui buvo paruošti 8 informacijos perdavimo variantai. Eksperimento rezultatų validavimui buvo pasirinktas ekspertinis vertinimas. Tyrimui buvo atrinkta 15 asmenų, dirbančių informacijos saugos srityje. Juos įvertinus pagal tam tikrus kriterijus buvo atrinkti aštuoni ekspertai tolimesniam ekspertiniam vertinimui. Ekspertams buvo pateikti organizacijos pavyzdžiai bei galimi informacijos perdavimo organizacijos viduje variantai. Situacijų įvertinimui ekspertai galėjo savo nuožiūra pasirinkti vertinimo įrankius ir metodikas. Buvo skirta viena savaitė sureitinguoti informacijos srautus pagal konfidencialumą, vientisumą ir prieinamumą. Ekspertinę nuomonę pateikė šeši ekspertai iš aštuonių.

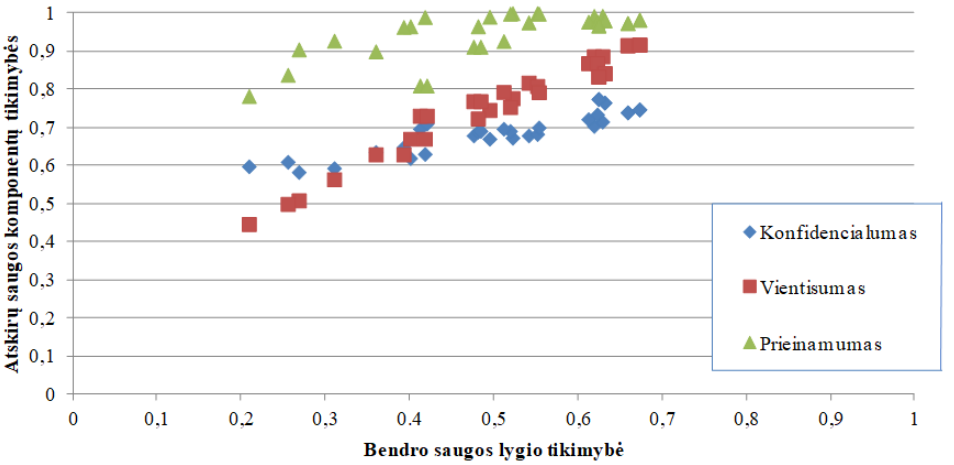
Disertacijoje pateikti skaitiniai informacijos saugos vertinimo rezultatai atsižvelgiant į atliktus duomenų nutekėjimo, prieinamumo ir vientisumo vertinimus. Kiekvienas iš šių aspektų buvo vertintas pagal organizacijos valdymo struktūrą (hierarchinė – su ir be departamentinio valdymo bei horizontali – su ir be departamentinio valdymo). Kiekvienu atveju buvo vertinamos šios informacijos srautų grupės:

- Organizacijos strategija – vadovybės inicijuojama, perleidžiama vadovaujančiam personalui, dalinamasi su klientais;
- Veiklos ataskaita – atskiros dalys generuojamos vadovaujančio personalo, perleidžiama vadovybei ir finansų departamentui;
- Projekto idėja – su į klientus orientuotomis projektų idėjomis dalinamasi su vadovaujančiu personalu, darbuotojais;
- Pradinė projekto kaina – iš dalies sugeneruotą kainą dizaino ir programavimo departamentai (asmenys) siunčia ją vadovaujančiam personalui, šis apdoroja informaciją pagal organizacijos strategiją, įvertina resursus, maržą, ir siunčia ją klientui;
- Detalūs reikalavimai projektui – kliento suformuluoti ir su vadovybe pasidalinti reikalavimai užduočiai atlikti;

- Naudotojų serverių prisijungimo duomenys – IT padalinys suformuoja prisijungimo duomenis ir siunčia juos programuotojams (tiesiogiai arba per vadovybę);
- Sukurtos sistemos dizainas – dizaineris sukuria dizainą ir siunčia jį programuotojui, šis integruoja jį į programos kodą ir siunčia vadovaujančiam personalui, kuris pristato rezultatą klientui;
- Sistemos kodas – programuotojas, pasinaudodamas serverio prisijungiamais įdiegia sistemos dizainą, tada siunčia pirminį kodą vadovaujančiam personalui, o pastarasis jį pristato klientui.

Darbo ketvirtajame skyriuje pateikti ekspertinio reitingavimo palyginimai ir modeliavimo rezultatai atskleidė aukštą (0,97) tarpusavio koreliaciją. Tačiau vienas ekspertas pateikė vieną absoliučiai nekoreliuojančią (-0,06) nuomonę duomenų prieinamumo įvertinimui. Tikėtina, jog šis rezultatas galėjo būti įtakotas klaidinančios konfidencialumo ir prieinamumo elementų kombinacijos.

Skirtingų saugos komponentų (konfidencialumas, vientisumas, prieinamumas) intervalai pateikti S4.1 paveiksle, kur visos reikšmės pateiktos atsižvelgiant į suskaičiuotas saugos tikimybes. Visi trys komponentai turi linijinį priklausomumą, tuo tarpu konfidencialumo ir prieinamumo nuolydžiai yra labai panašūs (0,38 konfidencialumui ir 0,32 prieinamumui), o vientisumo nuolydis yra ženkliai aukštesnis (0,95). Tai parodo, kad vientisumo vertinimo rezultatai yra labai išsibarstę ir turi didesnius verčių diapazonus.



S.4.1 pav. Ryšiai tarp modeliuotų duomenų konfidencialumo, vientisumo ir konfidencialumo verčių, surūšiuoti pagal apskaičiuotas bendras saugumo vertes

Nors atlikti eksperimentai nėra pakankami, norint įrodyti pasiūlytų modelių rezultatų tikslumą, nes buvo taikomas neunifikuotas ekspertinis vertinimas, tačiau modeliai pademonstravo rezultatų panašumą su ekspertų vertinimais, kada didžioji dalis modelio rezultatų koreliuoja su ekspertų nuomone. Tai rodo, kad pasiūlyti modeliai tinkami

naudoti skirtingų situacijų palyginimui. Šio palyginimo metu galima nustatyti geriausiąją alternatyvą pagal duomenų konfidencialumą, prieinamumą ir vientisumą.

Pasiūlytas informacijos saugos valdymo karkasas ir jį lydintys modeliai buvo sudaryti tam, kad supaprastintų informacijos saugos valdymą mažoje ir vidutinėje įmonėje. Taigi, pagrindinis karkaso tinkamumo kriterijus – realus karkaso pritaikymas mažoje ir vidutinėje (MVĮ) įmonėje.

Karkaso suvokimui įvertinti, buvo surengta diskusija su skirtingų organizacijų atstovais. Kiekvienam diskusijos dalyviui buvo skirta nuo 2 iki 6 valandų. Diskusija vyko tokiais etapais:

1. Dalyviui buvo pateiktas trumpas klausimynas, siekiant nustatyti jo sąsajas su informacijos saugos valdymu ir jo atsakomybes organizacijoje;
2. Dalyvis buvo paprašytas įvardinti pagrindines informacijos saugos valdymo silpnybes ir priemones, kurios padėtų pataisyti situaciją jo/jos organizacijoje;
3. Diskusijos vykdytojas pristatė dalyviui Informacijos saugos valdymo karkasą ir atsakė į dalyviui kylančius klausimus;
4. Dalyvio buvo paprašyta adaptuoti karkasą pasirinktoje (kurioje dirba) organizacijoje. Adaptacija vyko diskusijos forma, buvo naudojami brėžiniai. Dalyvis naudojosi visomis galimomis priemonėmis ir įrankiais, galėjo prašyti eksperimento vykdytojo pademonstruoti tam tikras situacijas su pasirinktais įrankiais. Šis procesas dėl ilgos jo trukmės nebuvo nuolatos stebimas diskusijos vykdytojo;
5. Dalyvis buvo paprašytas atsakyti į diskusijos antrojo etapo klausimus, kad būtų galima išsiaiškinti informacijos saugos valdymo supratimo skirtingose organizacijose skirtumus;
6. Diskusijos pabaigoje dalyvis buvo paprašytas apibendrinti patirtį, įgytą eksperimento metu.

S4.1 lentelė. Diskusijoje dalyvavusių asmenų ir jų atsakymų apibendrinti duomenys

Organizacijos duomenys			Respondento nuomone pagrindinės jo įmonei kylančios grėsmės yra	
Darbuotojų skaičius	Dalyvio pareigos organizacijoje	Ar yra už saugą atsakingas padalinys?	Prieš naudojant karkasą	Po karkaso naudojimo (susipažinimo su juo)
1	2	3	4	5
2	Savininkas, programuotojas	Ne	Resursų stoka	Resursų stoka ir įmonės veiklos specifika
10	Programuotojas	Ne	Techninė/ Programinė įranga	Saugumo politika, jos nesilaikymas ir suinteresuotų šalių nepatikimumas

S4.1 lentelės pabaiga

1	2	3	4	5
12	Savininkas, dizaineris	Ne	Resursų stoka	Resursų stoka ir suinteresuotų šalių nepatikimumas
~200	Programuotojas	Taip	Saugumo politika, jos nesilaikymas	Saugumo politika, jos nesilaikymas
~300	Kokybės užtikrinimo inžinierius	Taip	Saugumo politika, jos nesilaikymas	Saugumo politika, jos nesilaikymas

Iš viso diskusijoje dalyvavo penki skirtingų organizacijų darbuotojai. Jų atstovaujamose organizacijose dirba nuo 2 iki 300 žmonių (atsakymai buvo 2, 10, 12, ~200, ~300). Nors dviejų atstovų įmonės yra laikomos mikro įmonėmis, o didelės įmonės darbuotojų skaičius viršija 250, vis tik diskusijoje dalyvauti buvo palikti šių, MVĮ apibrėžties neatitinkančių, organizacijų atstovai tam, kad patikrinti karkaso tinkamumą ir šių dydžių įmonėms.

Surengta diskusija nesuteikė išsamių duomenų informacijos saugos valdymo karkaso taikymo analizei, nes buvo sunku surasti organizacijų, kurios galėtų skirti pakankamai laiko ir resursų karkaso diegimui organizacijos viduje. Tačiau gautas grįžtamasis ryšys iš penkių diskusijos dalyvių buvo teigiamas, ir parodo, kad karkasas yra nesunkiai suprantamas ir gali būti pritaikomas verslo vadovybei priėmus atitinkamus sprendimus. Taip pat nustatyta, kad įmonėse, kuriose jau vykdomas informacijos saugos valdymas, darbuotojai žino pagrindinius informacijos saugos valdymo principus ir suvokia galimas grėsmes, o siūlomame karkase apibendrintos informacijos saugos valdymui svarbios vietos (nuomonė pakito tik įmonių atstovams, kuriose nėra saugos valdymo).

Bendrosios išvados

1. Informacijos saugos valdymo įrankių ir karkasų analizė atskleidė sprendimų, skirtų mažoms ir vidutinėms įmonėms, trūkumą. Aptikti ir nagrinėti sprendimai koncentruojasi į tam tikras labai specifines informacijos saugos sritis arba reikalauja gilios rekomendacijų ar valdymo gairių analizės. Todėl žmonėms, neturintiems pakankamai informacijos saugumo žinių, yra sudėtinga pritaikyti šiuos sprendimus mažoje ir vidutinėje įmonėje.
2. Naujai pasiūlytas informacijos saugos valdymo karkasas apjungia pagrindinius informacijos saugumo užtikrinimo principus bei sukuria pridėtinę vertę įtraukdamas didesnį ratą skirtingų organizacijos suinteresuotų šalių. Dėmesys suinteresuotoms šalims karkase užtikrina, kad informacijos sauga atspindės pakankamą informacijos saugos lygmenį, o integruotas PDCA ciklas užtikrins informacijos saugos valdymo nenutrūkstamumą organizacijoje.

3. Pasiūlytieji informacijos saugos įvertinimo (duomenų nutekėjimas, duomenų vientisumas ir prieinamumas) modeliai yra paremti tikimybių teorija ir analizuotose situacijose jų rezultatai stipriai koreliuoja (iki 0,97) su ekspertiniu vertinimu. Saugos lygio nustatymui ekspertai pateikė ne metrikas, o situacijų reitingavimą, todėl modelių tikslumas negali būti visiškai patvirtintas.
4. Pasiūlytas hierarchinis analizės procesas daugiakriterinei analizei nustato informacijos saugos vertinimo kriterijų svarbą, svorius ir leidžia analizuojamus informacijos saugos valdymo karkasus reitinguoti taip pat, kaip tai darytų ekspertas, kai tuo tarpu vertinamų kriterijų nesvertinė suma neatitinka ekspertų vertinimų.
5. Pasiūlytas daugiakriterinis informacijos saugos valdymo karkasų tinkamumo taikyti mažame ir vidutiniame versle metodas išreiškiamas kiekybiniu matu. Remiantis šiuo matu lyginami analizuojami informacijos saugos valdymo karkasai ir pastebėta, kad naujai pasiūlytas karkasas yra geresnis, nei kiti analizuoti karkasai (pasiūlyto karkaso įvertinimas yra 72%, kai tuo tarpu sekantis geriausias karkasas pasiekė tik 69 % įvertį).

Annexes[3]

Annex A. Author's Declaration of Academic Integrity

Annex B. The Co-Authors' Agreements to Present the Material of Publications as a Part of the Doctoral Dissertation

Annex C. Copies of Scientific Publications by the Author on the Topic of the Dissertation

[3] The annexes are supplied in the attached compact disc.

Laima KAUŠPADIENĖ

INFORMATION SECURITY MANAGEMENT FRAMEWORK
FOR SMALL AND MEDIUM ENTERPRISE

Doctoral Dissertation

Technological Sciences,
Informatics Engineering (T 007)

INFORMACIJOS SAUGOS VALDYMO KARKASAS
SMULKIAM IR VIDUTINIAM VERSLUI

Daktaro disertacija

Technologijos mokslai,
informatikos inžinerija (T 007)

2019 07 22. 12,0 sp. l. Tiražas 20 egz.
Vilniaus Gedimino technikos universiteto
leidykla „Technika“,
Saulėtekio al. 11, 10223 Vilnius,
http://leidykla.vgtu.lt
Spausdino BĮ UAB „Baltijos kopija“
Kareivių g. 13B, 09109 Vilnius