VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

Dmitrij OLIFER

AUTOMATION OF HARMONIZATION, ANALYSIS AND EVALUATION OF INFORMATION SECURITY REQUIREMENTS

DOCTORAL DISSERTATION

TECHNOLOGICAL SCIENCES,
INFORMATICS ENGINEERING (T 007)

Vilnius VGTU LEIDYKLA TECHNIKA 2019

Doctoral dissertation prepared at Vilnius Gediminas Technical University in 2014–2019.

Supervisor

Prof. Dr Arnas KAČENIAUSKAS (Vilnius Gediminas Technical University, Informatics Engineering – T 007).

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

Chairman

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

Members:

Dr Robertas DAMAŠEVIČIUS (Kaunas University of Technology, Informatics Engineering – T 007),
Prof. Dr Habil. Gintautas DZEMYDA (Vilnius University, Informatics Engineering – T 007),
Prof. Dr Habil. Ioan DZITAC (Agora University of Oradea, Romania, Informatics Engineering – T 007),
Dr Rytis MASKELIŪNAS (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 **2 p. 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 sent 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 at the Library of Kaunas University of Technology (K. Donelaičio st. 20, LT-44239 Kaunas, Lithuania).

VGTU leidyklos TECHNIKA 2019-028-M mokslo literatūros knyga

ISBN 978-609-476-184-3

dmitrij.olifer@gmail.com

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Dmitrij OLIFER

INFORMACIJOS SAUGOS REIKALAVIMŲ HARMONIZAVIMO, ANALIZĖS IR ĮVERTINIMO AUTOMATIZAVIMAS

DAKTARO DISERTACIJA

TECHNOLOGIJOS MOKSLAI,
INFORMATIKOS INŽINERIJA (T 007)

Vilnius LEIDYKLA TECHNIKA 2019

Disertacija rengta 2014–2019 metais Vilniaus Gedimino technikos universitete.

Vadovas

prof. dr. Arnas KAČENIAUSKAS (Vilniaus Gedimino technikos universitetas, informatikos inžinerija – T 007).

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

Pirmininkas

prof. dr. Romualdas BAUŠYS (Vilniaus Gedimino technikos universitetas, informatikos inžinerija – T 007).

Nariai:

dr. Robertas DAMAŠEVIČIUS (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. Rytis MASKELIŪNAS (Kauno technologijos universitetas, informatikos inžinerija – T 007).

Disertacija bus ginama viešame Informatikos inžinerijos mokslo krypties disertacijos gynimo tarybos posėdyje **2019 m. rugpjūčio 23 d. 14 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 išsiusti 2019 m. liepos 22 d.

Disertaciją galima peržiūrėti VGTU talpykloje http://dspace.vgtu.lt, 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

The growing use of Information Technology (IT) in daily operations of enterprises requires an ever-increasing level of protection over organization's assets and information from unauthorised access, data leakage or any other type of information security breach. Because of that, it becomes vital to ensure the necessary level of protection. One of the best ways to achieve this goal is to implement controls defined in Information security documents. The problems faced by different organizations are related to the fact that often, organizations are required to be aligned with multiple Information security documents and their requirements.

Currently, the organization's assets and information protection are based on Information security specialist's knowledge, skills and experience. Lack of automated tools for multiple Information security documents and their requirements harmonization, analysis and visualization lead to the situation when Information security is implemented by organizations in ineffective ways, causing controls duplication or increased cost of security implementation. An automated approach for Information security documents analysis, mapping and visualization would contribute to solving this issue.

The dissertation consists of an introduction, three main chapters and general conclusions. The first chapter introduces existing Information security regulatory documents, current harmonization techniques, information security implementation cost evaluation methods and ways to analyse Information security requirements by applying graph theory optimisation algorithms (Vertex cover and Graph isomorphism).

The second chapter proposes ways to evaluate information security implementation and costs through a controls-based approach. The effectiveness of this method could be improved by implementing automated initial data gathering from Business processes diagrams. In the third chapter, adaptive mapping on the basis of Security ontology is introduced for harmonization of different security documents; such an approach also allows to apply visualization techniques for harmonization results presentation. Graph optimization algorithms (vertex cover algorithm and graph isomorphism algorithm) for Minimum Security Baseline identification and verification of achieved results against controls implemented in small and medium-sized enterprises were proposed.

It was concluded that the proposed methods provide sufficient data for adjustment and verification of security controls applicable by multiple Information security documents.

Reziumė

Padidėjus informacinių technologijų (IT) taikymui kasdieninėje organizacijų veikloje, atitinkamai išaugo informacijos ir jos apsaugos įtaka organizacijos veiklai. Dėl šios priežasties informacija, techninė įranga, kuri naudojama jai apdoroti, ir jų apsauga yra itin svarbūs komponentai organizacijų veiklos tęstinumo bei veiklos atstatymo procesų užtikrinimui. Tai galima pasiekti įgyvendinant reikalavimus aprašytus informacijos saugą reglamentuojančiuose dokumentuose. Pagrindinis iššūkis, yra tai kad šiuolaikiniame pasaulyje iš organizacijų dažnai reikalaujama atitikti kelis informacijos saugos dokumentų reikalavimus.

Informacijos saugos užtikrinimas ir valdymas reikalauja nuodugnių žinių apie turimą informaciją, organizacijos turtą bei technologijas. Šiuo metu informacijos saugos įgyvendinimas priklauso nuo informacijos saugos specialistų, jų žinių ir patirties. Toks požiūris į informacijos saugos užtikrinimą įtakoja, kad informacijos saugos užtikrinimas remiasi subjektyviais kriterijais, ko pasekoje organizacijos gali įgyvendinti besidubliuojančias rizikos mažinimo priemones, o saugos užtikrinimo kaštai gali būti neadekvačiai dideli.

Disertaciją sudaro įvadas, trys pagrindiniai skyriai ir bendrosios išvados. Pirmajame skyriuje analizuojami informacijos saugą reglamentuojantys dokumentai, apibrėžiamos harmonizacijos metodikos, įvertinami esami informacijos saugos kaštų vertinimo metodai ir aptariami grafų teorijos algoritmai, kurie yra naudojami grafų pavidalu pateiktos informacijos analizei.

Antrajame skyriuje pristatomas patobulintas kaštų vertinimo metodas, kuris yra orientuotas į rizikos mažinimo priemonių įgyvendinimą. Pateikiami šio metodo automatizavimo būdai, pritaikant automatinius informacijos surinkimo mechanizmus. Taip pat siūlomi būdai, kaip harmonizuota informacija gali būti efektyviai reprezentuota, naudojant egzistuojančias vizualizacijos priemones. Trečiam skyriuje siūlomi metodai leidžiantys automatizuoti kelių Informacijos saugos dokumentų analizę, siekiant suformuoti minimalias saugos gaires ir palyginti gautus rezultatus su organizacijoje įgyvendintais sprendimais. Pateikti metodai grindžiami grafų teorija ir realizuojami naudojant jų padengiamumo algoritmus ir subgrafų izomorfizmo nustatymo algoritmus.

Eksperimentinio tyrimo metu nustatyta, kad siūlomi metodai leidžia automatizuoti kelių informacijos saugos dokumentų analizę, susiejimą, palyginimą ir vizualizavimą.

Notations

Symbols

B – the “Gain of investment”;

B_t – the present value of net benefits of period t;

C – the “Cost of Investment”;

C_{Action} – additional specific tools cost;

$C_{Asset\_analysis}$ – costs related to critical asset analysis;

$C_{configuration}$ – configuration costs;

$C_{consultant}(t)$ – Security consultant costs;

$C_{deployment}(t)$ – are project deployment costs;

$C_{Environment\_purchase}$ – are hardware and software procurement costs;

$C_{Environment\_support}$ – environment support costs;

$C_{Gap\_analysis}$ – costs related to gap analysis;

C_{Impact} – costs related to impact evaluation;

$C_{Implementation}(t)$ – is action implementation costs;

$C_{insurance}$ – cost of insurance, according to the signed off contract with the 3rd party (insurance company);

Complexity level – digital value from 1 to 5;

$C_{Metrics\_control}$ – cost of metrics control operations;

$\mathrm{C}_{Operation}$ – control operation costs;

$\mathrm{C}_{Other\_services}$ – cost of additional services needed for effective control functioning;

$\mathrm{C}_{Penetration\_testing}(N)$ – costs related to penetration testing needed for risk assessment;

$\mathrm{C}_{Personal_i}(t)$ – organization's employee costs and t is time spent to perform the analysis;

$\mathrm{C}_{Risk\_assessment}$ – risk assessment costs;

$\mathrm{C}_{SECURITY}$ – information security cost;

$\mathrm{C}_{Security\_control\_implementation_i}(standard)$ – security control implementation;

C_t – all costs;

$\mathrm{C}_{Threat\_analysis}$ – costs related to threat analysis;

$\mathrm{C}_{Training/Awareness}$ – training/awareness costs;

$\mathrm{C}_{Vulnerabilities\_analysis}$ – costs related to Vulnerabilities analysis;

I – the discount rate;

I_0 – the initial investment for security measure;

I_C – the Implementation cost;

$\mathrm{i}_{\mathrm{calc}}$ – the discount rate;

$\mathrm{Impact}_\mathrm{i}$ – impact recognized for asset i;

j – asset number;

lj – asset affected by a security incident;

Maturity level – digital value from 1 to 5;

$m_i(Risk_i)$ – is control criticality coefficient;

n – the time period;

N – is the number of different organization systems, which have to be tested;

NPV – net present value;

R_B – the baseline risk;

Risk_apetite – is an organization willing to handle the existing risk;

ROI – return on investment;

R_R – the residual risk;

RROI – the rate of return on investment;

$\mathrm{Threat}_\mathrm{i}$ – the threats identified for asset i;

$T(l_j)$ – amount of impacted systems;

$\mathrm{Vulnerability}_\mathrm{i}$ – the vulnerabilities identified for asset i;

$\overline{W}$ – impact average;

α and β – are coefficients which define the percentage of time spent by a consultant for discussion with organization employees and information evaluation;

$\Delta\mathrm{E}(\mathrm{L}_\mathrm{t})$ – the reduction in an expected loss in t;

$\Delta\mathrm{OCC}_\mathrm{t}$ – the reduction in opportunity costs in t;

$\Delta T(t)$ – amount of security incidents during defined time t;

φ – the complexity and maturity coefficient.

Abbreviations

ACME – A Company Making Everything;
AMSS – Adaptive Mapping of Security Standard;
ANSI – American National Standards Institute;
BPMN – Business Process Model and Notation;
CIRA – Customer identification and Risk Assessment;
CIS – The Center for Internet Security;
CMM – Capability Maturity Model;
COBIT – Control Objectives for Information and Related Technology;
COSO ERM – The Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk management;
DCG – Deployed Controls Graph;
DFD – Data Flow Diagram;
EMCA – Everything Making Company;
EPC – Event-Driven process Chains;
FIPS – Federal Information Processing Standard;
FISMA – Federal Information Security Management Act;
GDPR – General Data Protection Regulation;
HIPAA – Health Insurance Portability and Accountability Act;
IEEE – Institute of Electrical and Electronics Engineers;
ICFR – Internal Control on Financial Reporting;
ISACA – Information Systems Audit And Control Association;
ISMS – Information Security Management System;
ISO/IEC – International Organization for Standardization / International Electrotechnical Commission;
ISRAM – Information Security Risk Assessment Model;
ISSA – Information Systems Security Association;
MSB – Minimum Security Baseline;
NIST – National Institute of Standards and Technology;
NISTIR – NIST Interagency/Internal report;
NPV – Net Present Value;
PCI DSS – Payment Card Industry Data Security Standard;
PDCA – Plan Do Check Act;
PHI – Protected Health Information;
RAD – Role Activity Diagram;
ROI – Return on Investment;
RROI – Rate of Return on Investment;
SME – Small and Medium-sized Enterprises;
SOX – Sarbanes – Oxley Act;

UML – Unified Modeling Language.

Domain Specific Definitions

Asset – A major application, general support system, high impact program, physical plant, mission-critical system, personnel, equipment, or a logically related group of systems (Kissel 2013);

Attack – attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset (ISO 27000: 2014);

Attack Scenario – algorithm or calculation combining one or more measures with associated decision criteria (ISO 27000: 2014);

Control – a measure that is modifying risk. Controls include any process, policy, device, practice, or other actions which modify risk (ISO 27000: 2014);

Cybersecurity – The ability to protect or defend the use of cyberspace from cyber attacks (Kissel 2013);

Data – A subset of information in an electronic format that allows it to be retrieved or transmitted (Kissel 2013);

Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (Kissel 2013);

Information Security Risk – The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems (Kissel 2013);

Risk – effect of uncertainty on objectives. An effect is a deviation from the expected – positive or negative. Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. Risk is characterized by reference to potential events and consequences, or a combination of these and is expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence (ISO 27000: 2014);

Risk Analysis – process to comprehend the nature of risk and to determine the level of risk. It provides the basis for risk evaluation and decisions about risk treatment (ISO 27000: 2014);

Risk Management – coordinated activities to direct and control an organization with regard to risk (ISO 27000: 2014);

Security Requirement – need or expectation that is stated, generally implied or obligatory (ISO 27000: 2014);

Taxonomy – a controlled vocabulary consisting of preferred items, all of which are connected in a hierarchy or polyhierarchy (ANSI 2010);

Threat – a potential cause of an unwanted incident, which may result in harm to a system or organization (ISO 27000: 2014);

Vulnerability – weakness of an asset or control that can be exploited by one or more threats (ISO 27000: 2014).

Contents

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

Introduction

Problem Formulation

Given the increasing amount of cyber attack, the pressure imposed by government regulatory authorities is accumulating since they are concerned with the current situation of information and personal data protection. The main issue in such a case is related to the fact that applied security controls have different effectiveness and cost, and from an organization's point of view, it is critical to ensure that implemented security controls are cost-effective and guarantee the needed level of protection (Correia, Gonçalves and Teodoro 2017).

Another problem, which is common to all organizations, is related to the fact that competitive advantage could be achieved if an organization is aligned with more than one security document (Daud, *et al.* 2018). For example, financial organizations must be compliant with PCI DSS standard requirements (in case they process cardholder data) (PCI 2016) and Sarbanes-Oxley Act (SOX 2002), which is applicable for all organizations providing financial services in the United States of America. The fact that SOX and other security controls can be covered by implementing different frameworks, such as COBIT (ISACA 2013) or COSO (COSO 2013) complicates the situation even more.

Harmonization techniques would help to map multiple security documents and their requirements (Haufea, *et al.* 2016). Such an approach allows us to understand the links between different documents. However, identification of mandatory requirements, needed to ensure sufficient information and data protection, still requires manual review of the harmonized information.

To solve this problem, security documents adaptive mapping through security ontology was proposed. Further security requirements presentation as graph vertices allows the application of graph theory, such as vertex cover and graph isomorphism properties. Vertex cover algorithms enable identification of duplicated requirements (Nirmala, Lekshmi and Nadarajan 2016), whereas subgraph isomorphism allows comparing minimum security baseline requirements with security controls implemented in the organization.

Relevance of the Thesis

Many researches concentrate more on the implementation of Security requirements in narrow areas, rather than reviewing Information security and security controls implementation in symbiosis with already existing processes and controls. Such an approach contributes to ensuring an organization's protection and improving security solution in all its complexity. However, it increases security implementation costs.

To solve this issue, information security specialists need to understand the requirements applicable to their organization by different Information security documents and best practices. It is imperative to understand how implemented controls are related one to another and to what extent they cover the required requirements. The automatic approach, which would allow to automatically harmonize different documents on the basis of already existing knowledge and techniques allowing the comparison of existing controls with the required one, would reduce the subjectivity presented in this process and increase its efficiency.

One of the best ways to do that is to apply graph theory, which makes it possible to effectively visualize existing Information security documents and also enable the use of the graph theory algorithms, such as vertex cover and subgraph isomorphism properties, aimed at analyzing and evaluating information security documents.

The Object of Research

The object of the present study is method for information security documents requirements harmonization and analysis.

The Aim of the Thesis

The aim of this research is to help to identify minimum security baseline for the cases when information security requirements of multiple information security documents or regulations are applied. The proposed solution concentrates on automation of harmonization, analysis, and verification of information security documents and regulations.

The Tasks of the Thesis

To achieve the aim of the thesis, the following tasks had to be accomplished:

1. To review existing information security documents and their requirements and identify methods and techniques for their requirements harmonization, analysis and verification.
2. To propose a method for improvement of evaluating security requirements implementation costs.
3. To propose an improved method for automating harmonization, analysis and verification of multiple information security documents and their requirements.
4. To perform experimental validation of the improved method for automating harmonization, analysis and verification, consisting of Minimum Security Baseline identification and security controls matching processes.

Research Methodology

For the object investigation, the following research methods are chosen:

- Action: theoretical (analysis and synthesis) study has been performed to improve the strategies aimed at finding a solution to the problem.
- Classification: strength, weaknesses and existing gaps presented in the literature have been summarised: the dissertation research object has been recognised and understood.
- Experience: the solution to the problem has been found by intuition and experience.
- Experimental: the hypothesis has been tested by taking a practical test.
- Statistical: conclusions have been drawn collecting, analyzing and explaining the statistical data.

Scientific Novelty of the Thesis

The scientific novelty of this study is specified as follows:

1. A novel control-based method is developed for implementation of information security cost. It includes an extensive definition of the security implementation components and their impact on the organization's overall security landscape.
2. A novel method, based on graph theory and vertex cover algorithm, is used for the analysis of existing Information security documents and ways to identify critical security requirements covered in the set of different documents and best practices.
3. A novel method, based on graph theory, optimisation algorithms and subgraph isomorphism properties,was proposed and used for comparing security requirements of different Information security documents. The proposed method allows identifying how specific requirements are represented and covered in other security documents

Practical Values of the Research Findings

The achieved results are important both from the theoretical and practical points of view for the dynamic and rapidly changing area of information security management, which integrates technological, organizational and physical security measures for information security insurance.

The proposed methods for control-based security implementation costs evaluation, adaptive mapping of security regulatory documents through the proposed security ontology and graph theory based method for Minimum security baseline identification and verification against existing documents demonstrate an interdisciplinary approach, combining both informatics engineering and managerial methods aimed at solving information security insurance tasks. Exceptionally unique is the proposed Minimum security baseline identification method that suggests using graphs for the representation of regulatory documents, which allows utilizing a well-known vertex cover algorithm and graph isomorphism features for automating the task at a later time. The developed tool for visualization of mapped security documents can be directly used by companies for managing the complexity issue and user-friendly representation of the relationship between documents.

Part of the results of the research was financed, implemented and validated as a part of the project "Virtualization, visualization and security in e-service technologies" 2012–2014 program (project code: VP1-3.1-ŠMM-08-K-01-012).

The Defended Statements

The defended statements of this doctoral thesis are as follows:

1. The controls-based cost evaluation approach has to incorporate organization maturity and organization systems complexity levels into the calculation because it allows taking in account organization size and evaluate additional costs, common for the organizations of different sizes.
2. Adaptive mapping through security ontology, incorporating security frameworks and methodologies, allows harmonization of multiple security documents requirements without the need to re-evaluate previously linked data and allows link security requirements from different security areas.
3. Minimum Security Baseline identification from the set of previously harmonized security documents and its verification against implemented controls within an organization could be automated by using Vertex cover algorithm and Graph isomorphism properties.

Approval of the Research Findings

The results of the dissertation were published in 8 scientific publications. 3 of them are published in reviewed scientific journals indexed in Clarivate Analytics (also referred to as Thomson Reuters) Science Citation Index, and 5 are published in conference proceedings. The author has also made 3 presentations at international scientific conferences:

- Business Process Management conference 2017: Business Process Management Workshops. September 10–11, 2017, Barcelona, Spain,
- Electrical, Electronic and Information Sciences (eStream): proceedings of the 2015 Open conference. April 21, 2015, Vilnius, Lithuania.
- 2nd International conference on Information Technology and Science (ICITS 2014). March 27–28, 2014, Shanghai, China.

Structure of the Dissertation

The dissertations consist of an introduction, three main chapters, general conclusions, references, a list of publications by the author on the topic of the dissertation and a summary in Lithuanian. The total scope of the dissertation is 138 pages and includes 35 figures and 22 tables.

1

Information Security Requirements Harmonization, Analysis and Evaluation Methods

This Chapter provides the analysis of published information security documents, frameworks, best practices and other security assurance documentation. Primary attention is dedicated to security controls implementation and assurance for organizations without having a dedicated information security specialist. Organizations are made to seek compliance with a set of applicable security regulations. However, identification of security requirements mandatory for the organizations and decision about how to satisfy them is mostly based on expert knowledge, skills and experience. To ensure cost-effective security implementation, organizations must be able to identify security requirements applicable to them from the set of various security documents, identify existing non-compliances with these requirements and calculate the cost of implemented and missing controls (Sugiura, Suwa and Ohta 2015).

The performed analysis covers existing security costs implementation verification methods. Analysis has been conducted on the principal components of these methods. Their advantages and disadvantages are identified, and their applicability to solving raised problems is validated.

The information provided in is Chapter 1 analyzes existing harmonization techniques, validating their possibility to be used for multiple security documents linking and analysis at a later time. The techniques need to ensure a flexible approach for the increasing set of harmonized documents and re-usage of the previous results. As part of the analysis, visualization of achieved results was reviewed. Visualized information allows quickly and effectively representing information about harmonized documents and highlighting the level of documents, similarity and differences.

A harmonized set of security documents provide a list of all possible requirements; however, they are not suitable for identification of mandatory security requirements, which would allow the organization to be compliant with security requirements without paying extra costs. In this chapter, Minimum security baseline identification methods were analyzed and presented.

Researches provided in the chapter 1 were published in (Ramanauskaite, Olifer, *et al*. 2013) and (Ramanauskaite, Goranin, *et al*. 2013).

1.1. Information Security Documents and Requirements

During the last ten years, the importance of information and data protection increased exponentially and has evolved into a vital organizational process. Security management and organization assets protection are perceived today as one of the key points of an organization's success. According to Dhillon *et al.* (Dhillon and Backhouse 2000), security has become fundamental in our society, and the survival of organizations depends on the correct management of modern security elements. According to the technical report (PricewaterhouseCoopers 2015), average costs of single Information security and Data protection breaches increased twice during the last year, from 600 000 £ in 2014 to 1 460 000 £ in 2015. The results of such analysis explain why the implementation of Information security requirements is so important nowadays. The complexity of this problem creates a situation in which the same data and information could be protected in different ways (Lee, Geng and Raghunathan 2016). From the organization's point of view, it is imperative to make certain that organizations apply "security-in-depth" principles and ensure "due diligence".

One of the best ways to achieve this result is to apply best security practices defined in the different types of security documentation, starting from security methodologies, frameworks and finishing with specific security documents and procedures (Ahanger and Aljumah 2018).

During the analysis, a lot of attention was dedicated to security documentation, which defines security requirements for small and medium-sized enterprises (hereinafter SME). Information security documentation aims to solve critical organizational issues such as:

- Identification of organization maturity level in the security area;
- Recommendation and roadmap for the organization, which seeks to improve organization maturity level in the security area.

Security documentation is trying to cover all main security areas and provide a solution to how one or another security issue or problem could be solved (Lee, Geng and Raghunathan 2012). Document applicability indirectly impacts the level of details defined in information security documents. Because of that some information security documents provide abstract security requirements (for example – "*Organization must ensure users credentials and password management*"), and at the same time other documents define requirements with high level of details (for example – "*Organization password length must be at least 8 symbols and must consist at least one Uppercase symbols, one Lowercase symbol, one number and one special symbol*"). During this analysis, different types of security documentation were identified:

- International standards: ISO 27001 / ISO 27002 (ISO/IEC:27001 2013); PCI DSS – Payment Card Industry Data Security Standard (PCI 2016); FIPS – Federal Information Processing Standards (FIPS 200 2006);
- Information security acts: HIPAA – Health Insurance Portability and Accountability Act (HIPAA 1996); FISMA – Federal Information Security Management Act (E-Government Act 2002); SOX – Sarbanes-Oxley Act (SOX 2002);
- Methodologies: COBIT – Control Objectives for Information and related Technology (ISACA 2013); COSO Internal Control – The Committee of Sponsoring Organizations of the Treadway Commission (COSO 2013);
- Laws: GDPR – General Data Protection regulation (EU regulation 2016);
- Information security publications: NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 2012); NISTIR 7621 – Small Business Information Security – The Fundamentals (NISTIR 7621 2016);
- Security documentation in development: ISSA 5173 – The Security Standard for SME‘s (Information Systems Security Association 2011).

1.1.1. International Standards for Information Security

Some International organizations, such as ISO/IEC, Visa, Mastercard developed and presented information security regulatory documents, which apply to the organization working in the area of their responsibility.

International Organization for Standardization and International Electrotechnical Commission published ISO27000 standards series. This series is also known as the "ISMS Family of standards". ISO27000 standards series is broad in scope and provides best practice recommendations for information security management. This series consists of 46 different standards covering all aspects of information securities starting from privacy, confidentiality and finishing with processes dedicated to solving IT/technical/cyberissues.

The British standard BS7799 was taken as a foundation for ISO27001 and ISO27702 standards. The British standard was reviewed by security experts and published as international standard applicable to organizations working in different industries and having different sizes. ISO27001 standard defines an Information security management system (hereinafter ISMS) and requirements applicable to such a system. ISMS must help the organization to adequately ensure the necessary level of protection, by applying security requirements to different organization processes and procedures (Haufe, *et al.* 2016). ISO27002 standard is named as "*Code of practice for information security controls*" In principle, it is a detailed catalogue of information security controls, which would help to develop and maintain effective ISMS.

To prove the alignment of an organization's processes and controls with ISO 27001 and ISO 27002, an organization could seek ISO/IEC certification. Certification decision is made on the basis of results of the independent audit, performed to verify an organization's ISMS and controls implemented to protect organization environment.

Last time ISO27001 and ISO27002 standards were reviewed in 2013. In 2017 standards were republished (ISO27001 2017). However, the new version didn't define new requirements, and all changes were related to a few minor cosmetic amendments and a slight modification of defined names.

Standards implementation principle is based on Plan–Do–Check–Act (hereinafter PDCA) management method (Fig. 1.1).

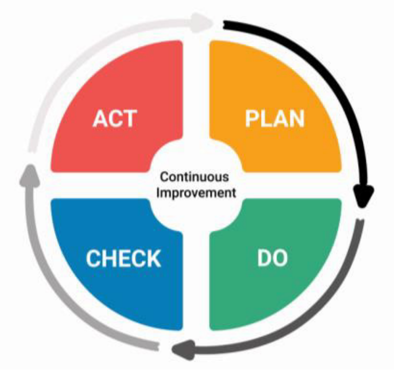


Fig. 1.1. Plan–Do–Check–Act management method (ISO/IEC:27001 2013)

Any changes in ISMS are implemented according to the PDCA management method and must go through the four steps defined below:

- Plan – this step is dedicated to defining policies, procedures and guidelines. Roles and responsibilities are assigned;
- Do – controls, resources and communication routes are defined during this step;
- Check – this step is dedicated to verify implemented controls, check their alignment with requirements; internal audits are performed if needed;
- Act – verification results are presented to management, and improvement priorities and routes are defined.

From a security implementation point of view, ISO27002 is the most relevant standard in ISO27000 standards series. It was slightly amended during 2013 reviewal. The main changes were related to the number of application areas. The previous version of this standard (ISO27002:2005) defined 11 security areas, whereas the new standard defined "Cryptography" and "Supplier management" as independent chapters and the divided chapter "Communications and network management" into 2 separate chapters. The previous version of the standard consists of 133 controls, whereas the new one includes only 114 controls. During the review process, some controls were merged because they covered the same aspect of information security; the others were removed as not relevant anymore.

ISO27002:2013 applicability areas: security policy, an organization of information security; human resources security; asset management; access control; cryptography; physical and environmental security; operations security; communications security; systems acquisition, development and maintenance; supplier relationships; information security incident management; information security aspects of business continuity management; compliance.

ISO 27002 series comprises the most detailed information security standards used for data and the organization's environment protection. Standard requirements apply to all organizations and all industrial sectors (Shojaie 2018). However, each organization must adopt the standards and conditions defined in these standards according to their needs.

Payment card industry data security standard (hereinafter – PCI DSS) (PCI 2016) is an international standard applicable to the payment card industry. This standard was developed by "Visa", "MasterCard", "American Express", "JCB" and "Discover". The primary goal was to standardise security requirements applicable to merchants, acquirers and payment systems and safeguard customer's personal information, including personal confidential information, protection against unauthorized usage, data leakage and data destruction.

PCI DSS defines two types of account data. Cardholder Data includes primary account number (PAN); cardholder name; expiration date and service code.

Sensitive Authentication Data includes full track data (magnetic-stripe or equivalent on a chip); CAV2/CVC2/CVV2/CID; PINs/Pin blocks.

Requirements of this standard are mandatory for organizations (merchants, cards issuers and acquirers) which have interaction with card payment systems. An organization must complete a security self-assessment or security audit process to satisfy licencing requirements. Both methods are helping to verify the security controls implemented in the organization. The decision regarding controls evaluation (self-assessment or external audit) depends on the level of interaction with the payment system. Overall, PCI DSS defines 12 High-level requirements from 6 main security areas: build and maintain a secure network and systems (2 controls); protect cardholder data (2 controls); maintain a vulnerability management program (2 controls); implement strong access control measures (3 controls); regular monitor and test networks (2 controls); maintain an information security policy (1 control).

PCI DSS standard covers fewer security areas compared to ISO27001 series standards. This difference could be explained by standards applicability scopes. PCI DSS is oriented to payment card system customers and their data protection, and all attention is concentrated on the areas which are directly related to payment card systems.

PCI DSS certification is much more rigorous and does not allow free interpretation of existing requirements. One of the main requirements is related to the continuous monitoring of existing controls and continuous security improvement where needed.

Federal Information Processing Standards (hereinafter – FIPS) series standards are publicly available. These standards apply to the United States of America government organizations and in principle are developed by accumulating security requirements defined and published by such well-known organizations as ANSI, IEEE and ISO/IEC.

FIPS standards are aligned with the Federal Information Security Management Act and are mandatory for the United States of America Government and Federal Institutions. The FISMA law mandated the development of federal standards for (i) the security categorisation of federal information and information systems based on their risk levels to provide the appropriate level of security for each system, and (ii) the minimum security requirements for each category.

FIPS 200 (FIPS 200 2006) addresses the specification of minimum security requirements for federal information and information systems. FIPS 199 (FIPS 199 2004) addresses the classification used for systems segregation. It divides the systems into high, moderate, and low impact systems based on their impact on individuals and organizations.

From Security implementation and Assurance point of view, the most interesting are FIPS 200: Minimum Security Requirements for Federal Information and Information Systems and NIST 800-53 (NIST 800-53 2012), which define security requirements and the ways of their implementation.

FIPS 200 highlighted 17 main security areas: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; system and services acquisition; system and communications protection; system and information integrity.

A lot of security areas are similar to the security areas defined by ISO27001 and ISO27002 standards. It is even more important that ISO27000 series standards apply to all industry sectors, and FIPS series standards are dedicated to the USA government.

1.1.2. Information Security Regulating Acts

Some governments, concerned with the challenge of information security regulation, propose to enforce controls applicable to the information security protection. Such security requirements were defined as support documents for the signed acts (Srinivas, Das and Kumar 2019). Acts define high-level requirements and fines, which will be applied if the organization breach these rules.

The Federal Information Security Management Act (hereinafter – FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or human-made threats. FISMA was signed into law as part of the Electronic Government Act of 2002 (E-Government Act 2002). In 2014 it was reviewed and renamed to the Federal Information Security Modernization Act (E-government Act 2014).

Main requirements are to: ensure that security implementation is a continuous process; define the roles and responsibilities of accountable security persons; and ensure continuous Governance, Risk and Compliance process, which would ensure security controls alignment with defined patterns.

FISMA is a high-level document defining high-level security requirements. Detailed requirements are developed and maintained by the National Institute of Standards and technology (hereinafter NIST) organization, and one of such regulation documents would be Federal Information Processing Standard (hereinafter FIPS) 200 standard which is presented below. According to NIST documentation, the organization needs to implement nine steps to comply with FISMA high-level requirements: Categorise the information to be protected; Select minimum baseline controls; Refine controls using a risk assessment procedure; Document the controls in the system security plan; Implement security controls for applicable information systems; Assess the effectiveness of the security controls once they have been implemented; Determine agency-level risk to the mission or business case; Authorise the information system for processing; Monitor the security controls on a continuous basis.

The above defined nine steps are the main actions, which would ensure alignment with FISMA requirements. However, a specific list of NIST recommendations strongly depends on organizational goals and processes. Depending on the organization's demands, this list could be expanded by other specific requirements important within this particular case.

Some information security documents are dedicated to cover information security for a narrow industry cluster or cover a specific area. We have previously presented documents devoted to the payment system (for example, PCI DSS) and the United States of America government institutions (for example, FIPS 200). Another specific area is Healthcare (Langer 2017). In the United States of America, patient personal data protection is ensured by the Health Insurance Portability and Accountability Act (hereinafter – HIPAA) (HIPAA 1996), (HIPAA 2013). HIPAA defines requirements applicable to all medical institutions and ensures patient privacy, personally identifiable information protection and overall security assurance provided by healthcare institutions.

Although HIPAA document covers a lot of different areas of security assurance and security implementation is defined in below mentioned documents: HIPAA Privacy rule is composed of national regulations for the use and disclosure of Protected Health Information (PHI) in healthcare treatment, payment and operations by covered entities; HIPAA Security rule defines administrative, physical and technical safeguards required to ensure needed level of data protection.

According to HIPAA, the appropriate level of security could be achieved by covering three main areas: Administrative Safeguards (security management process; security personnel; information access management; workforce training and management; evaluation); Physical Safeguards (facility access and control; workstation and device security); Technical Safeguards (access control; audit controls; integrity controls; transmission security).

HIPAA security rules also cover security policies and Security procedures management requirements. However, they are separated from controls mechanisms.

Sarbanes-Oxley Act (hereinafter – SOX) (SOX 2002) is a United States of America federal law, which defines new and expanded requirements for all United States of America public company boards, management and public accounting firms. From the Security point of view, it requires organizations to implement internal control mechanisms, which would ensure the necessary level of security protection.

The Act obligates all companies to implement internal control verification process and to ensure that the internal controls audit report is shared with the government controlling organization. Internal controls report must consist of information about the adequacy of the company's internal control on financial reporting (ICFR).

Due to the fact that the Act requirements and definition are high levels and abstract, re a set of supporting documents and frameworks were developed. Such organizations as Information Systems Audit and Control Association (ISACA) and Committee of sponsoring organizations of the Treadway Commission developed their frameworks COBIT v.5 and COSO Enterprise Risk Management – an Integrated framework to help the organization to meet SOX requirements and be aligned with them.

From the Information security implementation point of view, the frameworks developed by ISACA and COSO were chosen, because they cover detailed requirements applicable for organization security implementation. However, security requirements are a small part of conditions defined by these frameworks.

1.1.3. Laws and Methodologies

Security requirements could be defined and forced by regulations or law. The most famous example of regulation related to information security area is the General Data Protection Regulation (EU regulation 2016).

Some international associations proposed methodologies and framework, which would help an organization to satisfy the requirements defined by information security defined documents.

Trying to protect the personal information of a European Union citizen, the European Union published the General Data Protection Regulation (hereinafter GDPR). This document is a data protection law, which in high level, defines how EU residents' personal information must be stored, handled and processed. From the 25th of May 2018, this law is mandatory for all organizations working with EU citizens' and EU residents' data. GDPR has superseded the Data Protection Directive 95/46/EC.

According to the GDPR, any organization is obligated to apply a risk-based approach and ensure a sufficient level of protection for EU residents' personal data. GDPR "personal data" definition states that: "any information relating to an person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person".

GDPR separated the responsibilities and duties of data Controllers and Processors. Controllers are defined as "the natural or legal person, public authority, agency or another body which, alone or jointly with others, determines the purposes and means of the processing of personal data;" and Processors means:

“a natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller”. Controllers and Processors are required to “implement appropriate technical and organizational measures” taking into account “the state of the art and the costs of implementation” and “the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals” (EU regulation 2016).

From the Security point of view for data protection, GDPR requires to apply controls appropriate to the risk. The Law itself suggests: The pseudonymization and/or encryption of personal data; The ability to ensure ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data; The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident; A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Organizations need to implement controls, which would cover below-highlighted security areas, to achieve the following: identity and access management; data loss prevention; encryption & pseudonymization; incident response plan; 3rd party risk management; policy management.

GDPR breach could lead to the financial fines equal to the greater of 10 million € or 2% of the entity's global gross revenue for violations of record-keeping, security, breach notification, and privacy impact assessment obligations. Obligations related to the legal justification for processing data subject rights, and cross-border data transfers may result in penalties of the greater of 20 million € or 4% of the entity's global gross revenue.

Control Objectives for Information and Related Technology (hereinafter – COBIT) (ISACA 2013) is the methodology developed by the Information Systems Audit and Control Association and defining Information technology management, Information technology security and Information technology audit principles. COBIT v5 was released in 2012. At the end of 2018, COBIT presented a new version of COBIT framework – COBIT 2019. According to ISACA COBIT 2019, based on COBIT 5 and other authoritative sources. COBIT aligned with many related documents and frameworks. From a Security implementation point of view it should be highlighted that COBIT 2019 is aligned with such documents as ISO27000 standards series, The CIS Critical Security Controls for Effective Cyber Defence (Center for Information Security 2018), COSO framework, NIST special publications (800-37 and 800-53), HITRUST Common Security Framework v. 9 (HITRUST 2018). According to COBIT 2019 (ISACA 2019), the governance and management objectives are grouped into five domains.

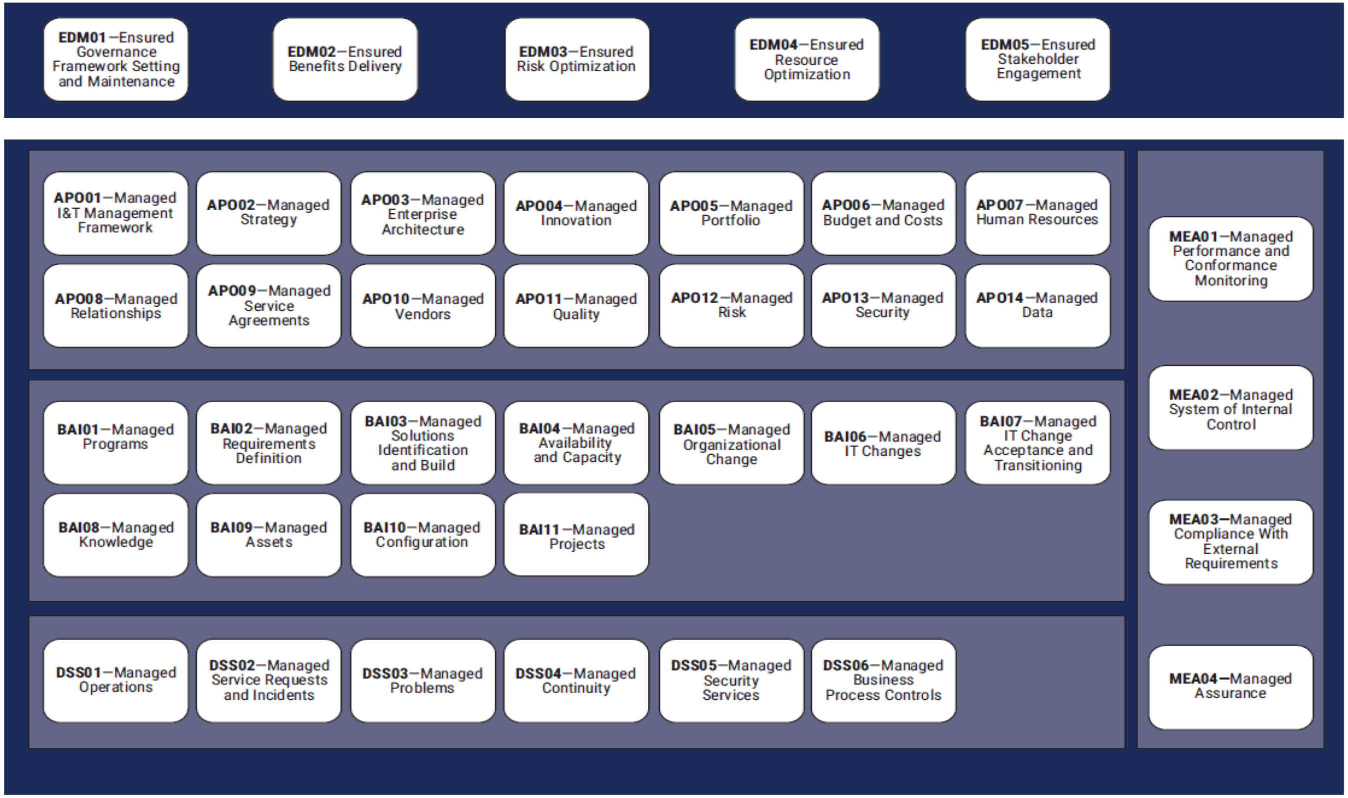

EDM01–Ensured Governance Framework Setting and Maintenance
EDM02–Ensured Benefits Delivery
EDM03–Ensured Risk Optimization
EDM04–Ensured Resource Optimization
EDM05–Ensured Stakeholder Engagement
APO01–Managed I&T Management Framework
APO02–Managed Strategy
APO03–Managed Enterprise Architecture
APO04–Managed Innovation
APO05–Managed Portfolio
APO06–Managed Budget and Costs
APO07–Managed Human Resources
APO08–Managed Relationships
APO09–Managed Service Agreements
APO10–Managed Vendors
APO11–Managed Quality
APO12–Managed Risk
APO13–Managed Security
APO14–Managed Data
BAI01–Managed Programs
BAI02–Managed Requirements Definition
BAI03–Managed Solutions Identification and Build
BAI04–Managed Availability and Capacity
BAI05–Managed Organizational Change
BAI06–Managed IT Changes
BAI07–Managed IT Change Acceptance and Transitioning
BAI08–Managed Knowledge
BAI09–Managed Assets
BAI10–Managed Configuration
BAI11–Managed Projects
DSS01–Managed Operations
DSS02–Managed Service Requests and Incidents
DSS03–Managed Problems
DSS04–Managed Continuity
DSS05–Managed Security Services
DSS06–Managed Business Process Controls
MEA01–Managed Performance and Conformance Monitoring
MEA02–Managed System of Internal Control
MEA03–Managed Compliance With External Requirements
MEA04–Managed Assurance

Fig. 1.2. Control Objectives for Information and Related Technology scheme (ISACA 2013)

fundamental purpose and areas of Governance objectives arranged in the: (Fig. 1.2):

- Evaluate, Direct and Monitor (EDM) domain. In this domain, the governing body evaluates strategic options, directs senior management on the chosen strategic options and monitors the achievement of the strategy.

Management objectives grouped into four domains:

- Align, Plan and Organize (APO) addresses the overall organization, strategy and supporting activities for I&T;
- Build, Acquire and Implement (BAI) treats the definition, acquisition and implementation of I&T solutions and their integration in business processes;
- Deliver, Service and Support (DSS) addresses the operational delivery and support of I&T services, including security;
- Monitor, Evaluate and Assess (MEA) addresses performance monitoring and conformance of I&T with internal performance targets, internal control objectives and external requirements.

EDM processes are owned by senior management and related to organizational strategy and developmental direction.

Other four processes are supportive processes, which allow achieving an organization’s goals and strategies. Each group defines subgroups, which are responsible for specific process implementation, and each subgroup establishes a list of IT controls used to obtain and evaluate requirements outlined and applicable for this group.

Such an approach allows COBIT methodology to interpret and assess all IT processes within an organization and ensure that information security impact on IT processes is within the scope and analyzed during implementation.

Trying to make COBIT framework more attractive to small/medium sized business COBIT 2019 added to scope such new focus areas as CyberSecurity, Digital transformation, Cloud computing, Privacy and DevOps. Also, COBIT 2019 highlights new factors that can influence the design of an enterprise’s governance system and position organizations for success in the use of information and technology (ISACA 2013). These include enterprise strategy; enterprise goals; risk profile; enterprise size; threat landscape; compliance requirements; role of IT; sourcing model for IT; IT implementation methods; technology adoption strategy.

These design factors take into account enterprise strategy and allow users to better customise COBIT to a specific organizational structure.

The Committee of Sponsoring Organizations of the Treadway Commission (hereinafter COSO) Internal Control – Integrated Framework (COSO 2013) and COSO Enterprise Risk Management Framework (COSO 2004) were developed to help organizations to verify the effectiveness of their internal controls and, if needed, to improve them. COSO framework orientation to internal controls allows the organization to use them to satisfy SOX requirements.

According to COSO, all organization employees, including senior management, are responsible for internal controls implementation. COSO defines 3 main areas which are impacting overall internal control effectiveness (Fig. 1.3): operations; reporting and compliance.

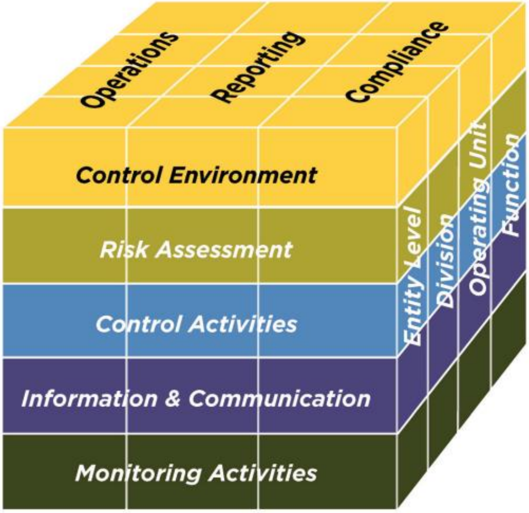


Fig. 1.3. The Committee of Sponsoring Organizations of the Treadway Commission framework approach (COSO 2013)

COSO methodology defines five key components, which allow ensuring the appropriate level of effectiveness: control environment; risk assessment; control activities; information and communication; monitoring.

COSO methodology is more oriented to the organization's processes and implemented internal controls. However, information security is only a small part of all controls which are implemented and processes which are running in the organization. Because of that, COSO frameworks are much broader, and from the perspective of security controls, implementation is not so detailed.

1.1.4. Information Security Special Publications

Many different associations declare information security implementation guidelines. These documents are dedicated to different types of organization and provide advice and recommendations on how one or another security area could be covered or a certain problem solved.

National Institute of Standards and Technology developed NIST SP 800-53 special publication (NIST 800-53 2012). As was stated above, this special publication is FISMA requirements implementation guidance and provides detailed information about controls and ways how they could be applied to reduce identified risk or existing gap.

The document divides all existing controls into three main categories: Low-Impact (115 controls), Medium-Impact (159 controls) and High-Impact (170 controls). It needs to be mentioned that the same control could be exerted in all three categories; it means that control impact level will depend on control applicability scope.

Special publication controls apply to such security areas as access control; awareness and training; audit and accountability; security assessment and authorization; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; system and service acquisition; system and communications protection; system and information integrity.

Revision 4 of the last publication was released on February 28, 2012. NIST SP 800-53revision 5 was developed, and according to existing plans it will be published in March 2019. Annex D. of this document provides a list of all possible controls, Annex F. defines recommendation how this control could be implemented, and Annex H. links existing controls with ISO 27001(ISO/IEC:27001 2013) and ISO 15408 standards. This information allows for developing security implementation roadmap.

Security standard ISSA 5173 (Information Systems Security Association 2011) was developed by the Information Systems Security Association in the United Kingdom in 2011. This Standard is dedicated to SME organizations and specifies minimum security requirements applicable to them.

The Standard highlights three security levels which could be compared with Organization maturity levels, and defines mandatory requirements for each level:

- Basic Security measures (owner/director commitment; understanding obligations; responding to security risks; essential security countermeasures);
- Defined security regime (security rules; security responsibilities; disaster survival plan; security oversight);
- Managed security system (policies and procedures; management system; security technology; security education).

Even though the levels defined and requirements specified in the Standard are abstract and could consist of different aspects of information security, overall, they are in alignment with international standards presented earlier.

NISTIR 7621 rev. 1 publication (NISTIR 7621 2016) was developed by the National Institute of Standards and Technology and dedicated to Small Business. Applicability scope is similar to ISSA 5173 standard presented earlier. Small Business Information Security: The Fundamentals define the following six key components of Information: cybersecurity; privacy; physical security; contingency planning & disaster; operational security; personnel security.

A revised version of this publication provides five main security steps for Cybersecurity assurance; each step has a list of controls which enable to achieve these goals: identify (4 controls); protect (9 controls); detect (2 controls); respond (1 control); detect (4 controls).

Regarding the fact, that this publication is dedicated to small business, requirements defined in it are granulated and assigned to the organization without dedicated security professionals.

To evaluate above defined security documents, we are proposing to use such criteria: Document type; Industry, where security documents requirements are applicable; Amount of covered security areas; level of requirements details defined in the security document; Amount of separate requirements; Security documents requirements applicability to the SME; Security documents requirements applicability to the Enterprises; Possibility to be certified, accredited regarding security document requirements; Obligation from regulatory to apply security document requirements. These criteria were chosen because they allow to present main security documents characteristics and compare them.

This analysis does not include Regional laws and regulations, which are different in each EU country and could have specific requirements applicable in the separate geographical region.

The performed analysis allows concluding, that between security documents criteria exist direct dependencies. Like example, all acts are mandatory and define high-level security principles. Recommendation how defined high-level principles could be meet is provided in the security frameworks or low-level security documents, such as procedures or guidelines. In the same time could be concluded, that healthcare (HIPAA) and financial sectors (PCI DSS) are highly oriented on countermeasures related to the customer's personal data protection, and standards (ISO27001/ISO27002, FIPS) are more oriented on covering all security areas. Security documents dedicated to SME, define high-level security principles, however without explaining how these principles could be implemented (Table 1.1).

Table 1.1. Comparison of different security documents (Created by author)

Information Security document	Type	Industry	Covered Security areas	Level of details	Amount of separate requirements	Applicability to the SME	Applicability to the Large enterprises	Certification	Are requirements mandatory
ISO 27001 / ISO 27002	Standard	Global	14	Detailed	114	Applicable	Applicable	Yes	No
PCI DSS	Standard	Financial	6	Detailed	275	Applicable	Applicable	Yes	Yes (Globally)
FIPS	Standard	Government	17	Detailed	51	Applicable	Applicable	No	Yes (USA)
ISSA 5173	Standard	Global	3	High-level	11	Applicable	Not applicable	No	No
HIPAA	Act	Healthcare	11	High-level	41	Applicable to the specific organizations	Applicable to the specific organizations	No	Yes (USA)
FISMA	Act	Government	4	High-level	10	Applicable to the specific organizations	Applicable to the specific organizations	Only for specialists	Yes (USA)

End of Table 1.1

Information Security document	Type	Industry	Covered Security areas	Level of details	Amount of separate requirements	Applicability to the SME	Applicability to the Large enterprises	Certification	Are requirements mandatory
SOX	Act	Financial institution	9	High-level	2	Applicable to the specific organizations	Applicable to the specific organizations	No	Yes
GDPR	Law / regulation	Global	5	High-Level	99	Applicable	Applicable	No	Yes (Globally)
NIST SP 800-53	Best practices	Government	16	Detailed	444	Applicable	Applicable	No	No (USA)
NISTIR 7621	Best practices	Global	7	High-level	20	Applicable	Not applicable	No	No
COBIT	Framework	Global	5	High-level Detailed	37 210	Applicable	Applicable	Only for specialists	No

Organizations, which must be aligned with more than two different security documents, must deal with this inconsistency, if want to ensure the needed level of security. In SME case, it even harder, because a lot of SME do not have an information security department or information security expert, who would be able to solve such issues.

1.2. Methods of Security Requirements Harmonization

Usage of security documents is one way to enhance the security level in a company. Some documents must be met in the company to be certified and acquire additional possibilities (for example, if a company wants to work with payment cards it has to be compliant with PCI DSS standard) while the other documents can be used as advisory to improve the security level in the company. However, use of more than one document at the same time (which becomes very common at present) may result in duplication or even conflicts between the requirements of different documents (Gaşpar and Popescu 2018). Such a situation in the company can lead to inefficient use of the company's resources during the implementation of security requirements, while the applicable components of ISMS can be redundant as well. Therefore, it's imperative to ensure a clear understanding of requirement relations in the applicable documents to optimise the process of its implementation and maintenance.

For the purpose of optimising the use of multiple security documents at the same time, harmonization of these documents has to be sought (Armstrong, *et al.* 2015). Harmonization is an activity that seeks to define and configure the most suitable harmonization strategy for achieving the strategic goals of an organization where two or more models are involved (Siviy, *et al.* 2008). However, it is noticeable that different terminology is used to address the harmonization of different documents in related works: harmonization, synergy, compatibility, etc. (Pardo, *et al.* 2012). All these terms are related. Nevertheless, they have a specific meaning in this context. Four different techniques can be identified to associate controls of different documents, which imply the use of different terms (Souag, *et al.* 2012):

- Semantic compatibility means achieving document harmonization through the same terminology. These methods attempt to unify the terminology in different documents eliminating any misunderstanding and establishing the relations between separate controls by the same terms (Aviad, Wecel and Abramowicz 2015). It can be a difficult task to associate controls of documents by terminology because the analysis must take into account both terminology and context it is used in, while different document structure and other properties in documents require more advantaged technologies to do it in a right way;

- Mapping is one of the most popular techniques used to harmonize different documents. It attempts to compare different documents and make links between different concepts, controls, structures, etc. The result of mapping two documents usually are shown in a table of matches between these documents, which indicates which parts of these documents match and which parts are unique just in a certain document (Gaynor, Bass and Duepner 2015). However, to map more than two documents at the same time can be tricky and sometimes ineffective;
- Adaptive mapping integrates selected documents automatically by using mapping documents for the selected document. To reduce the complexity and necessity of many mapping documents, one basis ontology is used to map all the other documents. Such an approach would require just as many mapping documents as there are documents that have to be integrated;
- Integration technique is used to combine a few documents into one. While mapping document supplies just links between documents, the integration creates a new document, which combines all information from used documents making no difference, which parts match between documents and which are unique for one of the documents. A user gets one combined document, which matches the usage of few documents in conjunction. However, this solution requires additional work to create it comparing to the document mapping. It is because elements of different documents must be identified as in the document mapping, while a new document structure and control formulations must be reasonably created as well. Removal or addition of the new document is difficult using this technique and requires an overall revision of the document.

To achieve harmonization goals different operations could be used. Cesar Pardo highlights 4 main operations between models or documents in our case: union, intersection, difference and complement (C. Pardo, *et al.* 2012).

According to author intersection is the identification process of the common elements between two models. In other words, identification of the similarities which are presented in both models or documents. The union is the process of the merging two models or documents. Union allows us to ensure, that the union of sets consist of all the elements of two models or documents. Differences are the process of identification of the elements, which are presented only in the one model or document. The complement is the list of all differences between models or documents (Fig. 1.4).

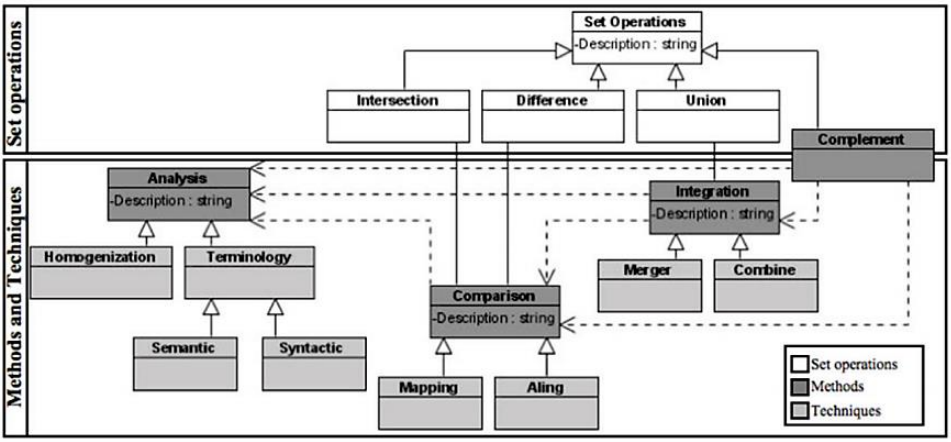


Fig. 1.4. Relationship between the set of operations, methods and technique harmonization (C. Pardo, *et al.* 2012)

As we can see, different techniques are using a different set of operations. Like example, mapping is oriented on intersections (similarities) and difference identification, and Integration is more oriented on union operation.

Table 1.2. Comparison of properties of different document harmonization techniques (Created by author)

Technique	Number of documents for harmonising n documents	Number of records for harmonizing n documents in one document	Usage examples
Semantic compati-bility	From 1 to n(n-1)/2	Same as the number of synonyms in these docu-ments	ISO standard family (ISO/IEC:27001 2013)
Mapping	From 1 to n(n-1)	Up to m_1+m_2, where m$_1$ is a number of controls in the first document and m_2 – in second	(Hofherr 2011), (Pardo, *et al.* 2012)
Adaptive mapping	N	Up to *m*, where *m* is a number of controls in the document	(Ramanauskaite, Olifer, *et al.* 2013)
Integration	1	Up to $\sum m_i$, where mi is a number of controls in the i-th document	(Ahuja, Goldman 2009), (IT Governance Institute 2008)

Table 1.3. Comparison of properties of different document harmonization techniques (Created by author)

Technique	Advantages	Disadvantages	Operations used by techniques
Semantic compatibility	✓ similar terminology and understanding of the concepts ✓ useful to harmonize set of documents, which are covered separate aspects of the same scope (like example ISO standards	✓ complicated way to add new external documents to the existing set ✓ take into account both terminology and context. However, and different security documents define security requirements with different level of details ✓ time-consuming process ✓ unify documents, and do not provide information about similarities and differences between security documents	Complement
Mapping	✓ provide information about similarities and differences between different security documents ✓ results presentation in the table form, which allows quickly analyze mapping results	✓ New document assigned to the mapping scope, require to map this document with all other documents in the scope ✓ effective for two documents harmonization, however time consuming in the cases when multiple security documents must be mapped. ✓ different security documents terminology require to validate concepts and context of each requirement	Intersection Differences Complement

End of Table 1.3

Technique	Advantages	Disadvantages	Operations used by techniques
Adaptive mapping	✓ allow add new security document to the scope, without need to map this document with all other documents in the scope ✓ allow to integrate to the scope security documents, which are covering different are of information security. Note: it is strongly depends from mapping basis quality ✓ provide information about similarities and differences between different security documents	✓ require to develop mapping basis, which will be used for security documents integration ✓ mapping quality directly depend from the level of details in the mapping basis ✓ different security documents terminology require to validate concepts and context of each requirement	Intersection Differences Complement
Integration	✓ as the results all security documents will be integrated to one document. ✓ document use the same terminology, concept and context-independent	✓ do not provide information about similarities and differences between security documents ✓ complicated way to add new external documents to the existing integrated documentation ✓ new document import is time-consuming process	Union

All mentioned harmonization techniques have different properties and usage area (see Table 1.2 and Table 1.3). However, the adaptive mapping solution combines all other harmonization techniques and allows using all the benefits it gives:

- harmonizing n documents exactly n mapping documents have to be created (less than in mapping technique);
- the integrated document can be regenerated automatically changing the list of harmonizing documents and the base of view (more flexible than integration technique);
- mapping document to ontology context of the class can be represented (this task for semantic analysis can be more difficult to achieve).

1.3. Existing Security Ontologies

Security becomes fundamental in our society, and the survival of organizations depends on the correct management of modern security elements (Dhillon and Backhouse 2000). As the security area is extensive and has many relations between its concepts, usage of security ontology could improve unambiguity of security knowledge description in information systems (Kim and Lee 2016), (Kim, *et al.* 2016). The necessity of security ontology can be noticed in various security communities and considered as a significant challenge and a research branch (Mouratidis and Giorgini, Integrating Security and Software Engineering: Advances and Future Visions 2006), (Donner 2003), (Tsoumas and Gritzalis 2006), (Wang, Wang and Wang 2016).

In small and medium enterprises, the knowledge database of the security area and its unambiguity is critical in formal or legal activities, such as certification, standard compliance, etc. In many cases, organizations have to meet specific security requirements from different sources, which may be redundant or overlapping by simultaneous usage . Therefore, security document mapping should be put into practice in cases where more than one security document has to be met. The mapping of security documents allows the optimisation of resources by indicating matching elements of documents and by eliminating duplicated activities and security measures to achieve it (Guan, Yang and Wang 2016). However, mapping of security documents can be complicated if more than two documents have to be mapped.

An ontology defines the basic terms and relations compromising the vocabulary of a topic area as well as the rules for combining terms and relations to identify extensions to the glossary (Gomez-Perez, Fernandez-Lopez and Corcho 2004). By decreasing language ambiguity and structuring transferred data, the ontology provides better communication, reusability and organization of knowledge (Gruber 1995), (Dobson and Sawyer 2006), (Fernandez-Breis and Martiinez-Bejar 2002), (Gruninger and Lee 2002).

Security ontology can be used to simplify the mapping of more than two security documents (Ramanauskaite, Goranin, *et al.* 2013). The ontology could act as a basis for document knowledge formalisation and would allow adaptive mapping of any documents, mapped to the ontology.

Existing security ontologies vary according to the described area and level of detail (Karande 2015). One of the first works mentioning information system knowledge concepts concerning security was published in 1990 by J. Mylopoulos *et al.* The paper "Telos: Representing Knowledge about Information Systems" (Mylopoulos, *et al.* 1990) describes a Telos language to describe the knowledge about information systems and suggests it can be employed for security specification as well. C. E. Landwehr *et al.* in 1994 published a paper called "A taxonomy of computer program security flaws " (Landwehr, *et al.* 1994) where types of computer program security flaws were summarised and claimed it could be used for an introduction to the characteristics of security flaws and their origins A. Avizienis *et al.* also proposed a taxonomy, concerning security concepts (Avizienis, *et al.* 2004). This taxonomy describes more abstract and full concepts than C. E. Landwehr *et al.* provided; however, clear relationships between categories of taxonomy are missing too.

The need for ontology rather than taxonomy was indicated in the paper "Toward a Security Ontology" by M. Donner (Donner 2003). In the same year G. Denker et. al. presented security-related ontologies for web services and published it in the paper "Security in the Semantic Web using OWL" (Denker, Kagalb and Finin 2005) while H. Mouratidis el al. published work "An Ontology for Modelling Security: The Tropos Approach" (Mouratidis, Giorgini and Manson 2003) presenting ontology for security modelling in agent-based information systems. H. Mouratidis provided more works concerning security ontologies (Giorgini, Manson and Mouratidis 2004), (Mouratidis and Giorgini 2006) where clear orientation to the use of security ontologies in software developments is noticed. Han presented Security vulnerability ontology used for organization issues data mining (Han and Yali 2015) . Venkata ontology is dedicated for security and resilience in the cyber-physical systems (Venkata, Kamongi and Kavi 2018). Wang and his colleagues proposed ontology for a defensive strategy for mobile security (Wang, *et al.* 2017). Veloudis proposed to use ontology-driven attribute-based access control for cloud environment and in such way ensure security-by-design principles (Veloudis, *et al.* 2019). Therefore these ontologies are meant more for system requirement representation rather than for basic security concepts.

There are ontologies concentrated specifically on security requirements only. One of such ontologies was presented by F. Massacci (Massacci, *et al.* 2011). Other specific security ontologies are proposed by D. Geneiatakis *et al.*

(Geneiatakis and Lambrinoudakis 2007) (designed for describing Session Initiation Protocol security flaws), by M. Karyda (Karyda, *et al.* 2006) (dedicated for describing applications of e-government), by J. Undercoffer *et al.* (Undercoffer, Joshi and Pinkston 2003) (designed for describing computer attacks), by A. Souag (Souag 2012) (designed for requirements engineering process) and by other authors. A. Kim extended specific ontologies and created one which can be applied to any electronic resource (Kim, Lou and Kang 2005). However, this ontology does not overlay all the concepts of information security. More detailed general security ontologies were proposed by A. Herzog *et al.* (Herzog, Shahmehri and Duma 2007) and S. Fenz *et al.* (Fenz and Ekelhart 2009).

Security ontology, proposed by Herzog *et al.*, represents the information security domain that includes both general concepts and specific vocabulary of the domain. The proposed ontology has four high-level concepts: assets, threats, vulnerabilities and countermeasures. The ontology overviews and analyses the information security domain in a context-independent and application neutral manner. Similar properties apply to security ontology proposed by S. Fenz *et al.* however, it covers more concepts, including non-core concepts such as the infrastructure of organizations. The main top-level concepts in this ontology are assets, control, organization, threat and vulnerability.

While S. Fenz security ontology includes concepts of several security documents (ISO 27001, Grundschutz (Federal Office for Information Security 2005)), one more version of S. Fenz's security ontology will be analysed in this study (hereinafter S. Fenz (raw)). All classes and elements of security documents will be excluded from S. Fenz's ontology, relying solely on raw concepts of ontology security.

The general comparison of security ontologies, the total number of different ontology elements, the depth and branching metric of the ontology tree are put into contrast. These metrics were gathered by an OWL ontology editor SWOOP (University of Maryland 2009). The data obtained using this tool are presented in Table 1.4.

The purpose of ontology usage inflicts on the number of individuals as well-wider scope ontologies have more individuals to allow the user to choose from; specific purpose ontologies have less or no individuals as all individuals should be known or unnecessary to the user. Another important metric is the depth and branching factor of the ontology class tree. It defines the main properties of the tree structure of the ontology and can be exercised to determine how intuitive the ontology should be for individual users. Analysis displays that the security ontology by A. Herzog has the most profound class structure and the most substantial detailing level. However, the maximum branching factor of the class tree is equal to 83, which may result in human users facing difficulties while viewing the ontology. Ontology by S. Fenz should be difficult to visualize as well because of its branching factor.

Table 1.4. Data of general comparison of security ontologies (Created by author)

Property	Ontology			
	G. Denker	A. Herzog	S. Fenz	S. Fenz (raw)
Total number of classes	39	460	641	311
Total number of data types properties	0	7	16	14
Total number of object properties	12	30	58	58
Total number of annotation properties	2	4	10	10
Total number of individuals	117	211	486	478
Number of sub-classes	11	571	1051	409
Max. depth of the class tree	4	8	6	6
Min. depth of the class tree	1	1	1	1
Avg. depth of the class tree	1.4	4.1	3.0	3.2
Max. branching factor of the class tree	27	83	199	114
Min. branching factor of the class tree	1	1	1	1
Avg. branching factor of the class tree	7.6	3.2	3.9	14.5

As it was mentioned, S. Fenz, G. Denker and A. Herzog ontologies have different goals and are oriented on different information security aspects. However, from an analysis point of view, it is important to understand how dissimilar they are. To do that, we will be using the Jaccard distance metric (Table 1.5).

Table 1.5. Ontologies similarity verification results (Created by author)

Ontologies	Jaccard index	Jaccard distance
S. Fenz (raw) and G. Denker	4.77	95.23
A. Herzog and G. Denker	8.16	91.83
S. Fenz (raw) and A. Herzog	33.26	66.74

Analysis showing that the lowest similarity levels are between G. Denker and other authors ontologies. Such results are predictable, because of specific of G. Denker ontology. This ontology has the lowest amount of ontology components (classes, individuals) and is oriented to the interface between various notations of security documents. S. Fenz and A. Herzog ontologies are oriented on overall security assurance. However A. Herzog ontology with a high level of details define network security and data encryption components.

A general comparison of security ontologies gives just some key quantitative metrics, while the quality of ontology is not taken into account. OntoMetric (Lozano-Tello and Gomez-Perez 2004) is a method for ontology quality measurement. This method compares ontologies into five dimensions:

- the ontologies content and the contents of the organization;
- the language in which it is implemented;
- the methodology that has been followed to develop it;
- the software tools used to build and edit the ontology;
- the costs that the ontology will require in an individual project and measures all the characteristics from 1 to 5 according to their low or high degree of accomplishment.

While all ontologies studied are written in the same file format, the content metrics were analyzed separately (metric of language, tools and costs should be equal, because all the ontologies studied are written in OWL files, while the development process of ontology does not have significant influence on its usage and is unknown to us). According to OntoMetric, the content of ontology can be defined by four factors: concepts; relations; taxonomy; axioms.

OntoMetric evaluation is qualitative by nature. All mentioned security ontologies were analysed for presenting the broadest security area possible. The imagination of ideal security ontology is vital to evaluate the concept factor in OntoMetric analysis as this measurement should provide information on how well the ontology covers the security area.

Other factors in OntoMetric analysis are more relative and describe how well the relations, taxonomy and axioms are defined in the ontology, not the whole security area.

The OntoMetrix analysis shows that G. Danker's ontology has the lowest scores, while S. Fenz's and A. Herzog's ontologies have similar scores. The analysis also reveals the level of detail and provides a wide range of security concepts. However, the data of OntoMetric analysis does not show differences between S. Fenz and A. Herzog.

All data of our OntoMetrix analysis are presented in Table 1.6.

Table 1.6. OntoMetric analysis data of the ontologies content and the contents of the organization (Created by author)

Characteristic	Ontology			
	G. Denker	A. Herzog	S. Fenz	S. Fenz (raw)
Concepts (factor)	2	4	4	4
Relations (factor)	3	3	3	3
Taxonomy (factor)	2	3	3	3
Axioms (factor)	2	4	4	4

While comparing the differences in S. Fenz's and A. Herzog's ontologies, it can be noticed that the ontology created by A. Herzog has more of a theoretical approach compared to the ontology of S. Fenz and describes more definitions, formal concepts of the information security area. S. Fenz's ontology provides more information on the practical side of information security, by listing basic controls as a guide for security administrators for system security assurance. However, it does not mention concepts related to organizational security.

1.4. Security Ontologies as Foundation for Mapping Techniques

To ensure security in an organization, security documents or best practices can be employed. In some cases, compliance with a particular security document is even required to obtain privileges to supply or to get different services (Guan, Yang and Wang 2016).

However, when an organization uses more than one security document, mapping or integration of security document usage should be done to avoid redundant activities, not optimal resource management, unnecessary outlays, etc. Integration or direct mapping of security documents are both time and knowledge consuming endeavour as well as a very static activity (everything has to be redone when a document has to be removed or added) (Souag, Salinesi and Isabelle 2015). Adaptive mapping of security documents provides more flexibility to change the list of used documents as well as requires less work to map a more significant number of documents as each document has to be allocated to ontology only (Fenz, Plieschnegger and Hobel 2019). Therefore, n mapping activities have to be done to map n documents instead of $n \times (n - 1)$ mappings for direct mapping. The process of adaptive mapping and integrated document generation is presented in Fig. 1.5.

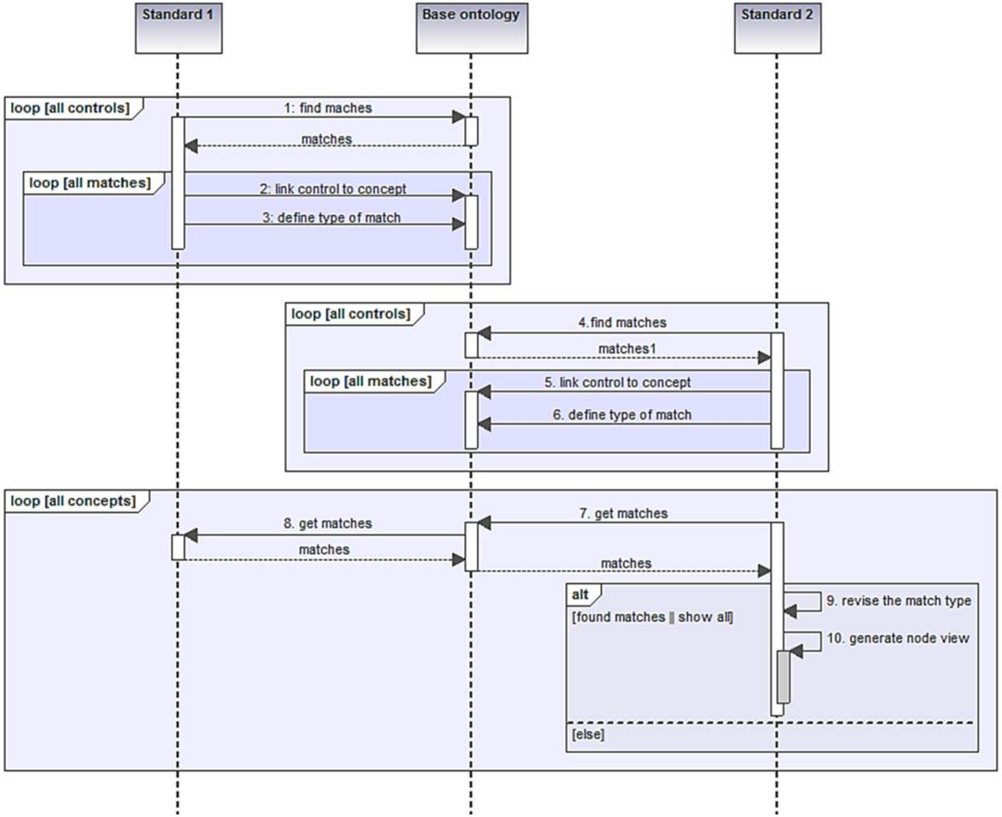


Fig. 1.5. The sequence of mapping two documents and generating the harmonized document with the structure of the ontology (Created by author)

In this example (Fig. 1.6), a control in ISO 27001 (A.8.3.3_Removal_of_access_righ...) and control in PCI DSS (PCI_DSS_8_5_4) standards are mapped with the same links to the security ontology (control in one document has the same relations to concepts of security document as a control in another document). As these two controls have no differences in mapping, the full match relation between these two controls of different documents can be generated. One more control of ISO 27001 standard (A.11.2.1_User_registration) is presented in this example to illustrate relevantly (not matching) controls. These two controls of ISO 27001 security standard define situations where the vulnerability of non-blocked unnecessary accounts or terminals can be exploited. However, both ISO 27001 controls have more links to different concepts of security ontology. Therefore, these two ISO 27001 controls cannot be treated as equal, but are still relevant on certain levels. This kind of information can be used to analyze security documents and to optimise resource usage when multiple security documents have to be met in an organization.

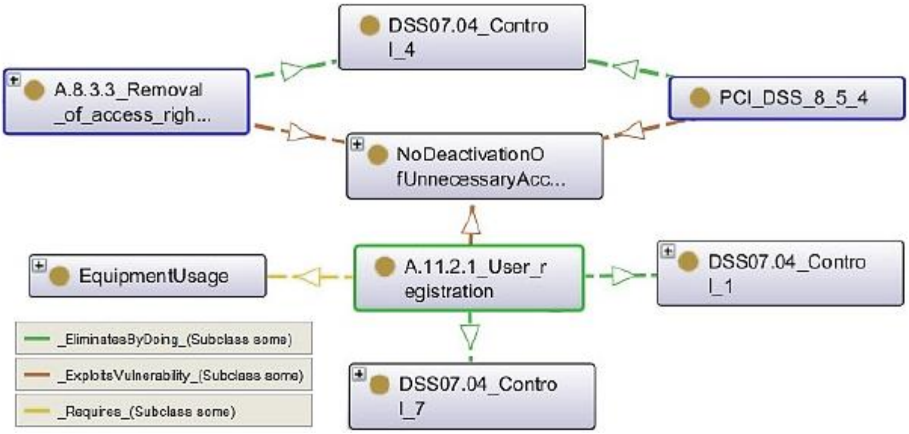

DSS07.04_Control_4
A.8.3.3_Removal_of_access_righ...
PCI_DSS_8_5_4
NoDeactivationOfUnnecessaryAcc...
EquipmentUsage
A.11.2.1_User_registration
DSS07.04_Control_1
EliminatesByDoing(Subclass some)
ExploitsVulnerability(Subclass some)
Requires(Subclass some)
DSS07.04_Control_7

Fig. 1.6. Example of document mapping trough ontology (Created by author)

The ontology and standards concept coverage were analysed to compare which security ontology is more suitable for adaptive security documents mapping and adaptive mapping. A. Herzog's and S. Fenz's ontologies (Fenz and Neubauer 2018) were mapped with:

- ISO27001 (ISO/IEC:27001 2013) – the most popular security standard, which was created according to the British Security standard BS7799. This standard practically covers all security areas, provides certification opportunity and is widely recognised;
- PCI DSS (PCI 2016) – security standard developed by such worldwide organizations as Visa, MasterCard, American Express, Discover and

JCB. This standard has been developed to ensure cardholder information protection and is a "Must-have" for all organizations who handle debit, credit, prepaid and other cards. Otherwise, these organizations are forbidden to use Visa, MasterCard, American Express and other cards;

- ISSA 5173 (Information Systems Security Association 2011) – security standard for SME (Small Medium Enterprise). Although this standard has not been approved or officially recognised, it describes the main security requirements which need to be implemented in any organization;
- NISTIR 7621 (NIST, NISTIR 7621 Rev. 1, Small Business Information Security 2016) – special publication, developed by the National Institute of Standards and Technology. The document clearly defines which actions are "necessary" for information, systems and networks protection. It also provides best practices on the needed security level implementation.

Data on links between these security standards are presented in a static form for two specific standards (as a table with matching controls between two security documents (Ramanauskaite, Goranin, *et al.* 2013)) mostly. S. Fenz was the first to have mapped ISO 27001 and Grundschutz (Federal Office for Information Security 2005) security standards to his ontology. He used this mapping for purposes of automated risk and utility management (Fenz 2010). However, this information can also be used for document adaptive mapping. S. Fenz mapped two standards only. Therefore links can only be generated between ISO 27001 and Grundschutz security.

All controls in all four chosen standards were analysed and mapped to related concepts in S. Fenz's and A. Herzog's security ontologies. The mapping of security standards was performed by mapping the lowest level concepts (usually it precise control, which is the requirement for the organization), while the classes in security standards, used for the presentation of the class hierarchy were not accounted for as mapping objects.

The process of security standard mapping to security ontologies revealed differences between the analysed ontologies as well. The biggest part of mapping links in S. Fenz's ontology is straightforward – one requirement of the standard has an equal or very similar control in S. Fenz's ontology. This type of mapping links is direct and easy to understand for individual users. However, the controls have to be detailed by other relationships between different concepts of the ontology. Otherwise, it will be challenging to define relations between standards controls, clustering, etc.

Meanwhile, mapping security standards according to A. Herzog's ontology was done from logical structure standpoint – one requirement of security standard is to have several links to ontology, by describing which concepts of ontology are related to this requirement (by defining what and how one has to do or use to protect against specific threat or vulnerability). This type of mapping requires more mapping links and has the potential to be easier to cluster controls of security standards into relevant groups. This type of mapping would be more understandable to information systems; however, it would require more analysis or visualizing tools for people to understand links between two security standards, mapped through ontology this way.

Summarizing the security document mapping process to security ontologies: S. Fenz's ontology can be used to simplify the mapping of security standards because all the most critical concepts for mapping are described as a list of classes, while in A. Herzog's ontology mapped classes have more links to ontology and provide more analysis and application possibilities after the mapping is accomplished.

Table 1.7. Amount and percentage of security ontology entities mapped with security requirements of the standards (Covered) and amount and percentage of security requirements of the standard mapped to the security ontology (Covers) (Created by author)

Standard	Ontology / Standard coverage			
	S. Fenz		A. Herzog	
	Covered	Covers	Covered	Covers
ISO27001	35/311 (11%)	23/133 (17%)	26/460 (6%)	19/133 (14%)
PCI DSS	42/311 (14%)	48/165 (29%)	25/460 (5%)	32/165 (19%)
ISSA 5173	31/311 (10%)	7/12 (58%)	29/460 (6%)	6/12 (50%)
NISTIR 7621	14/311 (5%)	8/10 (80%)	21/460 (5%)	8/10 (80%)

Analyzed ontologies and security documents mapped to them were verified to identify how they are covering each other requirements. To do that, two additional metrics "Covered" and "Covers" were calculated. "Covered" metrics showing the amount of ontology entities which could be linked with a specific standard. Like example, S. Fenz ontology has 311 entities. Only 35 of them could be linked with ISO 27001 standard and with PCI DSS standard could be linked 42 of S. Fenz ontology entities. "Covers" metrics showing the amount of security documents requirements which could be linked with specific ontology. Like example, ISO 27001 standard has 133 requirements, and only 23 of them could be linked with S. Fenz ontology entities. Form PCI DSS point of view only 48 requirements could be linked with S. Fenz entities. Amount of "Covered" and "Covers" are different, because of the level of details in ontology and security documents. It leads to the situation when a few requirements, could be linked to the same ontology entity and vice versus a few ontology entities are linked to the same security document requirement In Table 1.7, data on ontology coverage by standard (covered) and standard coverage by ontology (covers) are provided. The column "covered" defines what part of security ontology was used to map a certain standard while the column "covers" defines what percentage of security standard was mapped to the security ontology. The property "covers" is more important in this research as it provides information on how well the ontology is capable of presenting certain security standards in the knowledge database.

The analysis of security ontology and standard coverage revealed that ontologies of A. Herzog and S. Fenz are not capable to fully cover any of the analyzed security standards: only security standards with a small number of controls or requirements can be mapped with security ontology to include more than 50% of standard controls; security standards with more than 100 controls or requirements cannot be mapped to A. Herzog's and S. Fenz's security ontologies to cover more than 30% of standard controls or requirements. It shows the fact that these two security ontologies do not have all the necessary concepts to be fully mapped to security standards.

The analysis of concepts of security ontologies to be employed to map security standard has revealed that just a small part (5 – 18%) of classes from A. Herzog's and S. Fenz's ontologies are mapped directly to security standards. This number could be improved by providing a more detailed concept of relationship. However, it allows defining what part of ontology is directly related to concepts, mentioned in security standards.

Security ontology created by S. Fenz was able to cover a more substantial part of analysed security standards compared to A. Harz's ontology. The most significant difference (29% and 19%) was noticed in the PCI DSS standard. It could be an argument to choose S. Fenz's security ontology if a company is working with PCI DSS standards, while coverage differences for other analysed standards are minor. However, covering 29% of the PCI DSS standard is not enough to represent it. A new security ontology with more security concepts could help to improve the situation and would allow mapping of more prominent parts of security standards.

1.5. Visualization of Harmonized Security Documents for Further Analysis

Usage of mapped security documents can be simplified if the intuitive and informative graphical user interface is designed to analyse mapped documents. Visualizations are tools used to express both the structure of the data and cognitive mapping of the user observing and interacting with this data (Tversky and Simonson 1993). By default, one security document is usually presented as a graph or tree structure, and in some cases, cliques are derived from these graphs (networks or subnetworks). While mapping information between two or more documents is presented as a table, where controls of one document are shown in one column, and controls of other document are given in another column. The mapping information is obtained by identifying rows with controls in both documents. Any methods or tools for graphical presentation of mapped security documents were found. However, some visualization ideas for overlapping or similar networks in other areas than document mapping exists, which can be adopted for the visualization of document mapping (Wielebski and Medynska-Gulij 2018).

David C. Y. Fung *et al.* proposed to use 2.5D visualization of overlapping biological networks (Fung, *et al.* 2008) where three parallel two dimensional planes are placed in three dimensions to represent overlapping networks: one for each network (the top and the bottom planes) and one for the overlapping part (in the middle plane) see Fig. 1.7. This approach allows identifying overlapped nodes very visually but has some limitations – it would be difficult to visualize more than two networks or documents as links from one document to another can cross other documents and be confused with document nodes between these two.

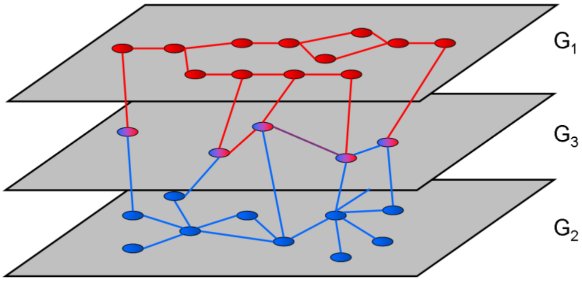


Fig. 1.7. The idea of 2.5D visualization of overlapping biological networks (Fung, *et al.* 2008)

Patrick M. Dudas *et al.* proposes a semi-supervised approach for visualizing and manipulating overlapping communities, where the 3D model is used (Dudas, de Jongh and Brusilovsky 2013). This model takes into account the potential number of edges between nodes. Therefore they reduced overlap and the number of connections by creating a single vertex for each clique as a marker for the entire clique. This idea was used for visualization of mapped security documents. Mapped nodes would be presented in the smaller group as one, combined node.

This solution helps to observe similar controls in different documents. However, document node hierarchy is not shown in this solution (see Fig. 1.8).

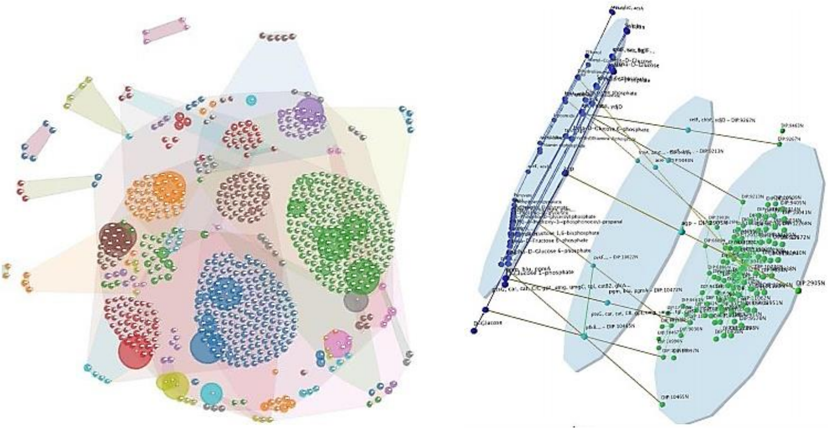


Fig. 1.8. Example of 3D visualization of overlapping communities by reducing the number of connections between document nodes
(Dudas, de Jongh and Brusilovsky 2013)

There are some examples, were overlapping in the network is presented by other structures rather than graph or tree. For visualization of gene networks, Steve Horvath and Peter Langfelder use a heatmap plot of the topological overlap matrix (Horvath and Langfelder 2009). In the heatmap, rows and columns correspond to nodes, light colours represent low topological overlap, and progressively darker orange and red colours represent higher topological overlap (see Fig. 1.9).

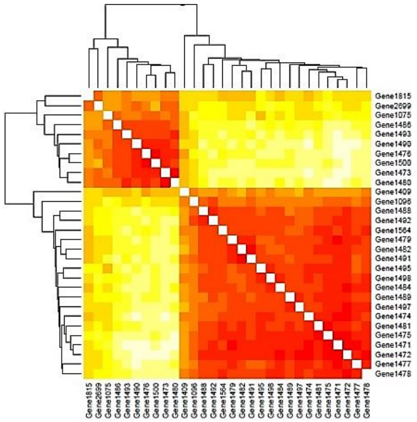


Fig. 1.9. Example of the heatmap plot usage for overlapping matrix
(Horvath and Langfelder 2011).

This visualization method can be used to present mapping information of security documents; however, the heatmap plot can only visualize overlapping of two documents.

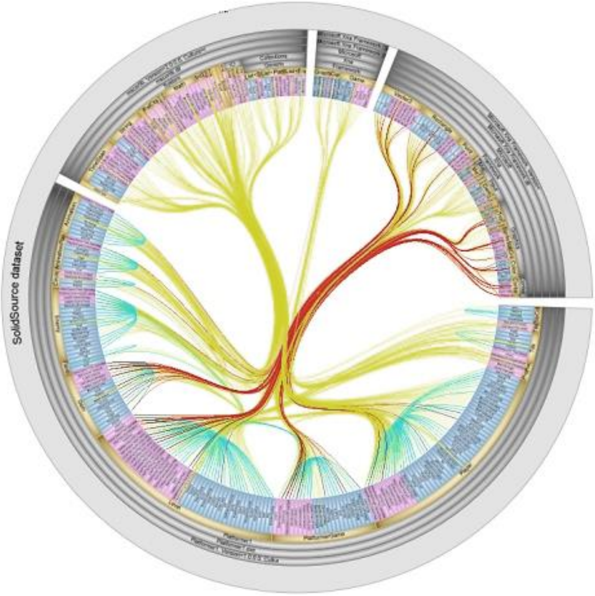


Fig. 1.10. Example of Chord diagram (Telea and Ersoy 2010).

Another idea which could be adapted for visualization of more than two documents is described in A. Telea and O. Ersoy paper “Image-Based Edge Bundles: Simplified Visualization of Large Graphs” (Telea and Ersoy 2010). These authors combine the advantages of edge bundles with a bundle-centric simplified visual representation of a graph’s structure. In Fig. 1.10. a simple list of nodes is presented; however, the required number of documents can be placed around the circle with all the nodes.

1.6. Evaluation of Information Security Documents Implementation Costs

From an Information security point of view, it is impossible to ensure absolute protection of an organization’s assets or information. Because of that, each organization must define the needed level of information and assets protection, which would satisfy their risk appetite, and implement security management controls, which would ensure such level of protection (Solic, Ocevcic and Golub 2015). Existing Security documents and requirements defined in such documents help to achieve such a goal and ensure that an organization is implementing due diligence principles (Schilling, *et al.* 2017).

It was already highlighted that the Information security requirements could be implemented in different ways, starting from the implementation of additional organizational controls (procedures, policies implementation) and finishing with complex technical solutions deployment. Li *et al.* (Li and Tang 2013) proposed four main contents of Information security Engineering, Security management; Communication Security; Access of Information Systems and Secure IS development). Wangwe *et al.* (Wangwe, Eloff and Venter 2012) proposed to concentrate on the other three areas (Governance, Operational; Technical) to ensure effective Information security management. Some authors were focused on specific Information security areas, starting from network security and finishing with cloud security. To protect data during client/server operation on the network, Kuo (Kuo 2007) proposed an intelligent agent-based collaborative information security framework. Tsalis *et al.* (Tsalis, Theoharidou and Gritzalis 2013) came up with a suggestion on how the return of Security investments for Cloud platforms could be calculated.

From a business perspective, it is essential to ensure that cost-benefit justification for Information security investments is in focus. Such an approach allows organizations to provide effective and efficient IT Security budget management. It is imperative to ensure that incident losses, together with countermeasures/controls deployment costs are lower than incident losses without countermeasures/controls in place (Ungureanu 2015). Deployed controls and countermeasures should reduce an organization's incident/risk probability to an acceptable level and appropriate cost.

However, Information security cost-benefits assessment is complicated, because of the lack of structured cost-benefit methods and problems with comparing IT security solutions in light of prevailing uncertainties. This problem became even greater for organizations which try to implement the requirements of more than one Information security document. Such a situation is typical for bank sector organizations when they are trying to fulfil Sarbanes-Oxley Act (SOX 2002) requirements, ISO27001 (ISO/IEC:27001 2013) and PCI DSS security standards (PCI 2016) and HIPAA requirements (Mohaghegh, *et al.* 2018).

An organization which is trying to implement more than two Security documents requirements is challenged to solve such issues as duplication of requirements in different Security documents and inefficient usage of organization's resources when similar security requirements are implemented in a separate way for each Security document. Because of that, Security cost-benefits evaluation, used by such organizations, must take into account these additional restrictions.

Use of cost-benefit evaluation and Information security cost evaluation methods would let an organization identify how effective countermeasure/controls deployment would be and how it would help the said organization to reduce potential losses in case of incident or breach. Unfortunately, the amount of cost-benefits evaluation and Information security evaluation methods is limited, and the majority of methods concentrate on processes, lifecycle steps and specific requirements of separate IT Security documents. Due to this reason, the existing methods do not cover all Information security areas and could not be easily re-used for new document re-evaluation.

The primary purpose of the cost-benefits evaluation is to ensure that the costs spent on Information security are lower than the benefits provided by them. In our case, it means that Information security requirements implementation costs are lower than the damage caused by lack of protection. Unfortunately, Information security does not generate direct profits for the business. In an attempt to assess the benefits, organizations calculate potential losses, that could be incurred if existing controls were not in place. Cost-benefits calculation is a complicated process. However, calculation results could be presented as a difference between the expected losses before countermeasures/controls deployment and after.

Currently, there exist different proposals on how Information security cost-benefits could be calculated. Lubich (Lubich 2006) and Mercuri (Mercuri 2003) propose to use the Return on Security Investments (hereinafter – ROSI) metric. Similar metric, Return on Investments (Eq. 1.1), is used in business to evaluate the benefits of the taken business solution.

$$ROI = \frac{B - C}{C}, \tag{1.1}$$

where B denotes the "Gain of investment" and C denotes the "Cost of Investment". Information security solution returns on investments are distributed over time and therefore, do not provide objective value. Another metric, Net Present Value (Eq. 1.2), which allows comparing benefits and costs over different time periods, was used to solve this issue.

$$NPV = \sum_{i=0}^{n} \frac{B_t - C_t}{\left(1+i\right)^t}, \tag{1.2}$$

where B_t denotes the present value of net benefits of period t, C_t denotes all costs, I indicate the discount rate and n means the time period.

As it was mentioned previously, Information security does not generate direct benefits, because of that, this formula for Information security was modified by adding additional criteria (Eq. 1.3):

$$NPV = -I_0 + \sum_{t=1}^{T} \frac{\Delta E\left(L_t\right) + \Delta OCC_t - C_t}{\left(1+i_{calc}\right)^t}, \tag{1.3}$$

where I_0 denotes the initial investment for security measure, $\Delta E(L_t)$ denotes the reduction in the expected loss in t, ΔOCC_t denotes the decrease of opportunity costs in t, C_t denotes the cost of security measure in t and i_{calc} denotes the discount rate. The presented model returns a positive or negative value. Investments are economically useful when NPV is positive and does not equal to 0.

From the Information security point of view, some of information security solutions still have to be implemented even if their Net present value is negative; it is mostly related to implementation controls which are mandatory for accreditations according to the Information security requirements. Another disadvantage of such calculation methods is the metric scope. Unfortunately, this metric is applied to a separate solution, requirement implementation or control implementation.

Arora *et al.* (Arora *et al.* 2004) have proposed another framework for cost-benefit evaluation. Their structure is more related to the organization's risk management evaluation and costs related to it. To evaluate the cost-benefits from the Information security implementation, they propose calculating the Risk-based Return on Investments (Eq. 1.4):

$$RROI(\sec urity\ solution) = \frac{R_B - R_R - I_C}{I_C}, \tag{1.4}$$

where R_B denotes the Baseline Risk, R_R denotes the residual risk, and I_C denotes the Implementation cost. Such calculation is closely related to the evaluation of security incidents and the possibility of their occurrence. The advantage of such methods is that it lets calculating metrics for the overall Information security area. The main disadvantage is that it concentrates on incidents and because of that could not take into account some controls which are mandatory from the regulatory point of view but are not closely related to the root cause of incidents (e.g., lack of documentation).

As it could be seen from Return on Security Investments, Net Present value and Risk-based Return on Investments methods, critical points in all calculation are Investment costs and Implementation costs, in other words, budgets related to countermeasures/controls deployment. Cost-benefit methods use this component, however, without offering an explanation of how they should be calculated. The major problem with Investment costs and Implementation costs calculation methods is related to the complexity of countermeasures/controls deployment.

Countermeasures/Controls deployment is a complex process, which involves the organization's different sub-processes and their implementation, controlled by different teams within an organization. Security countermeasures/controls deployment is even more complicated since identified risk could be reduced in different ways, starting from applying organizational procedures and finishing with deploying complex technical solutions (Ivkic, Mauthe and Tauber 2019).

Information security costs evaluation methods directly depend on significant cost factors, which are involved in Information security requirements implementation. de Brujin *et al.* (de Bruijn and Spruit 2010) separate information security costs to 2 categories: One-off costs and Recurring costs. Table 1.8 presents subgroups of One-off and Recurring costs.

Table 1.8. Information Security implementation costs (de Bruijn and Spruit 2010)

Description			
One-off costs		Recurring costs	
License	Licensing cost of tool or product. Only applied to vendor-based solutions.	Support	Support cost from the vendor. With some licensing schemes, a yearly fee has to be paid as well.
Policies	Policies and plans developed by to ensure organization information security requirements implementation and maintenance.	Administration	Costs for updating and configuring the solution. Reflecting changes in the business in the policies. User support (help desk)
Hardware	Hardware procurement, installation and configuration.	Monitoring	Monitoring the system
Implementation	The full process of implementing the security measure. Usually, this has an impact on the infrastructure and the organization. The application of the security measure is often phased and can require a long term.	Auditing	Audits and tests performed to ensure the correct implementation and workings of the system.
Embedding	The embedding of the implementation in the organization. Employees are needed to be hired or get training. Other employees might also need training or at least be notified about the changes.		

One-off costs generated in the planning, design and implementation stage and recurring costs created yearly during maintenance and support phases. Separate costs factor calculation could be different, and some of them could be calculated quantitatively, whereas others would require qualitative techniques.

However, all below provided Information security costs evaluation methods embed these costs factors during evaluation.

Brecht *et al.* (Brecht and Nowey 2013) proposed information security cost categorisation approaches from a different Information security perspective. The authors categorise information security costs for such methods:

- The Balance Sheet Oriented approach. This approach is understandable for management because it provides information security implementation costs in the way of IT-related budget planning. Gartner (Gartner 2011) proposed to use four categories: Personnel Costs; Hardware; Software and Outsourcing / Managed Security Services. Such an approach, even it is understandable to organization management, has some disadvantages. Classification of security costs into hardware and software is problematic because often they are part of the same solution. This approach more oriented to IT security rather than on information security;
- The Security measure life-cycle approach. Information security solutions evaluated according to the Information technology lifecycle. Such approach separates information security costs between Lifecycle phases: costs of purchase, costs of setup, costs of operation and costs of change. Advantages of such a view are that every single control could be easily evaluated according to expenses related to it. However, such an approach does not involve an organizational part of information security, such as policies, procedures and guidelines;
- IT-security process-oriented approach. Humpert-Vrielink *et al.* (Humpert-Vrielink and Vrielink 2012) proposed to view the information security costs from IT and Security points of view. The said authors categorise expenses into four groups such as costs for the tool; consulting costs; costs for operation and costs of risk. This method concentrates on a single information security requirement or control evaluation. However, it could be easily applied to cover requirements or controls in all needed information security areas. The Security measure life-cycle approach, described above, could be embedded into this method and will provide income for tool costs evaluation. The proposed model is not compatible with standard cost account models, used by business, and because of that information gathering could be complicated;
- The ISO/IEC 27001 oriented approach. The international standard ISO 27001 is widely used around the world. Brecht and Nowey (Brecht and Nowey 2013) proposed to look on information security implementation through ISO 27001 (ISO/IEC:27001 2013) controls point of view. The authors separated costs into 12 controls areas defined in the standard. If needed, each area could be divided into sub-costs. The authors proposed

two additional metrics: determinability, which describes how grim the determination of the related costs is in practice, and the information security cost ratio, which explains the real percentage of the values that may be accounted to information security. This standard is covering a full range of controls and is not only related to information security, but that is also why it is difficult to evaluate what part of implementation cost is related to information security and which is not (Sirisom, Payakpate and Wongthai 2017);

- The Information Security Management System – Layers approach. For accreditation, according to one of the existing Information security standards, the organization has to prove that it ensures effective Organization Security management. It could be done by implementing the organization an Information Security Management system. The approach is evaluating information security implementation through such categories as Management System; People and processes; Architecture and concepts; Operational Measures and Prerequisites (e.g. Inventory of assets or introduction of information ownership). The advantage of such an approach is that the area with high information security costs ratio is separated from an area with low prices. The disadvantage is that for each area, evaluation of implementation must be carried out separately.

This analysis is concentrated on information security implementation costs evaluation methods. It would be most useful for the organization which is required to implement two or more Information security documents and their requirements (Holik, *et al.* 2015).

As it was defined by Jacobson *et al.* (Jacobson, Griss and P. 1997) and Griss (Griss 2001) the main obstacles for effective component reuse are coming from the following areas: Business, Process, Organization, Engineering and Infrastructure. According to Zavadskas (Zavadskas and Vilutiene 2006), the analysis of the purpose is to be achieved by using attributes of effectiveness, which have different dimensions, different weight as well as different directions of optimisation In our case, for methods evaluation five criteria were chosen, covering 4 out of 5 Jacobson defined areas (Intelligibility for Senior management; Links with existing Information security documents and information security aspect coverage for Process area; Calculation complexity for Engineering; Reusability for Organization).

The above-mentioned information security costs methods were evaluated by seven Information security experts working in the Information security area. All the specialists represent the educational sector. The number of Information security specialists was chosen based on the analysis performed by Clemen *et al.* (Clemen and Winkler 1999) and Hora (Hora 2009). Both authors highlighted that differences among experts could be very important in determining the total uncertainty expressed about a question. Clemen and Winkler examine the impact of dependence among experts using a typical model and conclude that three to five experts are an adequate number. Hora created synthetic groups from the responses of real experts and found that three to six or seven experts would suffice the purpose, with little benefit from additional experts beyond that point. To verify experts knowledge was used Cooke's classical model.

1.7. Business Processes Models as a Data Source for Security Cost Implementation

Security implementation cost evaluation highly depends on the initial data. Considering the fact that often, data need to be gathered manually or require expert input, such an approach is complicated and time-consuming. If it could be automized by re-using information already known to the organization or extracting needed information from existing processes and procedure, it would help to simplify the organization security cost evaluation process. One of the ways to do that verifies the information presented in organizational Business processes models and diagrams.

There exist a set of different business process definitions. However, they commonly state that the business process is a collection/set of linked activities or tasks, that, once completed, will accomplish an organizational goal (Appian 2017). It is crucial to have clearly defined inputs and a single output for the business process model. In our case, the business process model would be a source to extract information about the main processes, stakeholders and related data of the organization. From the security point of view, it is very important to understand the infrastructure, which was used to manage these business processes.

Business processes could be presented in different ways. Johansson *et al.* (Johansson, Warja and Carlsson 2012) highlighted four graphical process-oriented modelling techniques: Business Process Model and Notation (BPMN), UML-activity diagrams, Event-Driven Process Chains (EPC) and flowchart/nodes maps. Aldin *et al.* present a comparative analysis of business process modelling techniques. Their study involves flowchart, Petri Net, Data Flow Diagram (DFD), Role Activity Diagram (RAD), BPMN, business use case, and business object interaction diagram. These seven techniques for business process modelling were evaluated against flexibility, ease of use, understandability, simulation, and scope. It is important to note that Aldin *et al.* (Aldin and de Cesare 2009) extract elements, which are common and generally accepted by the business modelling community. These elements are process, activity, service and product, role, goal, event and rule.

The Unified Modeling Language could be used to describe business processes. UML has many types of diagrams, which could be divided into two main categories: Behavior diagram (Activity diagram, Communication diagram, Interaction overview diagram, Sequence diagram, State diagram, Timing diagram and Use case diagram) and Structure diagram (Class diagram, Component diagram, Composite diagram, Deployment diagram, Object diagram, Package diagram and Profile diagram). For security requirements presentation in UML business processes researchers proposing to use UML-class and UML-activity diagrams (Rodriguez, *et al.* 2011), (Zapata-Barra, *et al.* 2018).

From the critical assets and environment identification point of view, it is essential to identify the vital data, which will be involved in the business processes, and infrastructure/environment which will be handling this process. From the provided list of business process modelling techniques commonly used notations, listed in Table 1.9, could be evaluated.

Table 1.9. Business process components, which can provide the information needed for security costs evaluation (Created by author)

Business process model techniques	Components, which could be used to present critical assets, stakeholders and infrastructure
BPMN	artefacts (data object, groups and annotations)
EPC	process owner, organization unit, information, material or resource object
Flowchart	an abstract or detailed description of units of work (rectangles), annotations
DFD	entity and data storage components
UML active diagram	activity, note, decision component

The market provides a number of different tools for business processes representation (e.g., Microsoft Visio, SmartDraw, ConceptDraw, Luchicart, and other). These tools have a predefined list of objects, which are later used to present the business process. The main disadvantages identified during the evaluation of these tools is a lack of libraries or classes for representation of infrastructure/environment components. This information can be presented in diagrams; however, it has to be entered manually by the diagram creator through annotation, notes or other objects.

1.8. Minimum Security Baseline and Usage of Graph Theory for its Analysis

As was explained previously, one of the main problems arise from the fact that organizations are required to be aligned with more than one security document or another regulating document. In many cases, organizations decide to implement only mandatory security document requirements that are named as a Minimum Security Baseline (MSB). MSB is a set of primary security objectives which must be met by any given service or system (CERN Computer Security 2018). In other words, the Baseline would be a subset of information security document and could be represented as its subpart. The conventional approach for Minimum Security Baseline identification is the use of expert knowledge (Bartens, *et al.* 2015). Information security specialists review the document or framework and identify which requirements are mandatory and are a part of MSB. Some researchers propose the use of Delphi method research for IT Governance MSB identification (de Haes and van Grembergen 2008). The main disadvantages of these methods are related to the fact that they are: based on expert knowledge; could be influenced by subjective opinion; are not affordable for SMEs; could not be easily adapted for dynamic changes in the information security area.

Another way for MSB identification is to present information security documents and their requirements as undirected graphs, where the graph is defined as a pair of sets (V, E), V is the set of vertices, E is the set of edges, formed by pairs of vertices. Security requirements would be graph nodes, and edges between graph nodes would show the links between these requirements. To achieve this, vertex cover and graph isomorphism algorithms could be used, where vertex cover algorithm is used for MSB generation, and graph isomorphism is used for organization implemented controls verification against MSB identified controls.

A vertex cover is one of the graphs related problems, where the primary objective is to extract a set of vertices of a specific graph, which covers all graph edges (Fig. 1.11). A vertex cover in an undirected graph G = (V, E) is the subset of vertices S ⊆ V such that every edge (u, v) in the graph G is connected to at least one vertex of S, in another word edge (u, v) is an edge of G, then either u in V or v in S or both. The size of a vertex cover is the number of vertices it contains (Eshtay, Sliet and Sharieh 2016). A minimum vertex cover is a vertex cover having the smallest possible number of vertices for a given graph. There also exist minimum weighted vertex cover algorithms with a weight function R associated with each vertex (Cai, *et al.* 2013).

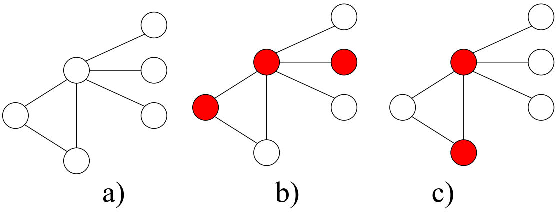


Fig. 1.11. Vertex cover: a) Graph G, b) Vertex cover of G, c) Minimum vertex cover of G (Created by author)

Vertex cover problems are widely used in the information technology area (Patel and Patel 2017), for example in solving network base routing delays (Ding, *et al.* 2009) or network traffic measurements (Zeng, *et al.* 2009). Some researchers proposed to use vertex cover algorithm for prediction of potential malicious attacks (Pushpam and Suseendran 2018), (Pushpam and Suseendran 2017). This algorithm is also used in biology for analysis of population-based evolutionary (Oliveto, Yao and He 2008) and many other areas. A vertex cover is an NP-complete problem. This statement was proved by R. Karp in 1972 (Karp 1972). Chvatal (Chvatal 1979) has proposed the use of approximation algorithm "Maximum degree Greedy", Clarkson has modified this approach and offered to perform a selection based on the degree (Clarkson 1983), Balaji, (Balaji, Swaminathan and Kannan 2010) have recommended an approach based on new criteria, which was named support of vertex. There exist other vertex cover algorithms, such as Nearly Optimal Vertex Cover NOVAC-1 (Gajurel and Bielefeld 2012), Advanced vertex Support Algorithm AVSA (Khan, Ahmad and Khan 2014) and Modified Vertex Support Algorithm MVSA (Khan and Khan 2013), heuristic algorithms ListLeft and ListRight (Delbot and Laforest 2008). Some researches (Khan and Khan 2014) performed a comparison of existing Minimum vertex cover algorithms.

For MSB graph verification against organization implemented requirements, Subgraph isomorphism algorithm could be used (Mishra, *et al.* 2017). Graphs G and G′ are said to be isomorphic if there exists a pair of functions $f : V \to V'$ and $g : E \to E'$ such that f associates each element in V with exactly one element in V′ and vice versa; g associates each element in E with exactly one element in E′ and vice versa, and for each $v \in V$, and each $e \in E$, if v is an endpoint of the edge e, then) f (v) is an endpoint of the edge g(e). Subgraph isomorphism from H to G is a function $f : V_H \to V$ such that if $(u, v) \in E_H$, then $(f(u), f(v)) \in E$. f is an induced subgraph isomorphism if in addition $(u, v) \notin E_H$, then $(f(u), f(v)) \notin E$. In other words, Graph isomorphism helps in verifying exact structural matching between 2 different graphs, even if they are represented in different ways. Graph Matching is the process of comparing two graphs to find an appropriate correspondence between their vertexes and edges. It refers to finding mapping solution S from the nodes of one graph G to the nodes of other graph G' that satisfies predefined criteria and ensure that the structure of one graph is similar to substructures of another graph. Subgraph isomorphism helps to verify structural matching between the graph and part of another graph (Fig. 1.12).

This property is widely used to analyze information and search similar patterns in different structures which are presented as graph, e.g. Image processing (Sanfeliua, *et al.* 2002), (Conte *et al.* 2003), where graph isomorphism is used to match two different images, social networks (Wenfei 2012), (Raymond and Willett 2002), where it is used for pattern analysis. However, the main area of isomorphism applicability is Biology and Chemistry, where subgraph isomorphism is used for Chemical bond structure (Balaban 1985) and Protein structure analysis (Elmsallati, Clark and Kalita 2007). It is necessary to mention that this problem could be solved in polynomial time. However, it was not proved that this problem is NP-complete and different researchers propose two main ways on subgraph isomorphism problem solving: try to identify exact subgraph matching identification or the use of approximate subgraph matching.

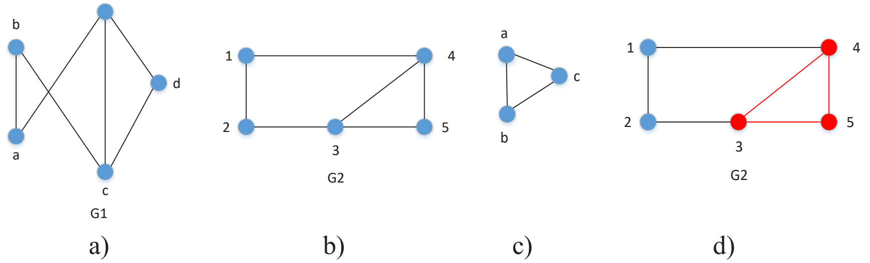


Fig. 1.12. Graph Isomorphism and Subgraph Isomorphism (Created by author): a) Graph G1, b) Graph G2 – isomorph of graph G1, c) Subgraph for graphs matching process, d) Two graphs (G2 and subgraph) matching results

Generic subgraph isomorphism identification algorithm is presented in (Lee, *et al.* 2012). Other examples of exact matching algorithms are GraphGrep (Shasha, Wang and Giugno 2002), FG-Index (Cheng, *et al.* 2007). These algorithms use indexes, which allow to reduce the number of candidates for the potential solution and later verification of chosen candidates. Other algorithms like Ullmann (Ullmann 1976), VF2 (Cordella, *et al.* 2004), QuickSI (Shang, *et al.* 2008), SPath (Zhao and Han 2010), K^+ (Rong, *et al.* 2018) find all embedding for the given query and original graph. Approximate algorithms, such as SIGMA (Mongiovi, *et al.* 2010), and Ness (Khan, *et al.* 2011) are defined approximate embedding and verify isomorphism through similarity measures.

1.9. Conclusions of Chapter 1 and Formulation of Tasks

1. External regulators and existing laws and regulations are forcing organizations to seek compliance. Minimum security baseline would help the organization to identify a list of mandatory controls required to ensure “due diligence” principles and guarantee cost-effective security implementation.

2. There are no effective ways to measure the influence of deploying a separate security document or control on the company's security expenditures. The existing methods for calculating security implementation costs are not oriented to security controls implementation of multiple security documents. Neither do they take into account the complexity and maturity levels of a company.
3. All existing harmonization approaches, except adaptive mapping, do not allow to re-use results of the previous harmonization. The performed attempts to harmonize multiple security documents by applying adaptive mapping through security ontology reveal that existing security ontologies are not oriented to security documents and their requirements. The verified ontologies (by A. Herzog and S. Fenz) covered less than 50% of 4 security documents harmonized with them and their graphical visualization, and quick knowledge search is complicated.
4. Minimum Security Baseline is a set of compulsory requirements for all systems and presents a subset of information security documents requirements. Formation of such a set of sets in cases of multiple security documents is complicated. Graph theory optimization algorithms, such as vertex cover algorithm and subgraph isomorphism property, allow to remove duplicated requirements and identify similar structures in different graphs.

Based on the conclusions, the following tasks are formulated:

1. Propose a method for improvement of evaluating security requirements implementation costs;
2. Propose method for harmonization of multiple information security documents and their requirements.
3. Propose method for minimums security requirement identification, analysis and verification.

2

Controls-Based Approach for Information Security Documents Requirements Implementation Cost Evaluation

As it was stated, there are no effective ways to measure the influence of deploying a separate security document or control on the company's security expenditures. The existing security implementation cost calculation methods are not oriented to security controls implementation of multiple security documents and present a complicated process for new security processes integration into the current calculation (W. Zeng 2019).

From an organization's point of view, an organization needs to ensure that security implementation is cost-effective, and the chosen controls satisfy regulatory requirements, provide the required level of protection and are not overpaid. According to the best security practices, control costs should not be higher than the cost of a potential security incident.

In an attempt to solve this problem, a new control-based security implementation costs evaluation method was proposed. Chapter 2 provides a theoretical and practical explanation of the proposed method. It also highlights identified advantages and disadvantages of this method and compares it with the existing security costs evaluation methods. Furthermore, it proposes and validates an automated initial data gathering process, which allows improving the method proposed and reduce the amount of time required for calculation.

The proposed methods were published in (Olifer, Goranin and Kaceniauskas, *et al.* 2017) and control-based security cost evaluation method improvements were published in the (Olifer, Goranin and Janulevicius, *et al.* 2017).

2.1. Controls-Based Approach for Evaluation of Information Security Documents

As it was defined in the chapter "Tasks of the Thesis", one of our goals is to identify information security implementation cost/benefits evaluation method, which would let us calculate information security implementation costs/benefits for organizations which use two or more different Security documents. The proposed method and calculation results must be:

- Understandable for Senior management;
- The method must be easily reusable for new Security documents implementation costs calculations;
- The method must cover all Security areas and control types (Administrative, Technical, Physical);
- Industry-independent;
- Applicable for the organizations of different sizes, starting from SME and finishing Enterprises.

Given the disadvantages of the existing methods identified in the first part of this thesis and taking into consideration the fact that the existing Security implementation costs evaluation methods are not oriented to security controls, defined by security documents, the new cost evaluation method was proposed. As a foundation for information security document evaluation costs, the IT Security process-oriented approach was taken. However, this approach was amended by adding components related to Risk evaluation, which is mandatory in the Security Assurance process. Regarding the fact, that proposed method is oriented on costs calculation, it is a quantitative way of security verification. However, some components or components used during evaluation could consist of qualitative techniques. Like example, complexity and maturity levels could be defined by applying qualitative techniques. Moreover, mitigation cost calculation requires define action cost boundaries, which are presented in the formula as "High" and "Acceptable" level.

The information security document costs evaluation involves two main processes:

- Risk assessment process;
- Security Control implementation process.

The risk assessment process is a mandatory process in any information security activities, starting from information security management and finishing with Information Security Audits. This process allows evaluation of the current situation and identification of missing gaps and probability of their exposure. Agrawal (Agrawal 2017) performed a comparative study on Information Security Risk Analysis methods and evaluated four different risk analysis methods (CIRA (Rajbhandari and Snekkenes 2013), CORAS (Stolen, *et al.* 2002), ISRAM (Karabacak and Sogukpinar 2005) and IS method (Suh and Han 2003)).

As it was stated above, the proposed information security costs evaluation method should be applicable for organizations of different size. Because of that, it was suggested to include into information security costs evaluation formula an additional coefficient φ. This coefficient allows to evaluate the organization's complexity, maturity and correlating information security costs. The proposed information security costs evaluation equation (Eq. 2.1) is the following:

$$C_{Security} = \varphi(C_{Risk\_assess} + \textstyle\sum_{i=1}^{n} C_{Sec\_Control\_implementation_i}(stnd)), \qquad (2.1)$$

where φ is the complexity and maturity coefficient; C_{Risk_assess} – Risk assessment costs, which explanation will be defined and described below (Eq. 2.3); $C_{Sec\_control\_implementation_i}(stnd)$ – security control implementation (Eq. 2.11).

Complexity and maturity coefficient depends on two factors: Complexity level and Maturity level

$$\varphi = \frac{Complexity\_level}{Maturity\_level}. \qquad (2.2)$$

Complexity level defines Overall Organization systems complexity and varies in the range from 1 to 5, where: 1 is Simple systems; 2 is Somewhat Complex systems; 3 is Complex systems; 4 is Very Complex systems; 5 is Highly Complex systems. The complexity level is evaluated and defined by the organization and is directly related to the number of existing systems, systems interconnections, amount of processes maintained by these systems, amount of authorised users, amount of different roles and privileges, etc. The complexity level is evaluated in a Qualitative way by experts.

Maturity level defines the Overall organizations' maturity. For maturity level evaluation Capability Maturity Model (CMM 1995) is used. Maturity levels are distributed in the range from 1 to 5, where: Level 1 is Initial (Chaotic); Level 2 is Repeatable; Level 3 means Defined; Level 4 – Managed; Level 5 – Optimizing.

Interdependency of complexity level and maturity level dependency ensures that costs of Information Security Assurance in organizations with low maturity level and high systems complexity level will be higher than in organizations with high maturity level, i.e., maturity is decreasing the information security implementation and Assurance costs, while the use of complex systems will increase them.

Risk assessment is a well-known process, where all components could be evaluated from the costs point of view. According to the common practice, defined in different documents (NIST SP 800-30 2012), the Risk assessment process must involve such steps as:

- Critical asset analysis. Such analysis involves assets identification, evaluation of their importance and impact to organizational functionality
- Vulnerability analysis (Identify vulnerabilities within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation)
- Threat analysis (Identify threat sources that are relevant to organizations; Identify threat events that could be produced by those sources; Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful)
- Impact evaluation (Determine the adverse impacts to organizational operations and assets, individuals, other organizations, and the overall resulting from the exploitation of vulnerabilities by threat sources (through specific threat events))
- Penetration testing (Attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities).
- Gap analysis (Existing situation comparing with Information security documents requirements and identifying controls or implementations which are not aligned with mandatory security document requirements)

2.1.1. Risk Assessment Costs Evaluation Formula

Risk assessment costs are calculated according to the following equation:

$$C_{Risk\_assess} = C_{Asset\_analysis} + C_{Vulnerabilities\_analysis} + C_{Threat\_analysis} + C_{Impact} + C_{Penetration\_testing}(N) + C_{Gap\_analysis}, \quad (2.3)$$

where $C_{Asset\_analysis}$ – costs related to Critical asset analysis, $C_{Vulnerabilities\_analysis}$ – costs related to Vulnerabilities analysis, $C_{Threat\_analysis}$ – costs related to Threat analysis, $C_{Gap\_analysis}$ – costs related to gap analysis and $C_{Penetration\_testing}(N)$ – costs related to Penetration testing needed for Risk assessment, where N is the amount of different organization systems, which have to be tested, C_{Impact} – the costs related to the Impact evaluation.

In the critical asset analysis process, two parties are involved: a consultant performing a Risk assessment and Organization's employees). These two parties are working together to gather the needed information. It means that the overall costs of critical asset analysis will be the total costs of Consultant and organization employees who are involved in this process.

These costs depend on the time needed for consultant and employee conversations, discussions and information sharing. Additional time spent on the analysis process will increase the overall Critical asset analysis costs.

According to the provided statement, the Critical asset cost calculation is performed according to the Eq. 2.4:

$$C_{Asset\_analysis} = C_{consultant}(t) + \sum_{i=1}^{n} C_{Personal_i}(t), \tag{2.4}$$

where $C_{consultant}(t)$ is Security consultant costs, $C_{Personal_i}(t)$ – Organization's employee costs and t is time spent to perform the analysis.

Although more than one consultant can participate in risk assessment, for model simplification consultant costs were combined into one by increasing the price-per-hour.

Information security consultant (Eq. 2.5) and organization employee (Eq. 2.6) costs can be calculated by multiplying time t by hour costs, defined by their contracts.

$$C_{Consultant}(t) = Hour\_price * t; \tag{2.5}$$

$$C_{Personal}(t) = Hour\_price * \ t, \tag{2.6}$$

where *Hour_price consultant* is consultant price per hour and *Hour_price personal* average employee time price.

Vulnerability analysis process implementation is similar to the Critical Asset analysis process. It means that information security consultant performs vulnerability assessment and has to identify and review the list of vulnerabilities which are the most common for such type of organization, environment, etc. An information security consultant has to evaluate which vulnerabilities are relevant in this particular case.

Because of that, it could be stated that Vulnerability analysis process also involves two main parts: the 1st is conversation and discussion with organization employees to gather information related to such analysis; the 2nd part is gathering information for evaluation.

According to this vulnerability analysis costs could be calculated according to Equation 2.7:

$$C_{Vulnerabilities\_analysis} = \alpha C_{consultant}(t) + \Big(\beta C_{consultant}(t) + \sum_{i=1}^{n} C_{Personal_i}(t)\Big), \tag{2.7}$$

where $C_{consultant}(t)$ is Security consultant costs and $C_{Personal_i}(t)$ is Organization employee costs. α and β are coefficients which define percentage of the time spthe ent the for discussion with organization employees and information evaluation. Consultant and employee costs calculation is defined in Eq. 2.5 and Eq. 2.6.

During the Risk assessment, the existing threats have to be evaluated. Information security consultant fully implements this part of the risk assessment process and because of that cost calculation for this process directly depends on the time needed for an information security consultant to evaluate the existing threats and is calculated according to equation 3.12:

$$C_{Threat\_analysis} = C_{Consultant}(t), \tag{2.8}$$

where $C_{consultant}(t)$ is Security consultant costs, calculated by equation (2.5).

One of the fundamental principles in information security is to ensure that information security costs are not higher than the potential impact on the organization. Because of that, an essential step in Information Risk evaluation process is related to Impact analysis. This process involves two main participants: information security consultant, who is responsible for explaining to organizations employees what can happen with critical organization assets if identified threats exploit a vulnerability and organization's employees who are responsible for evaluating the potential impact and defining it financially.

Impact analysis is to be calculated according to equation 2.9.:

$$C_{Impact} = C_{consultant}(t) + \sum_{i=1}^{n} C_{Personal_i}(t), \tag{2.9}$$

where $C_{consultant}(t)$ is Security consultant costs and $C_{Personal_i}(t)$ is Organization employee costs. Consultant and employee costs calculation are defined in equation Eq. 2.5 and Eq. 2.6.

Impact costs require inputs from the organization's management. Due to this factor, the cost of such evaluation is higher than other calculation steps.

In some cases, information security consultant and organization employee are not able to identify all existing vulnerabilities that can be exploited. In such a case, the organization is recommended to perform penetration testing. Before performing penetration testing, an information security consultant has to define penetration testing scope and identify technical teams which will be involved in it. Penetration testing is performed by a specialist who has the appropriate knowledge level and experience in ethical hacking. The cost of such experts is usually defined in contracts.

Because of that, penetration testing costs could be calculated according to the equation:

$$C_{Penetraion\_testing}(N) = C_{consultant}(t) + \sum_{i=1}^{n} C_{Personal_i}(t) + Fix\ cost, defined\ by\ contract, \quad (2.10)$$

where $C_{consultant}(t)$ are Security consultant costs and $C_{Personal_i}(t)$ are Organization employee costs. Consultant and employee costs calculation is defined in equation Eq. 2.5 and Eq. 2.6, *N* is the amount of different organization systems, that have to be tested

After collecting the required information, the information security consultant has to analyse it and verify from the Information security document point of view. Any requirements which are mandatory according to the Information security document and not implemented in the organization have to be identified and listed. This process involves results from all previous steps. However, it is performed only by the information security consultant. Consequently, t costs calculations for such a process could be done in the same way as Threats analysis costs calculations (Eq. 2.8).

2.1.2. Security Control Implementation Costs

The next step in Information security documents requirements implementation is the identification of Security Controls, which have to be implemented by the organization. To identify the list of necessary controls, an information security consultant has to identify critical assets, evaluate the related risk and choose the appropriate mitigation strategy.

The overall Security controls implementation costs will be the aggregated sum of separate control implementation costs. To highlight the Security controls that are related to critical assets, a new Control criticality coefficient mi($Risk_i$) was proposed, which depends on the Risk identified for Critical asset and varies from 0 to 1, i.e., if the risk that the critical asset will be exploited is higher, then the cost the of such control will increase.

Security control implementation is directly linked with the chosen Mitigation strategy and action needed to implement it. According to such a statement, Security control implementation costs couldd be calculated in the following way, as shown in (Eq. 2.11):

$$C_{Sec\_control\_implementation} = \sum_{i=1}^{n}(m_i\,(Risk_i) * (C_{Mitigation\_strategy_i} + C_{Action_i})), \quad (2.11)$$

where $m_i(Risk_i)$ is Control criticality coefficient and *Risk*ᵢ is calculated according to (Eq.2.12):

$$Risk_i = Vulnerability_i * Threat_i * Impact_i, \tag{2.12}$$

where $Vulnerability_{\mathrm{i}}$ is the vulnerability identified for asset i, $Threat_{\mathrm{i}}$ is the threat identified for asset i, $Impact_{\mathrm{i}}$ is impact recognized for asset i.

Mitigation strategy depends on management risk appetite and information about historical issues, something that has happened to specific critical assets in the past. Historical data could be gathered by the organization individually, or it could be statistical data characteristic of a particular area (financial, infrastructure or government organization).

Usually, four main mitigation strategies are defined:

- Risk accepted – when the organization management understands the existing risk but because of the low probability of negative events or because of the high price of mitigation controls decides not to take any actions to reduce it;
- Risk avoided – when the organization management understands the existing risk and decides to remove the risk source;
- Risk remediated – when the organization management understands the existing risk and takes action to reduce it to an acceptable level;
- Risk transferred – when the organization management understands the existing risk and passes it to the 3rd party, which is responsible for risk management or compensation in a worst-case scenario.

According to that, the Mitigation strategy (Eq. 2.13) could be defined as:

$$C_{Mitigation\_strategy} = \begin{cases} -C_{Act}, \ where \ \frac{\Delta T(t_{in})}{T(l_j)} * \overline{W} \le RA \ and \ C_{Act} \ is \ HIGH \\ 0, \ where \ \frac{\Delta T(t_{in})}{T(l_j)} * \overline{W} \le RA \ and \ C_{Act} \ is \ ACCEPTABLE \\ C_{Metrics}, \ where \ \frac{\Delta T(t_{in})}{T(l_j)} * \overline{W} > RA \ and \ C_{Act} \ is \ ACCEPTABLE \\ C_{insur} + C_{Metrics} - C_{Act}, \ where \ \frac{\Delta T(tt_{in})}{T(l_j)} * \overline{W} > RA \ and \ C_{Act} \ is \ HIGH \end{cases}, \tag{2.13}$$

where RA is an organization willing to handle the existing risk, $\Delta T(t)$ – Amount of security incidents during defined time tin, $T(l_j)$ – Amount of impacted systems, lj – asset impacted by a security incident, j – asset number, $\overline{W}$ – Impact average, $C_{Metrics}$ – Cost of metrics control operations, which could involve $C_{personal}$ and C_{Act} for additional specific tools, C_{insur} – Cost of insurance, according to the signed off contract with the 3rd party (insurance company). Risk appetite and acceptability of actions costs depends from the organization. And the same cost could be high for one organization and acceptable for another organization. Because of that, before starting calculating of Mitigation strategy costs, organization must define boundaries for action cost, which would be acceptable for organization and which would be above organization expectations.

After confirmation of the risk mitigation strategy, the chosen control has to be implemented. This process is directly linked to the Security measure life cycle approach. In the proposed calculation (Eq. 2.14), two main tasks were identified: Action implementation costs and Control operation costs. Implementation costs are related to the time, needed to implement the chosen actions. For calculation simplicity, time could not be longer than one year. Otherwise, it would be problematic to calculate Return on investment values.

$$C_{Action} = C_{Implementation}(t) + C_{Operation}, \qquad (2.14)$$

where $C_{Implementation}(t)$ is action implementation costs and $C_{Operation}$is Control operation costs.

This part of our equation (Eq. 2.15.) depends on additional sub-steps related to hardware and software procurements and their deployment costs. Environment purchase could be evaluated as one time cost frozen in time, and deployment costs are connected to the deployment project. Environment definition includes hardware, software and any other technical components required for system or solution business as usual activities. According to this, Action implementation costs could be calculated in the following way:

$$C_{Implementation}(t) = C_{Environment\_purchase} + C_{deployment}(t), \qquad (2.15)$$

where $C_{Environment\_purchase}$ – are hardware and software procurement costs and $C_{deployment}(t)$ – are project deployment costs.

It needs to be mentioned that the same hardware and software could be used to ensure more than one information security control. In that case, Control implementation costs must be calculated only once. Any other controls should not be involved in the calculation, except the situation, when the existing control was amended, and such amendment costs were not calculated previously.

Deployment project costs could be divided into three main groups:

- Personnel who are performing such deployment actions. Technically it could be a team or even a whole department who will be deploying it;
- Costs for configuration, which could be implemented by the 3rd party as a one-time contract cost;
- Costs related to personnel training and awareness, before letting them use a new system. Training/ Learning or Awareness sessions could be implemented internally or performed by external systems.

Such an approach allows us to calculate the Deployment costs as following in (Eq. 2.16):

$$C_{deployment}(t) = \sum_{i=1}^{n} C_{Personal_i} + C_{config} + C_{Training/Awareness}, \tag{2.16}$$

where $C_{Personal_i}$ is the Organization's employee costs, which are defined by equation (Eq. 2.6), C_{config} – Configuration costs, $C_{Training/Awareness}$ – Training/Awareness costs.

Operation costs are continuous costs that apply to control during the whole life cycle. These costs also include Environment support costs. Very often, organizations are signing the Support agreements with hardware and software vendors trying to ensure the security and functionality of hardware and software in use. However, the use of hardware and software also requires an organization to safeguard its internal maintenance. For that purpose, often, internal resources are used. And the last part is related to the amendments implemented on existing solutions (hardware or software), defined as Other services. Such modifications could involve the implementation of new functionality, changes in process workflow and others.

Operation costs could be calculated according to the equation (Eq. 2.17):

$$C_{Operation} = C_{Environment\_support} + \sum_{i=1}^{n} C_{Personal_i} + C_{Other\_services}, \tag{2.17}$$

where $C_{Environment\_support}$ is Environment support costs, $C_{Personal_i}$ – Organization employee costs, which are defined by Eq. 2.6, $C_{Other\_services}$ – cost of additional services needed for effective control functioning.

Provided calculations are industry and organization size independent, and are oriented on information security implementation aspects, rather than on specific of different applicability scopes.

2.1.3. Proposed Method Verification Experiment

A modelling experiment was performed to verify the applicability and effectiveness of the proposed information security costs evaluation method. Due to the advantage of the proposed control-based approach, calculations were simulated for one specific IT Security requirement. During the experiment, information security costs were evaluated for two abstract companies ACME and EMCA, that are generally used for such modelling tasks. Both companies being modelled were implementing Logging and Monitoring control, required by ISO 27001 and PCI DSS standards. The starting modelling conditions are presented in Table 2.1.

Information security costs for Logging and monitoring control implementation was also calculated by five existing methods provided above.

Table 2.1. ACME and EMCA organizations initial configuration (Created by author)

ACME	EMCA
ACME implementation is not aligned\certified by any IT Security document. However, some Security areas (e.g., Logical Access management) are adequately covered by the organization. ACME Complexity level = 3, ACME has complex information systems, which are used for data management and interchange with 3rd parties. ACME maturity level = 2 “Repeatable”. Some processes in the organization are implemented. However, they are weakly documented. The same 3rd party performed a risk assessment and penetration testing for both systems in scope. ACME has 342 employees and 5 main departments (Management board; HR; Finance; IT support; Developers) Consultant hour rate – 30 € Employee hour rate – 11 €	EMCA organization is already certified and is aligned with ISO 27001 standard; however, wants to be aligned with PCI DSS standard. EMCA Complexity level = 3, EMCA has complex information systems, which are used for data management and interchange with 3rd parties. EMCA maturity level = 4 “Managed”. Main processes are fully managed, which means they are documented, monitored and are fully under the day by day control. The same 3rd party performed a risk assessment and penetration testing for both systems in scope. EMCA has 245 employees and five departments (Management board; HR; Finance; IT support; Developers) Consultant hour rate – 30 € Employee hour rate – 11 €

Information security implementation costs for both organizations were calculated according to the proposed methodology. Calculation results are presented in Table 2.2, where the calculation equation is provided along with related comments on each step. Detailed calculation is given in Annex A.

Table 2.2. Cost of information security implementation of ACME and EMCA organizations (Created by author):

Formula	ACME	EMCA
Information security implementation costs $C_{Security} = \varphi(C_{Risk\_assess} + \sum_{i=1}^{n} C_{Sec\_control\_implementation_i}(stnd))$	$C_{Security} =$ 1.5 $*$ (1977 + 246.4) = 3355.1 €	$C_{Security} = 0.75 * (1815.56 + 3671.4) = \mathbf{4115.22}$ €

Given methods were evaluated by comparing calculation time for initial iteration; methods calculation time, when security requirements of the new document were added to the calculation scope; possibility to integrate new security document; possibility to re-use previous calculation results. Second criteria allow us to evaluate methods re-usability and quality of links with existing or new security documents.

Calculation, according to The Balance sheet oriented approach took approximately the same amount of time as the new method (~ 1 hour to gather information and calculate control implementation cost). Cost calculations for ACME organization were easy and effective because the organization did not have any controls in place and tried to implement new controls from scratch. Cost calculations for EMCA were complicated because in this case, both the cost of existing controls and the cost of additional actions had to be identified. It should be noted that from the Security point of view, document mapping was performed manually. It means that each new document would require from us additional document and requirements mapping actions, which are growing exponentially with the number of mapped documents.

The Security measure life-cycle approach required 40 minutes to perform calculations. However, risk analysis costs and procedural controls implementation costs identification was complicated. It has to be mentioned that this method let easily re-use results from previous calculations, so the calculation for EMCA organization, which tried to be aligned with second IT Security document, was performed quicker than for ACME organization.

IT-Security process-oriented approach takes 1.5 hours to perform calculations. The most complicated part was risk calculation because it required to have historical data about the incidents related to this control. Another identified issue is that the calculated risk does not have any correlation with mitigation controls. From a security point of view, it means that is not clear why one or another decision was made.

The ISO/IEC 27001 method made it possible to calculate information security costs in 35 minutes. However, the calculations revealed that it was difficult to identify control implementation expenses related to such areas as organization and people. It should be mentioned that this method proves to be very useful during calculation for EMCA organization. The method closely aligned to ISO/IEC 27001 standard, which covers practically all information security areas and because of that could be easily mapped with PCI DSS standard requirements.

The Information Security Management System – Layer approach was low effective for single control calculation. It took 1.75 hours to calculate Logging and Monitoring control costs according to this method. Besides, it has to be mentioned that some important areas such as Architecture and concepts were ignored during single control calculation because their calculation required the involvement of other system costs, which was out of scope for our experiment.

A newly proposed method has one weak point, compared to the existing methods – it is based on a complicated calculation. However, even such complicated calculation took only twice as long as the quickest cost calculation method. Besides, it should be noted that the calculation is complicated just for the first time. During the second cost evaluation, a large part of the results obtained during previously performed calculations could be reused due to their control orientation. It means that previous calculation results could be easily reused if needed.

As far as the advantages of this method are concerned, it could be mentioned that this method t is control oriented, and as such is fully aligned with the existing Security documents and procedures and could cover all needed information security aspects.

According to Yolles (Yolles 1999), viability systems are complex actor systems which can survive under change through adoption. The same viability criteria could be applied to the proposed method. Our experiment, with the implementation of a single security requirement/control in 2 different organizations, proved that this method could be effectively applied for the organizations with varying levels of complexity and maturity. According to demand, it could be used to verify any current Information security document implementation costs, as soon as a list of Security requirements/controls related to this document is defined.

The proposed method could be most effectively used with specific tools or solutions, which would make it possible to map two or more information security document. In that case, after the first evaluation, the organization would be able to clearly identify which controls or areas in their organization are not secured or aligned with security document, and according to calculation results from previous evaluation to predict how much it will cost them. Such effects could be achieved by using IT Security document automation tools.

For verification of the proposed method and 5 security cost evaluation methods presented in Chapter 1, we used the Cooke’s classical model (Cooke 1991). Cooke’s classical model (Cooke 1991) builds a weighted expert probability assessment combination based on the proper scoring rule theory, where good calibration and low entropy are the main factors. This model elicits quantiles from the experts’ distributions. These scores are calculated based on the experts’ answers to the specific seed questions. A seed question is a specific type of question, for which the correct answer is known at the time of analysis and is used for evaluation of the experts’ knowledge.

The calibration score shows the deviation of the respondent’s evaluation scores from the true values of the known seed questions. These questions require the respondents to specify a probability distribution to describe an uncertain continuous variable that is divided into a number of ranges. For this calibration, it is divided into four ranges with the dividers being 5th, 50th and 95th quantile values based on (Cooke 2008). Let s = s1, …, sn be a probability distribution and assuming pi > 0, i = [1; 4]; then the relative information of s with respect to p is (Cooke 1991):

$$I(s,p) = \sum_{i=1}^{4} ln \frac{s_i}{p_i}. \tag{2.18}$$

I(s, p) is an index of the information learned if it was believed that p was correct but subsequently learnt that s is correct.

A set of experts *e* = 1*, ...,* E assesses probabilities of each uncertain event. They assign the corresponding indicator functions to one of *B* probability bins that are associated with a distribution over the possible outcomes. These bins are described by the probability p_b of occurrence, in the range of [0; 1], *b* = 1, …, *B*.

Based on the observed values and the assignments, weights, w_e are determined for each expert. The weights have to satisfy the following: $w_e \geq 0$ and $\Sigma w_e = 1$. The weight w_e are defined for each expert individually.

Let n_b be a number of variables assigned to *b*, s_b – the sample distribution of variables in bin *b* and *N* – the sum of the variables n_b and *H*(p_b) – the probability vector. Then the average response entropy is:

$$H_e(n) = \frac{1}{N} \sum n_b \, H(p_b). \tag{2.19}$$

The calibration score is:

$$C(e) = 1 - \chi_B^2 [\sum 2 n_b I(s_b, p_b)]. \tag{2.20}$$

If the expert sample distribution realizations are drawn independently from a distribution with quantiles as stated by the expert, then the likelihood ratio statistic *2NI*(*s, p*) is asymptotically distributed as a chi-square variable with 3 degrees of freedom (Cooke 2008). Then (2.7) becomes:

$$C(e) = 1 - \chi_3^2 (2NI(s,p)). \tag{2.21}$$

As opposed to the entropy, the information score is the second variable for the scoring. In distribution, the information is the distribution concentration degree. Concentration or dis-concentration is measured relative to some other distribution. The information is expressed as:

$$I_e(n) = \frac{1}{N} \sum_{i=1}^{N} I_i. \tag{2.22}$$

Expert assessment combination is called a decision maker. “Good expertise” is considered to have good calibration and good information. Weights are associated with rewarding the “good expertise” in the process of decision making.

If the expert calibration score is above the set threshold, the weight of the expert e is the multiplication of calibration and information scores:

$$w_{\alpha}(e) = C(e)I_e(n). \tag{2.23}$$

Otherwise, the weight is set to zero. The threshold is set at the optimal position that is described as the highest possible weight of a virtual expert (Sommestad *et al.* 2011).

The seed questions are required to be very well validated and fall for the same domain of which the unknown variables are. These seed questions serve as an expert performance evaluation mechanism leading to weighing the importance of individual expert's opinion to the whole dataset The robustness of the weighting is highly dependable on the number of seeds used. Based on (Cooke 1991) eleven questions is enough to recognize a substantial difference in calibration. These questions include both – overall knowledge about information security (questions from 1 to 21) and specific questions about information security documents (questions from 22 to 25) The known answer values of known questions are taken from the information security reports developed by such well-known security players as PwC, Verizon, Ernst and Young, Ponemon institute and others Questions from 22 to 25 are taken from ISO 27001 standard, GDPR regulation, PCI DSS standard and NIST best practices.

The seed questions of the survey are presented in the Annex B Table A.2. The quality of expert knowledge is to be expressed by the weights that are to be assigned to the experts, depending on their knowledge. The quality of knowledge is assessed using the Cooke's expert elicitation method and the expert input correlation to the known facts in Annex B Table A.2.

To collect the required information – a set of experts of the domain is selected, and their expertise acquired. Based on the method, three main metrics are acquired – the calibration score, mean relative total and the weight of an expert. The weights are then normalized so that the sum of the weights equals 1. The results of these calculations are presented in Table 2.3.

Table 2.3. Weights of expert assessments (Created by author)

Id	Calibration	Mean relative total	Unnormalized weight	Normalized wight w_e
E1	0.00476	2.072	0.00986	0.2597
E2	0.00277	2.108	0.00583	0.1535
E3	0.00264	2.111	0.00558	0.1468
E4	0.00264	2.112	0.00558	0.1469
E5	0.00264	2.107	0.00557	0.1466
E6	0.00218	2.116	0	0
E7	0.00264	2.105	0.00556	0.1464

After verification of expert knowledge, we left 5 experts, who asked to evaluate given 5 cost evaluation methods according to 5 criteria provided by us. Two worst evaluation results were eliminated. Each factor was evaluated in the scale from 1 to 10, where 1 shows that the method does not satisfy the requirement, and 10 shows that it entirely fills it. Averages of expert evaluations were used as qualitative values for each criterion (Table 2.4). Graphical presentation for comparison results is presented in Fig. 2.1.

Table 2.4. Information security costs implementation methods evaluation (Created by author)

Cost evaluation method	Intelligibility for Senior management	Links with existing Information security documents	Calculation complexity	Information security aspects coverage	Reusability	Overall results
The Balance Sheet Oriented approach	9.6	3.4	5.6	3.6	7.4	29.6
The Security measure life-cycle approach	6.8	6.4	7.2	5.8	8.6	34.8
IT-security process oriented approach	5.2	7.6	7.8	8.8	8.2	37.6
The ISO/IEC 27001 oriented approach	6.4	9.4	4.2	9.6	7.6	37.2
The Information security Management System – Layers approach	3.8	9	3.8	9.6	7.4	33.6

The results obtained highlight the fact that each technique has its weak points. The best effect was achieved by IT-Security process-oriented approach. However, senior management might find it difficult to understand this method. Furthermore, reusing it for another IT Security document implementation could be an issue. However, this approach allows covering all Information security areas, starting from operational controls and finishing with technical risk mitigation controls implementation.

Other methods had some disadvantages, which do not let them be effectively used for new Information security document requirements implementation purpose.

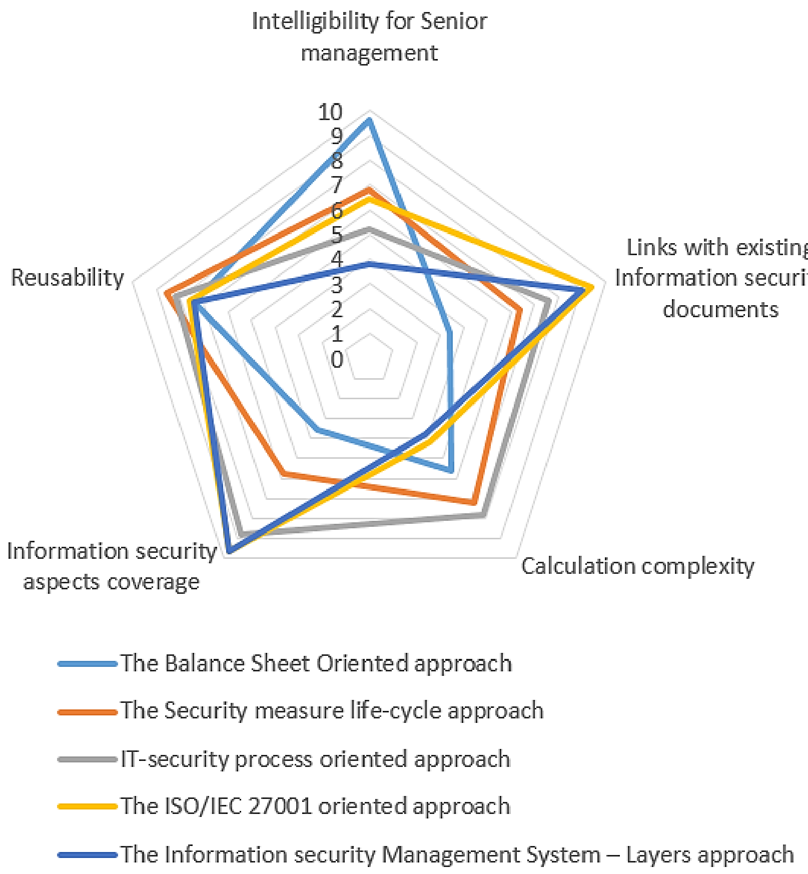


Fig. 2.1. Information security costs implementation methods comparison results (Created by author)

The main identified obstacles are:

- Issues with covering organizational controls related to information security;
- Too narrow or too wide view on security control cost evaluation;
- Problems to separate controls between different categories of costs.

To verify the new method against an already existing method, the same five criteria were used. Verification was performed by the same 5 experts. Table 2.5 presents information security consultant evaluation results for the newly proposed method:

Table 2.5. Evaluation of the proposed method against existing security cost evaluation methods (Created by author)

Cost evaluation method	Intelligibility for Senior management	Links with existing Information security standards	Calculation complexity	Information security aspects coverage	Reusability	Overall results
Proposed method	8.2	9.6	2.4	9.6	8.8	38.6

Achieved results were compared with information security costs evaluation results, calculated and presented in table 2.6. In comparison with existing Information security costs implementation methods, the proposed method is most effective in Links with existing Information security standards and Information security aspects coverage areas.

Table 2.6. Evaluation of the proposed method against existing security cost evaluation methods (Created by author)

Cost evaluation methods	Proposed method	The Balance Sheet Oriented approach	The Security measure life-cycle approach	IT-security process-oriented approach	The ISO/IEC 27001 oriented approach	The Information Security Management System – Layers approach
Results	38.6	29.6	34.8	37.6	37.2	33.6

The proposed method has the highest overall result. However all experts highlighted calculation complexity and complicated initial information gathering. Experts highlighted strong connections with Existing Security standards. IT Security process-oriented method, showed similar results as the main disadvantage was mentioned intelligibility to the management.

2.2. Improvement of Security Costs Evaluation Process by Using Data Automatically Captured from Business Process Model and Notation also Event-driven Process Chain Models

At least four main calculations components (asset analysis; incident impact; control implementation and control operation), presented in our control-based security implementation cost verification method, directly depend on organization's business processes and elements which are participating in them. If these elements are correctly defined in the business process diagrams, it could help with automating the identification of an organization's critical data assets. These assets (and their environment) could be integrated automatically in our security costs evaluation process.

To identify the most effective diagrams, evaluation criteria must be defined. Two criteria were chosen from a set used by Aldin *et al.* (Aldin and de Cesare 2009). The other three criteria, proposed by the author, are not so important for business process techniques integration to security cost evaluation process. The 3rd criteria was offered by us and used to evaluate data presented by business process techniques. Our evaluation will be based on:

- Availability of details needed for security cost evaluation. From the proposed security cost evaluation method point of view, it is very important to identify hardware and software, which are participating in critical business processes. Also, it is important to define the key stakeholders or organization employees who are implementing the business processes and data, which is used in the operations. Thus, the business process diagram should have the possibility to present details about the components mentioned above.
- Ease-of-use. This criterion helps us to understand the extent, to which the business stakeholders who do not have specialist knowledge of the technique could be ready to apply the business process model technique. It is important because business process diagrams will be developed by different types of specialists and will need to have a sufficient level of details about components used to ensure this process.
- Understandability. This criterion helps us to understand the extent to which the business stakeholders who do not have specialist knowledge of the technique could understand the business process model technique. The argument for choosing this criterion is the same as for the previous one.

In the first chapter, Business process modelling methods (i.e., BPMN, EPC, Flowchart, and Data Flow Chart) were presented and evaluated against these three criteria. BPMN and EPC were identified as the most effective because they provide more information needed for security cost evaluation.

In the first chapter, Business process modelling methods (i.e., BPMN, EPC, Flowchart, Data Flow Chart and UML activity diagram) were presented and evaluated against these three criteria. BPMN and EPC were identified as the most effective because they provide more information needed for security cost evaluation. UML activity diagram wasn't chosen for the further experiment because Cibran provided a way for translating BPMN models into UML activities (Cibran 2009). In addition comparison performed by Geambasu does not offer evidence that exists differences in modelling using BPMN and UML 2.0 Activity Diagrams from the point of view of end-user readability (Geambasu 2012).

To verify these models as the sources for initial input for the implementation costs evaluation method, the same simulation as the one performed during verification of the security costs evaluation method itself was used. For the experiment, an abstract organization ACME and implementation of logging and monitoring control (mandatory according to all IT security documents) processes were taken.

Fig. 2.2 and 2.3 illustrate information they could provide and the type of missing information.

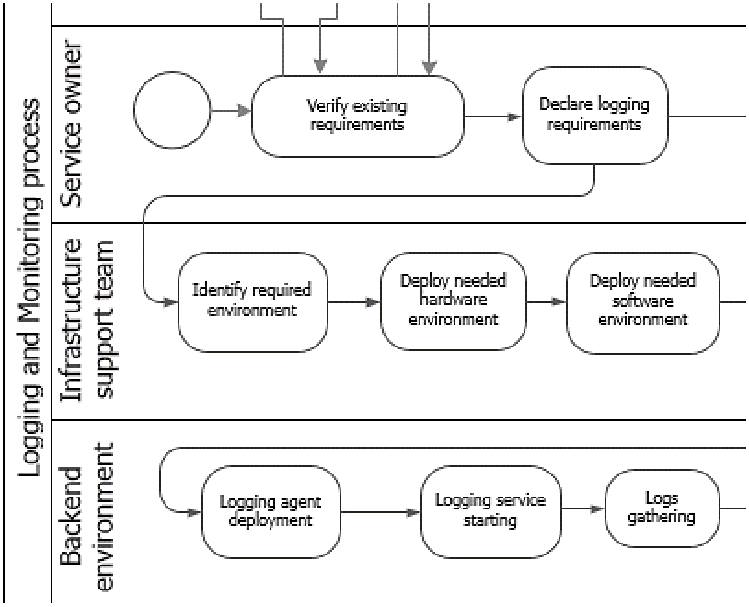

Logging and Monitoring process
Service owner
Verify existing requirements
Declare logging requirements
Infrastructure support team
Identify required environment
Deploy needed hardware environment
Deploy needed software environment
Backend environment
Logging agent deployment
Logging service starting
Logs gathering

Fig. 2.2. Part of the Logging and Monitoring process Business Process Model and Notation Diagram (Created by author)

It is necessary to mention that some diagram components can provide the only piece of needed information, and some elements are participating in the evaluation; however, they are not directly related to the control implementation costs.

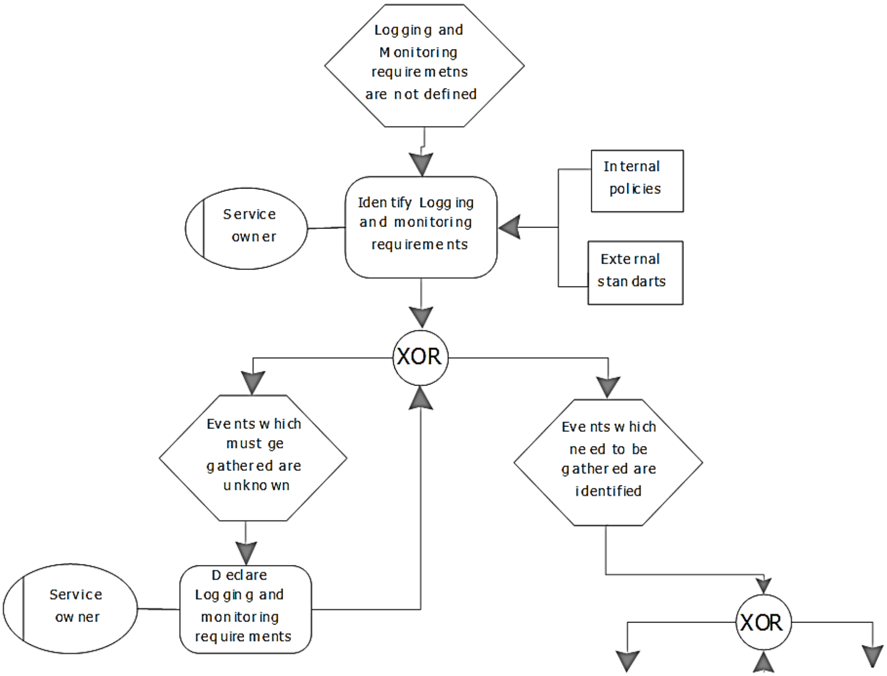

Logging and Monitoring requiremetns are not defined
Service owner
Identify Logging and monitoring requirements
Internal policies
External standarts
XOR
Events which must ge gathered are unknown
Events which need to be gathered are identified
Service owner
Declare Logging and monitoring requirements
XOR

Fig. 2.3. Part of the Logging and Monitoring process Event-driven Process Chain Diagram (Created by author)

Provided example showing only part of the Logging and Monitoring process. This process is starting from the event, that organization do not have defined Logging and Monitoring requirements. This event initiates “Identify Logging and Monitoring requirements” function. Given function is executed by Service owner and is based on two documents “Internal policies” and “External policies”. These two documents describe Logging and Monitoring requirements. Function “Identify logging and monitoring requirements” could initiate one of 2 possible events. In the cases, when organization do not know, which events must be gathered initiated “Events which must be gathered are unknown” and in the cases, when logging and monitoring events are known initiated event “Events which need to be gathered are identified”. This decision is made by applying operator XOR (Exclusive OR). XOR operator allows splitting one control flow into at least two branches. Event “Events which must be gathered are unknown” initiate function “Declare Logging and Monitoring requirements” owned by Service owner.

To present a variety in our analysis, four classes were used: provide all needed information (Full), provide part of the required information (Partial), required information does not directly link with control implementation (Not linked), and does not provide the required information (Missing). Table 2.6 summarises our results.

The analysis shows that the possibility to use business process diagrams for security controls implementation directly depends on the level of details provided. Some parts of the cost evaluation method calculation are out of the scope since they are related to the organization itself and could not be identified from separate business processes diagrams. Other calculations are connected to the risk assessment process, which is used to determine the actual risk.

Table 2.6. Analysis of the cost method components from the business process perspective (Created by author)

The cost evaluation method component	BPMN and EPC	Comments
Complexity and maturity coefficient	Not linked	This component is common for the whole organization, and from the separate control evaluation point of view, it could be ignored.
Assets analysis	Partial	Fig. 2.1 and 2.2 allow the identification of primary stakeholders and infrastructure participating in the process, but it does not provide enough information on software and hardware details.
Vulnerability analysis	Partial	Lack of hardware and software details. Lack of information on organization procedures and policies. Automation is not possible.
Threats analysis	Missing	A security consultant performs this part of cost evaluation; thus, the diagram does not have this information.
Impact analysis	Partial	Diagram provides details on assets; however, it could not provide information about losses.
Penetration testing	Missing	This activity is optional and should not be present in business as a usual process unless the yearly test is planned.

End of the Table 2.6

The cost evaluation method component	BPMN and EPC	Comments
Gap analysis	Partial	Our diagrams can provide a part of the needed details on infrastructure. However, the list of applied security requirements is out of scope.
Control criticality coefficient	Not linked	Risk identification is a result of risk assessment activities, which are out of scope for us.
Mitigation strategy	Not linked	Mitigation strategy, from the business process point of view, is not directly related to the business process flow.
Environment purchase (Action implementation)	Partial	Business process flow allows identification of environment, which is needed to ensure process; however, lack of details does not allow to define hardware or software.
Implementation team (Deployment Action implementation)	Full	Business process diagram allows us to identify units which will be participating in a new environment implementation process.
Configuration tasks (Deployment – Action implementation)	Partial	Business process diagram does not provide enough details on hardware and software configurations, because of that, it could be challenging to identify costs related to these activities.
Training/Awareness (Deployment – Action implementation)	Partial	Information on infrastructure and main stakeholders could help in identifying missing training, but lack of details does not allow us to ensure, that all needed training is recognized.
Supporting team (Operation activities)	Full	The business process allows us to identify all main stakeholders and their functions in the defined business process flow.
Environment support (Operation activities)	Partial	The business process allows us to identify infrastructure which will be used; however, lack of details does not allow to determine the level of support that will be needed and its price.
Other services (Operation activities)	Partial	This component is optional and will not be presented in all business processes.

It has to be mentioned that the business process can provide a part of the information for risk assessment, while other components, such as threat and vulnerability assessments, could not be linked to business processes. The high-level process design is presented in Fig. 2.4:

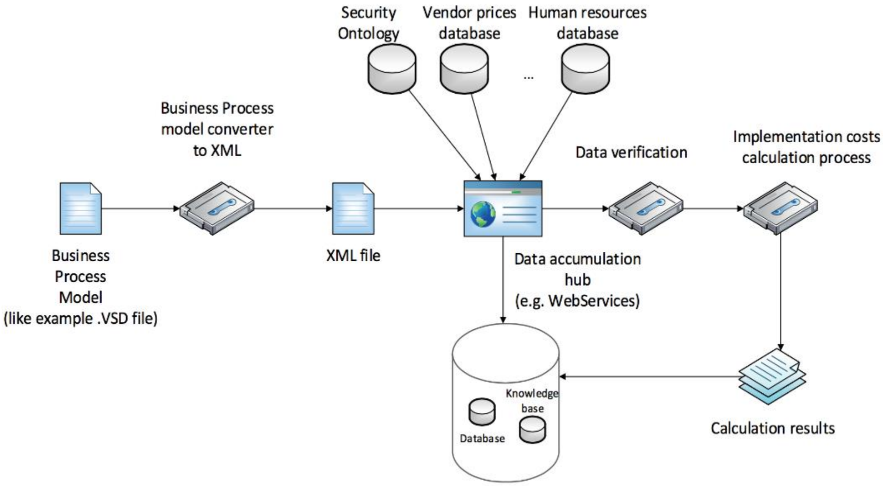

Security Ontology
Vendor prices database
Human resources database
...
Business Process model converter to XML
Data verification
Implementation costs calculation process
Business Process Model (like example .VSD file)
XML file
Data accumulation hub (e.g. WebServices)
Knowledge base
Database
Calculation results

Fig. 2.4. Business process model data integration with the cost evaluation method (Created by author)

The analysis of existing business process modelling tools has shown that all of them can store data process in a portable format, which is close to XML or can be converted to the XML format. Such an opportunity allows us to automate the process.

For the Logging and Monitoring processes provided in Fig. 2.1 and Fig. 2.2 improved data extraction allowed automatically extract data about process service owner, environment (hardware and software) under the logging and monitoring scope and procedures/documents which define logging and monitoring requirements. In our experiment were used such tools as Microsoft Visio for business process diagram presentation and conversion to the XML; Microsoft Excel for the calculation. Data accumulation step without involved in our experiment and data verification was performed manually

The initial file of a business process diagram is generated by one of business process modelling tools (in our experiment, Microsoft Vision was used). The generated data is transferred to a separate layer, where file data was converted to the XML format. Then the generated XML files are assigned to the middleware application. This application should help to extract and collect data needed for the security costs evaluation. Data sources could be different, starting from business process models, security documents, and finishing with ontologies (Ramanauskaite, Olifer, *et al.* 2013). As a middleware layer, Web-services solutions could be used. In our experiment, we used as a middleware layer the techniques, which allowed us to import data to Excel format. This data later on was used for security control cost calculations. Additional information required for calculations was entered into the XLSX spreadsheet manually.

It should be noted that in the principle diagram, the additional component "Data conversion verification" is used. In our experiment, this verification was done manually, by reviewing converted data. However, from the automation point of view, this process should be independent of the manual review.

The last component is the calculation process. In our experiment, the Microsoft Excel application was used for this purpose. Data from the business process model was imported to an Excel spreadsheet with the help of open source tools. After that, Microsoft Excel was used to calculate security cost for Logging and Monitoring control.

The proposed approach for automatic data gathering from business processes and gathered data integration to security cost evaluation process was verified in the experiment, which was performed in the ACME organization. The cost evaluation was performed for the Logging and Monitoring control system. The middleware components were replaced with open source conversion and import tools. To simplify the experiment, verification and additional data entry were performed manually. Need to be mentioned, that BPMN already has connections with security ontologies and has developed BPMN-security extensions (Maines, *et al.* 2015).

The performed experiment has proven that the approach could be used to gather initial information needed for security cost evaluation. However, several gaps need to be handled to make this approach more effective. The main issues identified by the experiment are as follows:

- A lack of details in the business process models. However, this vital information was not presented in the business process model developed by the business process owners by default;
- A lack of details on the environment or activities costs. It is essential to know the number of person-months and respective price to estimate the cost. This issue could be solved by performing additional mapping against vendors' prices or data supplied by the human resources (in the case of internal resources used);
- A lack of details related to the organizational (policies, procedures, guidelines) controls, which are in place in the organization;
- A manual approach for a part of activities that require further automation or application using more sophisticated tools.

During the experiment, the following valuable features of the method proposed were confirmed:

- An approach allows us to collect initial information needed for security requirements cost implementation evaluation from sources, which are well understood by the business owners. The use of the XML format allows us to easily integrate the proposed model with other input systems needed for cost evaluation methods if their data is presented in a compatible format. In the future implementation, WebServices could be used to integrate the existing solution with the security ontology or other valuable sources of information;
- The approach can automate the cost evaluation method because a massive amount of data and calculation could be done without operator interference. It is still critically important to automate the data verification process, which would allow us to ensure that data from different sources were imported without any errors.

2.2. Conclusions of Chapter 2

1. The proposed approach is security controls oriented and incorporates decision making and decision implementation costs. Complexity and Maturity level, incorporated in the calculations, allows applying the calculation to a broad set of organizations, characterized by a different level of systems and process complexity. Orientation to separate controls makes it possible to incorporate new security document without the need to re-calculate previous results.
2. The performed experiments have shown that although the first calculation is time-consuming (more then 1 hour) and requires a large amount of information (up to 17 formulas with up to 32 different components), every next calculation for a newly added control or security document reuses data from the previous calculation and takes more than 50% less time. Information re-usage reduce amount of information needed for furher calculation up to 70%.
3. The amendments suggested enable data import from the Business Process Model and Notation diagram also Event-driven Process chain diagram. Some calculation components weren't presented in the business processes diagram (up to 32%). The research revealed that 11 (68%) of 16 components used for Logging and Monitoring cost evaluation of are presented in the business processes.

3

Automation of Harmonization, Analysis and Evaluation of Information Security Requirements

As it was highlighted, organizations are forced to seek compliance with a set of multiple security documents. The proposed security cost implementation method would let us calculate the cost of specific security control or document. However, it would not be able to identify mandatory requirements applicable to the organization. To solve this problem, there needs to be an approach defined which would enable the harmonization of a set of various security documents. Further analysis would allow identifying a list of requirements, which are applicable to the organization, from the set of requirements of multiple security documents.

This Chapter describes the harmonization technique, which was chosen for multiple security documents linking and visualization of the linking result. Regarding the fact that existing security ontologies (A. Herzog, G. Decker and S. Fenz) are not oriented to security controls implementation and do not cover a large amount of existing security documents requirements, a new ontology has been proposed. The new ontology is based on COBIT v5, allowing to increase the number of security requirements covered by the new ontology. For effective analysis of a harmonized set of security documents, graph-based and Chord diagram-based visualizations were proposed.

A harmonized set of security documents explains how various security documents requirements are linked and covered. However, it does not allow to identify the Minimum Security Baseline. Thus, a new graph theory optimization algorithms-based approach was proposed. Vertex cover algorithms and subgraph isomorphism property allow removing duplicated requirements and generating Minimum Security Baseline from the graph of a harmonized set of security documents. Furthermore, subgraph isomorphism property makes it possible to identify similar structures in the different graphs and is used for verification of organization implemented controls against Minimum Security Baseline.

The proposed methods and results were published in international journals and presented in international conferences. The new COBIT v5 based ontology was published in (Ramanauskaite, Goranin, *et al.* 2013) and (Ramanauskaite, Olifer, *et al.* 2013). The proposed Minimum Security Baseline identification method was published in (Olifer, Goranin and Cenys, *et al.* 2019).

3.1. Security Ontology for Adaptive Mapping of Security Documents

As was summarized in Chapter 1 of this thesis, S. Fenz's and A. Herzog's ontologies have low-security document coverage and because of that do not allow to effectively link multiple security documents. At the same time, adaptive mapping as harmonization technique proves that a unified security framework would enable to develop a flexible structure, which could be easily amended upon demands.

Harmonization through adaptive mapping requires having the base, which would be oriented to the security controls and allow covering as many security areas as possible. Existing security documents are not fit for the purpose because they define security requirements with a different level of details and cover different security aspects.

3.1.1. Security Ontology for Adaptive Mapping of Security Documents

Because of that, a new general-purpose security ontology, which would extend these two ontologies and would be more suitable for adaptive mapping of security documents, was proposed.

The proposed ontology consists of five high-level classes in Fig. 3.1:

- Asset;
- Countermeasure;
- Organization;
- Threat;
- Vulnerability.

These five classes are the most basic in the security area and are detailed at lower levels.

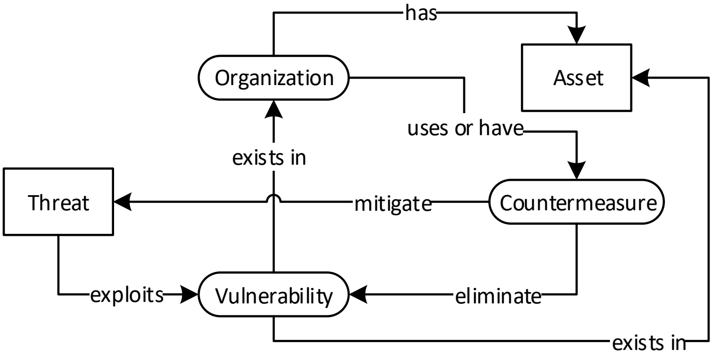


Fig. 3.1. The top-level structure of the proposed Security ontology (Created by author)

Asset class describes both tangible and intangible assets an organization can have. In proposed ontology. This class is described more appropriately than other security ontologies are adding more information on the usable data by the organization, location and other equipment, owned or used in the company and related to organization's security. The intangible asset is divided into Data and Software, while the inner structure describes various types of data and software. The tangible assets are structured into subclasses of Movable and Unmovable assets in Fig. 3.2. Immovable assets describe the location and building concepts and the main elements, which can be found in it. Movable assets are structured into four subclasses: alarm systems and detectors; furniture; IT components; utilities. These four categories allow the creation of more links to security documents by defining what kind of assets are related to specific controls (what is at risk, what has a vulnerability, etc.).

Countermeasure and Threat classes are described pretty well in A. Herzog's ontology. Therefore, minor changes were made to it, and a similar structure and components to A. Herzog's ontology were used.

The need for more organizational concepts arose during the mapping of security documents, according to A. Herzog's and S. Fenz's security ontologies.

These two ontologies have a poor description of organization structure and policies, while the companies' information security policy is the most important to ensure its security. As subclasses of the organization, Department, Personnel and Policy concepts were distinguished (see Fig. 3.3). Precise control description of security documents can be achieved if links to confident executor are be made. Therefore, the Department and Personnel classes were added and detailed to distinguish plausible types of departments and positions within it.

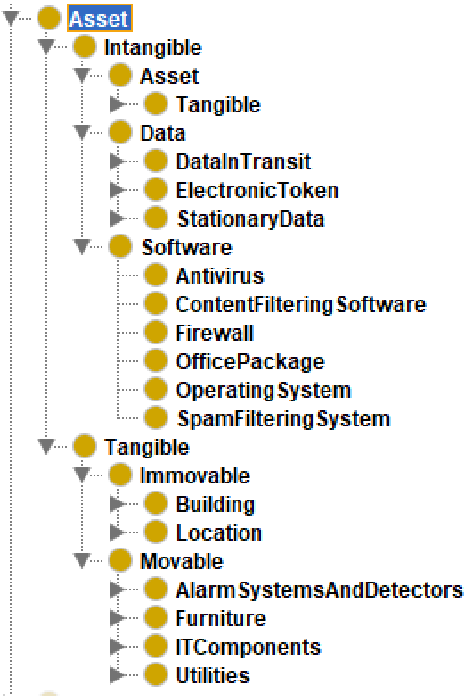
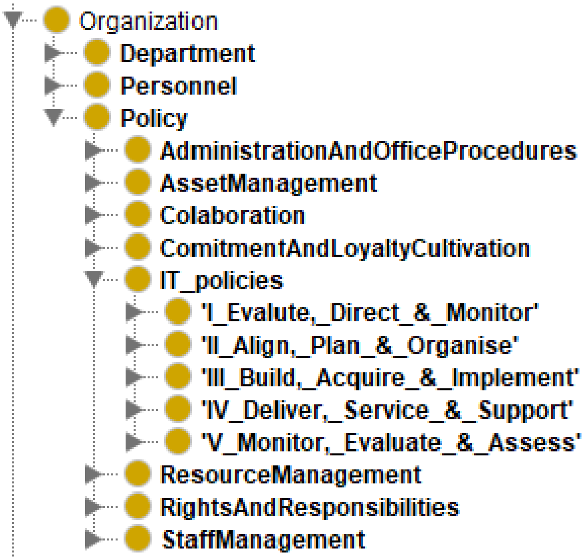


Fig. 3.2. The basic hierarchy of asset concept (Created by author)

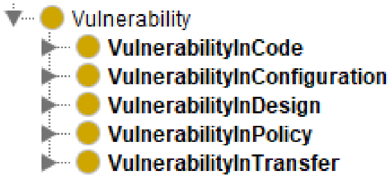
Therefore, the COBIT 5 framework (ISACA 2013) was adopted into our ontology, by defining IT policy class as organization policy subclass, where all COBIT 5 ideas are detailed. The COBIT 5 framework guarantees the intuitive use of an ontology to those who are familiar with the COBIT framework. Meanwhile, to propose multiple views and ways to find the necessary concepts in the ontology, more subclasses were added to Policy class (see Fig. 3.3). These classes should present more general policies of the organization. However, most of them have relations to classes of IT policy class (COBIT 5 framework).



- Organization
  - Department
  - Personnel
  - Policy
    - AdministrationAndOfficeProcedures
    - AssetManagement
    - Colaboration
    - ComitmentAndLoyaltyCultivation
    - IT_policies
      - 'I_Evalute,_Direct_&_Monitor'
      - 'II_Align,_Plan_&_Organise'
      - 'III_Build,_Acquire_&_Implement'
      - 'IV_Deliver,_Service_&_Support'
      - 'V_Monitor,_Evaluate_&_Assess'
    - ResourceManagement
    - RightsAndResponsibilities
    - StaffManagement

Fig. 3.3. The basic hierarchy of organization concept (Created by author)

Vulnerability class was not properly detailed in A. Herzog's (Herzog, Shahmehri and Duma 2007) and S. Fenz's (Fenz 2010) ontologies as well. S. Fenz provides a list of vulnerabilities describing individuals with no structure, while A. Herzog describes basic types of vulnerabilities. Therefore, vulnerability class was extended by dividing it into Code vulnerabilities, Configuration vulnerabilities, Design vulnerabilities, Policy vulnerabilities and Transfer vulnerabilities (see Fig. 3.4). Those classes are detailed to reflect the basic security vulnerabilities. However, they are more structured than in S. Fenz's ontology, to make them more intuitive and more straightforward for visualization.



- Vulnerability
  - VulnerabilityInCode
  - VulnerabilityInConfiguration
  - VulnerabilityInDesign
  - VulnerabilityInPolicy
  - VulnerabilityInTransfer

Fig. 3.4. The basic hierarchy of vulnerability concept (Created by author)

To use this ontology as a basis for adaptive mapping of security documents, a clear and intuitive ontology structure has to be maintained (Fig. 3.5).

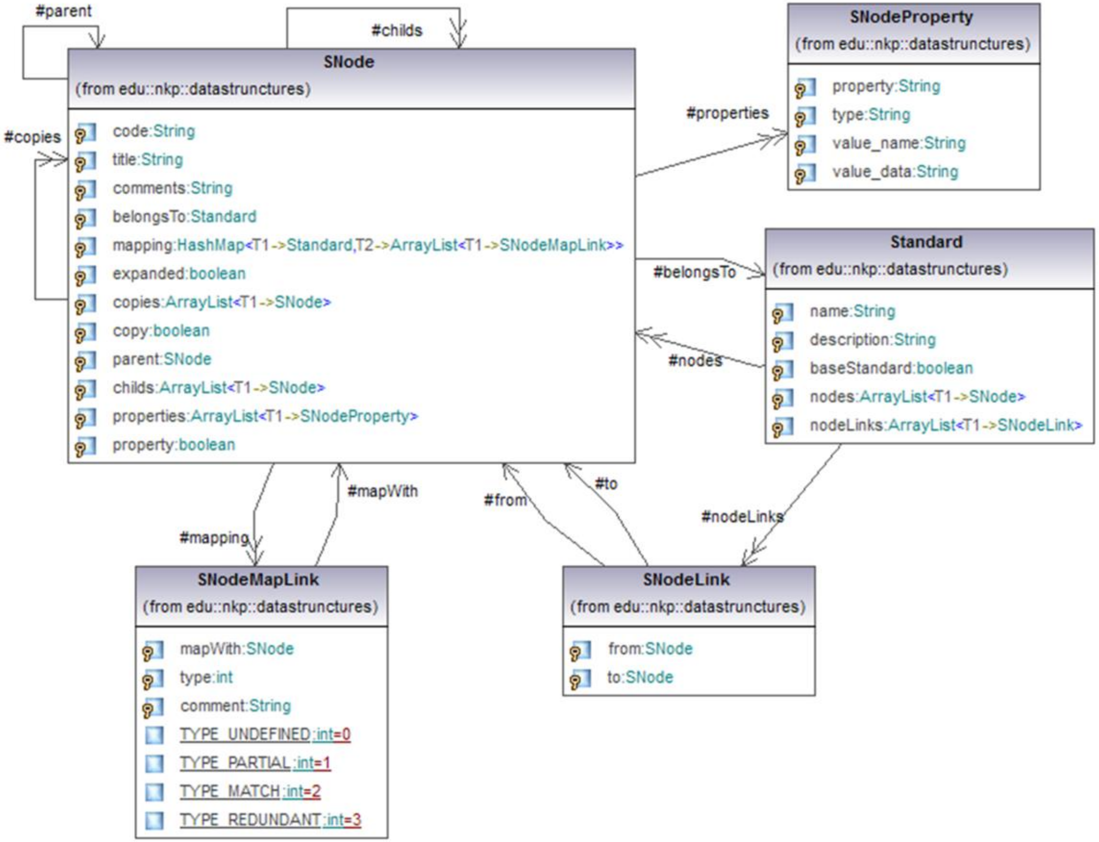
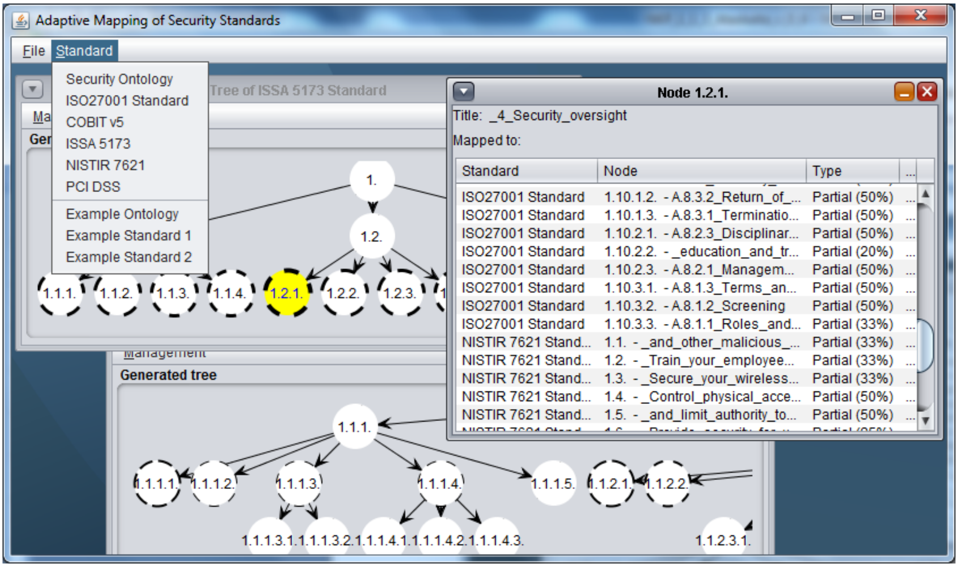


Fig. 3.5. Data structure for security ontology dedicated to adaptive mapping (Created by author)

The tree structure of the ontology was optimised. Therefore it currently has 1795 classes, an average depth of the class tree is 6.5 (maximum value of the depth of class tree was equal to 9), and an average branching factor of the class tree is 4.8 (has from 1 to 18 subclasses). Such a structure is more viewable in a tree structure and should be more intuitive for ontology users (see Fig. 3.6). Ontology consistency was verified by Protege 5.5 Reasoner plug-in Pellet 2.2. It is an automatic tool, which allows analyzing ontology characteristics seeking to evaluate classes, object property, data property, individuals. Identified inconsistency issue was amended on the fly during the ontology development phase.



Title: _4_Security_oversight

Mapped to:

Standard	Node	Type	...
ISO27001 Standard	1.10.1.2. - A.8.3.2_Return_of_...	Partial (50%)	...
ISO27001 Standard	1.10.1.3. - A.8.3.1_Terminatio...	Partial (50%)	...
ISO27001 Standard	1.10.2.1. - A.8.2.3_Disciplinar...	Partial (50%)	...
ISO27001 Standard	1.10.2.2. - _education_and_tr...	Partial (20%)	...
ISO27001 Standard	1.10.2.3. - A.8.2.1_Managem...	Partial (50%)	...
ISO27001 Standard	1.10.3.1. - A.8.1.3_Terms_an...	Partial (50%)	...
ISO27001 Standard	1.10.3.2. - A.8.1.2_Screening	Partial (50%)	...
ISO27001 Standard	1.10.3.3. - A.8.1.1_Roles_and...	Partial (33%)	...
NISTIR 7621 Stand...	1.1. - _and_other_malicious_...	Partial (33%)	...
NISTIR 7621 Stand...	1.2. - _Train_your_employee...	Partial (33%)	...
NISTIR 7621 Stand...	1.3. - _Secure_your_wireless...	Partial (33%)	...
NISTIR 7621 Stand...	1.4. - _Control_physical_acce...	Partial (50%)	...
NISTIR 7621 Stand...	1.5. - _and_limit_authority_to...	Partial (50%)	...

Fig. 3.6. Structure fragment of proposed security ontology and adaptive mapping data in Adaptive Mapping of Security Document (created tool for adaptive mapping of security document) (Created by author)

While structure optimisation of new security ontology is more important to ensure user-friendly usage and understanding, the new concepts allowed better coverage of security documents. A direct list of controls was not provided, and a similar ontology structure was used for document mapping as in A. Herzog's ontology. Therefore, security document mapping to this ontology has to be done by defining more than one link to ontology. This mapping property is useful to analyse and map security concepts according to different documents.

ISO27001(ISO/IEC:27001 2013), PCI DSS (PCI 2016), ISSA 5173 (Information Systems Security Association 2011) and NISTIR 7621 (NISTIR

7621 2016) security standards were specified and mapped to the new security ontology to evaluate its suitability to link security standards. 80% of ISO27001, 100% of PCI DSS, ISSA 5173 and NISTIR 7621 standards were mapped to the ontology (see Table 3.1), by using adaptive mapping through ontology.

The 100% mapping of ISO27001 standard was not achieved because particular security standard requirements (like security properties of the operating system being used, etc.) were not mapped to high-level components of our ontology.

Table 3.1. Amount and percentage of ontology entities mapped with security requirements of the standards (Covered) and amount and percentage of security requirements of the standard mapped to the ontology (Covers) (Created by author)

Standard	Ontology / Standard coverage	
	Proposed ontology	
	Covered	Covers
ISO27001	130/1795 (7%)	107/133 (80%)
PCI DSS	132/1795 (7%)	165/165 (100%)
ISSA 5173	15/1795 (1%)	12/12 (100%)
NISTIR 7621	19/1795 (1%)	10/10 (100%)

The ontology in question and mapping of the above four security standards to it can be used to generate adaptive maps between any of the two mapped security standards, or an integrated standard can be created with the use of any set of the mapped security standards without the necessity of directly mapping two security standards. As our proposed security ontology can cover a more substantial part of concepts in the analyzed security standards (the average coverage of these 4 security standards is 92%, while S. Fenz's average coverage of these security standards is 27%, A. Herzog's – 20%), the adaptive mapping of security standards will be more precise by applying it as a basis ontology (Table 3.1). However, the ontology does not cover all standards by 100%. Therefore it should be improved to get an even bigger precision of adaptive mapping.

3.1.2. Visualization of Mapped Security Documents

From the list of visualization methods analysed in Chapter 1 of this thesis for Security ontology representation, the tree (a specific kind of graph) structure was proposed. Such an approach allows us to represent the concepts of the document and to display inheritance links to describe only the main structure. Other connections could be presented through node notation and analysed by viewing detailed information of a specific node.

Some node notation modifications are proposed to make the document tree more representative for viewing the mapped documents:

- The width of stroke for a node defines how many documents have an analogue for this control (the number of mapped documents, and not the number of mapped nodes in other documents).
- The pattern of stroke for a node defines what type of match the node has with the nodes of other documents (if the node of a different document partially matches the node – the value is 1; if the node of a different document fully matches the node – the value is 2; if the node of a different document is redundant – the value is 3):
  - The length of the dash defines the maximum match value.
  - The length of space defines the minimum match value.

Additional information, such as a full description of the node, details of controls matching, etc. should be represented separately for each of the nodes. A small example of integrated security document tree notation usage is presented in Fig. 3.7. It can be noticed that nodes A-1, A-2, A-9, A-3, A-10 and A-7 have no matches in other documents while nodes A-4, A-11, A-5 and A-8 have one match, whereas nodes A-6 and A 12 have two matches with different documents. The width of a node stroke can retrieve this information.

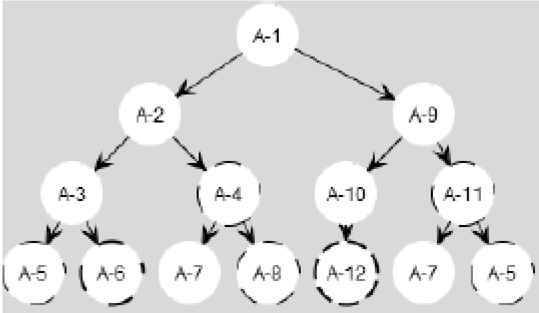


Fig. 3.7. Example of proposed security document mapping visualization, using graph structure (Created by author)

Graph-based visualization of the security documents with a large number of components is complicated because the graph requires a lot of space to present all of them. Besides, other disadvantages of this visualization are that only one document structure can be viewed at once (the user chooses which document should be displayed). Therefore, the mapping of only one document to other documents can be displayed, and there will be no full information about how different documents are mapped to each other.

To achieve full mapping information visualization with Chord diagram, it is better to use centric charts. They are more appropriate, as all document nodes can be viewed at once. A large number of links between nodes identified are grouped to increase the abstraction level. However, information that is more detailed can be extracted, including interactive explanations, highlights, etc. The biggest disadvantage of this type of mapped document visualization is the lack of document structure presentation. However, the visualization was improved by adding the document structures in the outer border of the circle. It increases the size of the diagram. However, both full mapping information and document structures can be visualized at the same time, see Fig. 3.8.

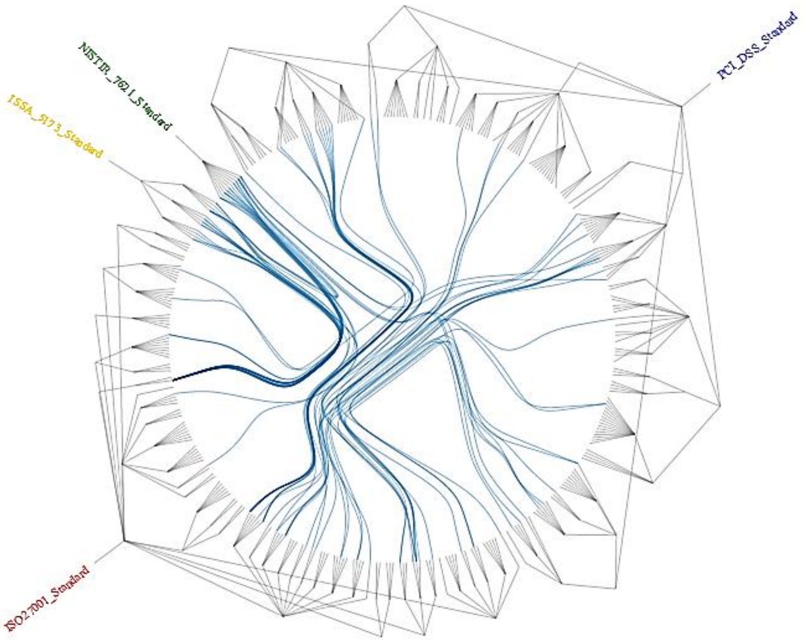


Fig. 3.8. Example of the Chord diagram for security document mapping visualization (Created by author)

Proposed visualization instances were verified by applying the System Usability Scale. The System Usability Scale provides a reliable tool for measuring usability. It consists of a 10 item questionnaire with five response options for respondents; from Strongly agree (5 points) to Strongly disagree (1 point).

Originally created by John Brooke in 1986, it used to evaluate a wide variety of products and services, including hardware, software, mobile devices, websites and applications. Visualization instances were verified by the same 7 Information Security experts, who participated in the evaluation of Information cost methods. According to the System Usability Scale verification method, systems which collect more than 80.3 are defined as "Excellent", between 68 and 80.3 are defined as "Good", systems which collect 68 are defined as "Average", between 51 and 68 are defined as "Poor", and below 51 are "Awful". Experts results are presented in Table 3.2.

Table 3.2. The System Usability Scale verification results (Created by author)

Expert	Chord diagram	Graph representation
E1	75	67.5
E2	78	78
E3	73	63
E4	80	88
E5	70	70
E6	78	83
E7	80	53
Average	76.29	71.79

As we can see from given results, both values are between 68 and 80.3, and it means, that both proposed instances could be defined as "Good". However need to be mentioned, that Chord diagram visualization gathered higher score and according to the experts are more usable, than graph representation. However, graph representation allows providing detailed information about each requirement and its links with other security documents requirements.

3.1.3. Method Evaluation Results

A general comparison of G. Denker's (Denker, Kagalb and Finin 2005), A. Herzog's (Herzog, Shahmehri and Duma 2007) and S. Fenz 's (Fenz, Ontology-based Generation of IT-Security Metrics 2010) security ontologies has shown the necessity of user-friendly ontology structure – all three ontologies have classes, with more than 25 subclasses in them. Such ontology could be challenging to use for visual presentation or quick knowledge search.

The OntoMetric methodology allows a more precise judgment of security ontologies rather than general comparison because it enables an evaluation of the content of compared ontologies. However, the evaluation marks are very dependable on the evaluator's opinion and requirements for the ontology. Assessment of ontologies' ability to be mapped to security documents is a more suitable measurement to choose the basis of the ontology for adaptive mapping of security documents compared to OntoMetric (Lozano-Tello and Gomez-Perez 2004).

To evaluate ontologies' suitability to map different security documents, percentage of concepts in security standards (ISO 27001 (ISO/IEC:27001 2013), PCI DSS (PCI 2016), ISSA 5173 (Information Systems Security Association 2011) and NISTIR 7621 (NISTIR 7621 2016)), which can be mapped to security ontology, was compared. This research revealed there are no security ontologies that would be able to map at least 50% of the analysed security documents. This fact implies the necessity of a new or modified ontology which could be used to present larger parts of knowledge, used in security documents.

A new security ontology was proposed. The new ontology was developed by integrating concepts of COBIT framework (ISACA 2013) and integrating part of classes of A. Herzog's and S. Fenz's ontologies. The new ontology increased the coverage of security documents. Using this security ontology, from 80% to 100% of the analysed security standards (ISO 27001, PCI DSS, ISSA 5173 and NISTR 7621) can be mapped to it. This percentage can be increased even more with the addition of more specific (related to payment cards, law and standard requirements, etc.) concepts to this ontology. The proposed security ontology has a more balanced tree structure as well, which increases its visualization possibilities.

Both of the proposed visualization methods were implemented in our adaptive mapping of security standard (hereinafter – AMSS) tool where four standards (ISO 27001, PCI DSS, ISSA 5173 and NISTIR 7621) were mapped using the proposed security ontology. The use of both of these documents mapping visualization methods showed that:

- A chord diagram is very helpful when the main trends in document similarities have to be estimated or summarised as the width of mapping links illustrates how often specific control is mapped to other controls. Furthermore, this visualization method helps to identify unmapped controls as "blank areas" with no mapping connections are seen.
- The improvement of Chord diagram to add the hierarchy of document nodes was useful, as now the Chord diagram can provide almost the same information as a graph structure diagram.
- Graph structure visualization is more suitable when one security document has to be analyzed, and the information is needed on how controls of this document match control in another document, what type of matching exists between those two nodes, etc.

3.2. The Proposed Method on MSB Identification and Verification Against Deployed Controls

The previously proposed adaptive mapping method (Ramanauskaite, Olifer, *et al.* 2013) was valid for an understanding of the overall security requirements and visualization of their connections but could not be used for MSB identification. It was proved in (Olifer *et al.* 2017) and (Olifer, Goranin and Janulevicius, *et al.* 2017), where security requirements implementation cost evaluation through control-based method was proposed, that security controls and security document requirements presentation as nodes and their connections as a link between nodes is effective.

Minimum Security baseline identification for the set of security documents, require to implement a few steps. The first step requires to harmonize set of different security documents to define a list of all requirements applicable for the organization. Security ontology and adaptive mapping through it allows adding a new security document, without the need to review previous harmonization results. The second step requires to analyze a set of security requirements from different security documents and identify unique requirements. This step could be implemented by applying graph theory properties (Johna and Wilscy 2015).

For MSB identification, information security documents presentation as undirected graphs, when the graph is defined as a pair of sets (V, E), where V is the set of vertices and E is the set of edges, formed by pairs of vertices, were proposed. In our case, security requirements are graph nodes, and edges between graph nodes show the links between these requirements. When two or more information security documents have to be mapped, a new graph is created by establishing relationships between the corresponding requirements of these documents. Previously created graphs of information security documents will be the subgraphs of a newly created graph. For simplicity purposes, a restriction was defined that if requirements of different documents are linked, i.e. has edges between vertexes, then they define the same requirement and duplicate each other, although in reality requirements can be not entirely identical and could define a security requirement with a different level of detail. MSB identification requires removing duplicated requirements from the new graph by applying Vertex cover algorithms. After identification of MSB, it could be compared how controls implemented by the organization are aligned with it. The controls implemented by an organization can also be presented as a graph. This graph can be compared with previously identified MSB graph to verify matches between them.

Vertex cover algorithm and Graph isomorphism property was described in Chapter 1 of the thesis.

The methods presented below help to solve two different problems: MSB identification and MSB verification against controls implemented by the organization.The method is based on graph theory and graph optimisation algorithms (Vertex cover and Subgraph isomorphism).

3.2.1. Minimum Security Baseline Identification

For MSB identification, the use of Vertex cover algorithm is proposed. It is used for amending the created mapping graph, by removing from its specific vertexes. However, it needs to be ensured that only duplicated requirements are removed. Two options exist to achieve that:

- to apply minimum weighted vertex cover algorithms to ensure that the critical requirements having lower value are presented in a newly generated graph;
- to use the selected minimum vertex cover algorithm with additional rules to ensure that higher level security requirements are not overwritten by lower-level requirements, and requirements without direct connections with another document are not removed.

The second option was selected for implementation for simplicity reasons. The following rules were specified to ensure prioritisation of specific requirements:

- Restriction to remove requirements having a connection to parent vertex, but no links to other documents. To achieve that, additional null vertex to such vertex will be added.
- Additional evaluation of removed vertexes. It is important to ensure that vertexes without a direct connection to other security documents are not removed from the graph. Vertexes must be restored manually if they were removed.

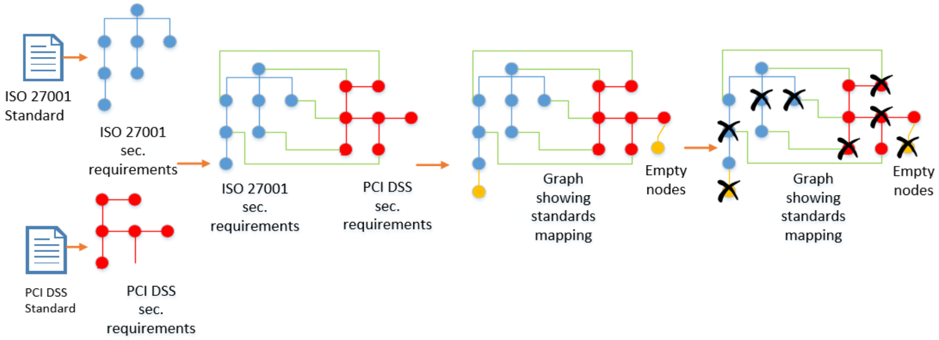


Fig. 3.9. Schematic Minimum security baseline identification method representation (Created by author)

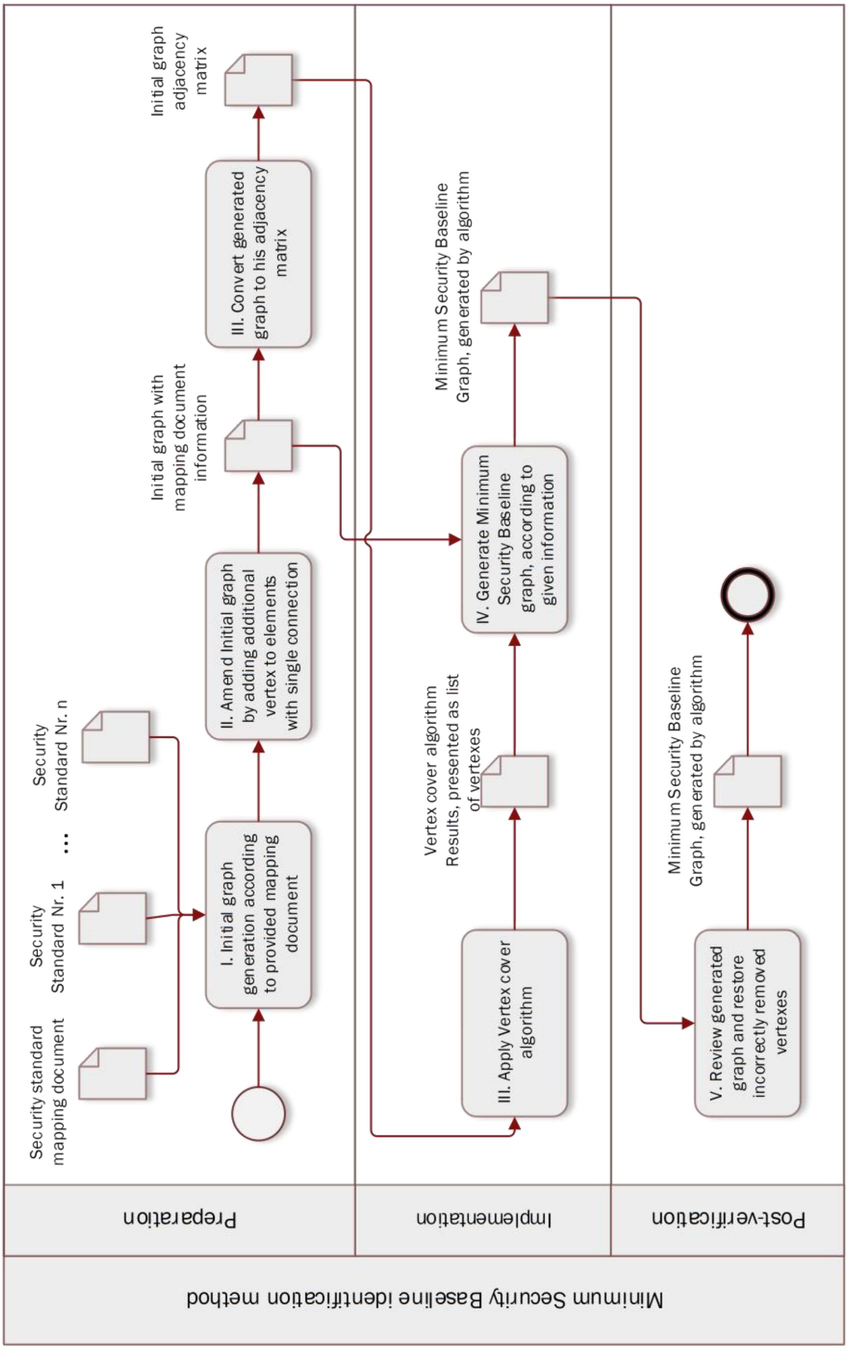

Minimum Security Baseline identification method
Preparation
Implementation
Post-verification
Security standard mapping document
Security Standard Nr. 1
…
Security Standard Nr. n
I. Initial graph generation according to provided mapping document
II. Amend Initial graph by adding additional vertex to elements with single connection
Initial graph with mapping document information
III. Convert generated graph to his adjacency matrix
Initial graph adjacency matrix
III. Apply Vertex cover algorithm
Vertex cover algorithm Results, presented as list of vertexes
IV. Generate Minimum Security Baseline graph, according to given information
Minimum Security Baseline Graph, generated by algorithm
V. Review generated graph and restore incorrectly removed vertexes
Minimum Security Baseline Graph, generated by algorithm

Fig. 3.10. Minimum security baseline identification method (Created by author)

The method is formed of 4 the main steps (schematic method representation is provided on Fig. 3.10):

- represent information security documents' requirements to be mapped as separate graphs;
- generate a new graph by linking requirements of N subgraphs (representing different information security documents);
- add the vertex to the vertexes with a single edge;
- apply the Minimum Vertex Cover algorithm.

Table 3.3. Minimum security baseline identification method action description (Created by author)

Action No.	Description
I	Documents' requirements are presented hierarchically. If vertexes have edges between them, this means that the requirements are identical. Differentiation by coverage level is out of scope for this method feasibility verification. For our purpose, link directions are not important.
II	Generated graph is reviewed, and temporary vertexes are added. Additional vertexes are added to the graph to ensure that the Minimum vertex cover algorithm does not remove existing vertexes, which do not have direct connections with other security documents.
III	The mapping graph is represented as an adjacency matrix for technical processing by a vertex cover algorithm.
IV	Vertex cover algorithm is applied. The result is presented in the form of rows. Since the assumption that duplicated vertexes are identical, and removal of any vertex would provide a suitable result, this leads to the situation when several similar solutions (several rows) can be generated.
V	Vertexes without a direct connection to other documents that were removed from the mapping graph are restored (the process is currently manual). Because of a different level of detail in various documents, the future approach could make use of additional criteria, which would allow removing vertexes, with a specified level of detail.

The proposed algorithm was also presented in pseudocode form (see Table 3.4). Below provided code explain all algorithms steps and actions:

Table 3.4. Minimum security baseline identification method algorithm (Created by author)

Algorithm

```
algorithm Minimum Security Baseline identification methodologies is
    input: Security documents set,
        Security documents mapping schema
    output: Minimum Security Baseline graph-based G(V, E)

for each Security documents in Security documents set do
        convert security requirement to the graph vertexes $G_i(\mathbf{V},E)$,
        convert relationships between requirements to the graph edges $G_i(V,\mathbf{E})$

if Security documents mapping schema wasn't used, then
    link graph $G_i(V,E)$ vertex to graph $G_{i+1}(V,E)$ vertex according to Security documents mapping schema
else Initial graph G(V,E) generation is finished

for each vertex in Initial graph do
    if Initial graph vertex $G_i(V,E)$ has one edge, then
        create new vertex and link new vertex with $G_i(V,E)$
    else check next vertex

convert Initial graph to the graph adjacency matrix

apply vertex cover algorithm to the graph adjacency matrix
    $C = \emptyset$
    $E' = G.E$

    while $E' \neq \emptyset$:
        let (u,v) be an arbitrary edge of $E'$
        $C = C \cup \{u, v\}$
        remove from $E'$ every edge incident on either u or v
    return C

for each value $V_{Ri}$ in vertex cover algorithm result set
    if $V_{Ri} \ni G(V, E)$ then
leave it in the G(V, E).
    else remove vertex and all its edges from G(V, E)

review Minimum Security Baseline graph G(V, E)
    if inconsistency spotted, then
        add missed vertexes and their edges

return G(V, E)
```

After Vertex cover algorithm is applied, it needs to be ensured that vertexes having no direct connection to other documents and thus removed from the graph are restored. The outcome of this process will be the MSB graph.

The formal MSB identification method described with the help of the Business Process Model, and Notation diagram is presented in Fig. 3.10.

In Table 3.3 a detailed description of actions defined in Fig. 3.10 is provided. The proposed method has 5 main steps, which cover 3 main phases: Preparation, Implementation and Post-verification.

3.2.2. Minimum Security Baseline Verification Against Deployed Controls

When the MSB graph is identified in the next step, graph vertexes (MSB requirements) verification against controls already deployed by the organization is performed. As stated earlier, subgraph isomorphism algorithms are used for that task. In our case, it is not significantly important which subgraph isomorphism algorithm will be used since our primary goal is to perform a feasibility study of such an approach and its practical applicability.

In this step, controls implemented by the organization are presented as a graph (further Deployed Control Graph or DCG), which is compared with the received MSB graph to verify alignment of requirements matches.

It is important to mention that the DCG graph may have stand-alone vertexes, i.e., not be connected with any other vertexes, which is usually caused by inconsistency while developing the information security management system (ISMS). Because of that, it is necessary to ensure that all controls (even stand-alone) are verified. It is achieved by introducing two additional conditions:

For simplicity reasons, while implementing a subgraph isomorphism algorithm, any other vertex verification properties (e.g. name matching or properties matching) will be used. Further verification could potentially make the approach more effective. However, it is not so important during this stage when just method feasibility is evaluated.

Due to the fact, that DCG graph could have stand-alone vertexes or small subgraphs separate parts of the DCG graph must be compared against the MSB graph.

The formal MSB verification against deployed controls method description with the help of the BPMN diagram is presented in Fig. 3.11.

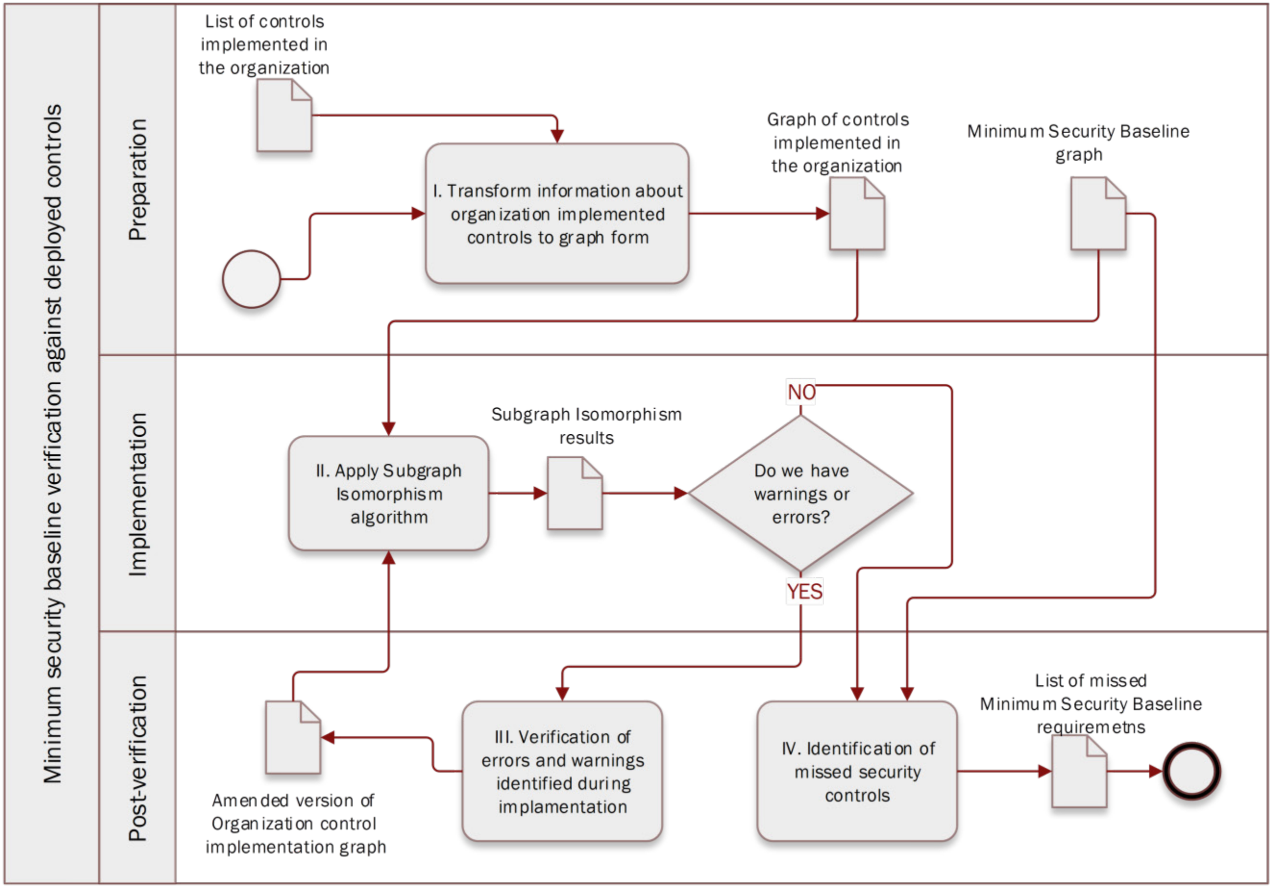

Minimum security baseline verification against deployed controls
Preparation
Implementation
Post-verification
List of controls implemented in the organization
I. Transform information about organization implemented controls to graph form
Graph of controls implemented in the organization
Minimum Security Baseline graph
II. Apply Subgraph Isomorphism algorithm
Subgraph Isomorphism results
Do we have warnings or errors?
NO
YES
III. Verification of errors and warnings identified during implamentation
Amended version of Organization control implementation graph
IV. Identification of missed security controls
List of missed Minimum Security Baseline requiremetns

Fig. 3.11. Method of Minimum security baseline verification against deployed controls (Created by author)

In Table 3.5. a detailed description of the Minimum Security baseline graph verification against deployed controls actions defined in Fig. 3.11. is provided.

Table 3.5. Description of Minimum Security baseline graph verification against deployed controls (Created by author)

Action No.	Description
I	This action includes two main activities: • Information gathering about controls deployed; • Presentation of information gathered in the form of a graph. Information gathering could be done manually or by automation tools that can process BPMN or EPC diagrams. The generated graph may have stand-alone vertexes, i.e. not be connected with any other vertexes, The process of identifying links between controls in the organization is complicated. It could be accelerated if it is known that the organization is compliant with one or another security document.
II	MSB and DCG graphs (or their representation form such as adjacency matrix or table) are imported to the graph processing tool, and the subgraph isomorphism algorithm is executed. If the DCG graph has stand-alone vertexes or small subgraphs, subgraph isomorphism algorithm is executed for each of them separately.
III	Since a stand-alone vertex is isomorphic to any vertex of MSB, additional verification based on a specified criterion (e.g. semantic similarity) should be used. Error verification can be done automatically, by applying additional verification criteria and re-executing subgraph isomorphism algorithm against subgraph or manually by a security specialist.
IV	Controls required by MSB but not present in DCG are identified.

The formal method of minimum security baseline verification against deployed controls described with the help of the Business Process Model, and Notation diagram is presented in Fig. 3.11

In Table 3.5, a detailed description of actions defined in Fig. 3.11 is provided. The proposed method has 4 main steps, which cover 3 main phases: Preparation, Implementation and Post-verification.

The proposed algorithm was also presented in pseudocode form in the Table 3.6.

Below provided code explain all algorithms steps and actions:

Table 3.6. Minimum Security baseline graph verification against deployed controls algorithm (Created by author)

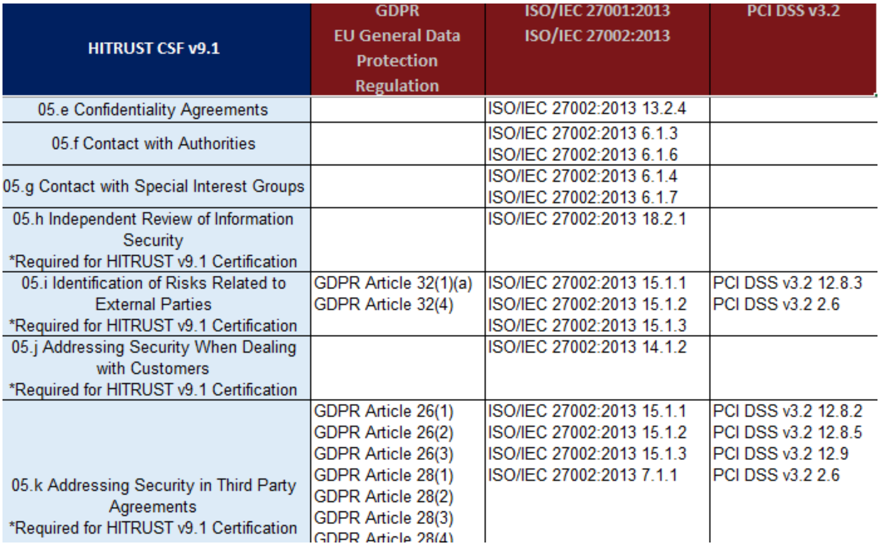
Algorithm

```
algorithm Verification method of compliance of organization controls is
    input: list of controls implemented by the organization,
          Minimum Security Baseline graph $G_{MSB}(V, E)$
    output: List of missed Minimum Security Baseline requirements L

transform controls implemented by the organization to the graph $G_{OC}(V,E)$

for each vertex and edges in  $G_{MSB}(V, E)$ and $G_{OC}(V,E)$ do
    procedure match(s)
        input: an intermediate state s; the initial state $s_0$ has $M(s_0) = Ø$
        output: the mapping between the two graphs

        if  M(s) covers all the nodes of $G_{MSB}(V, E)$ then
            output: M(s)
        else compute the set P(s) of the pairs candidate for inclusion in M(s)
            for each p in P(s) do
                if the feasibility rules succeed for the inclusion of p in M(s) then
                    compute the state s´ obtained by adding p to M(s)
                    call match(s)
              Restore data structures
    return match(s)

if warnings or errors > 0 then
    review warnings and errors;
    amend $G_{OC}(V, E)$;
    re-execute Subgraph isomorphism algorithm

for each vertex in match(s) do
       if match(s) $\ni$ $G_{MSB}(V, E)$ then
              remove vertex and all it edges from the $G_{MSB}(V, E)$.
    else leave vertex in the $G_{MSB}(V, E)$

rename $G_{MSB}(V, E)$ to List of missed Minimum Security Baseline requirements L
return L
```

The method concept was tested experimentally to prove its feasibility for real-life applications. The test results are presented and discussed in the “Method Experimental Testing Results and Discussion” section.

3.2.3. Experimental Method Verification Results

Three regulating documents were selected for mapping: ISO27002 (ISO/IEC 27002 2013), PCI DSS (PCI 2016) and a newly introduced GDPR (EU regulation 2016). Mapping (see Fig. 3.12) was based on the HITRUST CSF 9.1 framework (HITRUST 2018), which provides a table-based mapping of the majority of modern information security documents and other regulating documents.



HITRUST CSF v9.1	GDPR EU General Data Protection Regulation	ISO/IEC 27001:2013 ISO/IEC 27002:2013	PCI DSS v3.2
05.e Confidentiality Agreements		ISO/IEC 27002:2013 13.2.4	
05.f Contact with Authorities		ISO/IEC 27002:2013 6.1.3 ISO/IEC 27002:2013 6.1.6	
05.g Contact with Special Interest Groups		ISO/IEC 27002:2013 6.1.4 ISO/IEC 27002:2013 6.1.7	
05.h Independent Review of Information Security *Required for HITRUST v9.1 Certification		ISO/IEC 27002:2013 18.2.1	
05.i Identification of Risks Related to External Parties *Required for HITRUST v9.1 Certification	GDPR Article 32(1)(a) GDPR Article 32(4)	ISO/IEC 27002:2013 15.1.1 ISO/IEC 27002:2013 15.1.2 ISO/IEC 27002:2013 15.1.3	PCI DSS v3.2 12.8.3 PCI DSS v3.2 2.6
05.j Addressing Security When Dealing with Customers *Required for HITRUST v9.1 Certification		ISO/IEC 27002:2013 14.1.2	
05.k Addressing Security in Third Party Agreements *Required for HITRUST v9.1 Certification	GDPR Article 26(1) GDPR Article 26(2) GDPR Article 26(3) GDPR Article 28(1) GDPR Article 28(2) GDPR Article 28(3) GDPR Article 28(4)	ISO/IEC 27002:2013 15.1.1 ISO/IEC 27002:2013 15.1.2 ISO/IEC 27002:2013 15.1.3 ISO/IEC 27002:2013 7.1.1	PCI DSS v3.2 12.8.2 PCI DSS v3.2 12.8.5 PCI DSS v3.2 12.9 PCI DSS v3.2 2.6

Fig. 3.12. GDPR–ISO27002–PCI DSS mapping (partial view) (HITRUST 2018)

Each of the security documents (ISO27002, PCI DSS, GDPR) was presented as a graph (sample presented in Fig. 3.13). Cytoscape 3.6.1 application was used for graph visualization.

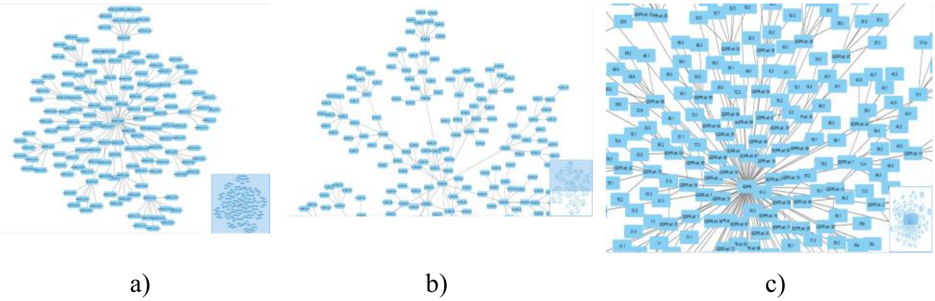


Fig. 3.13. Security document graph (partial view) generated with Cytoscape help (Created by author): a) ISO27002 standard, b) PCI DSS standard, c) GDPR regulation

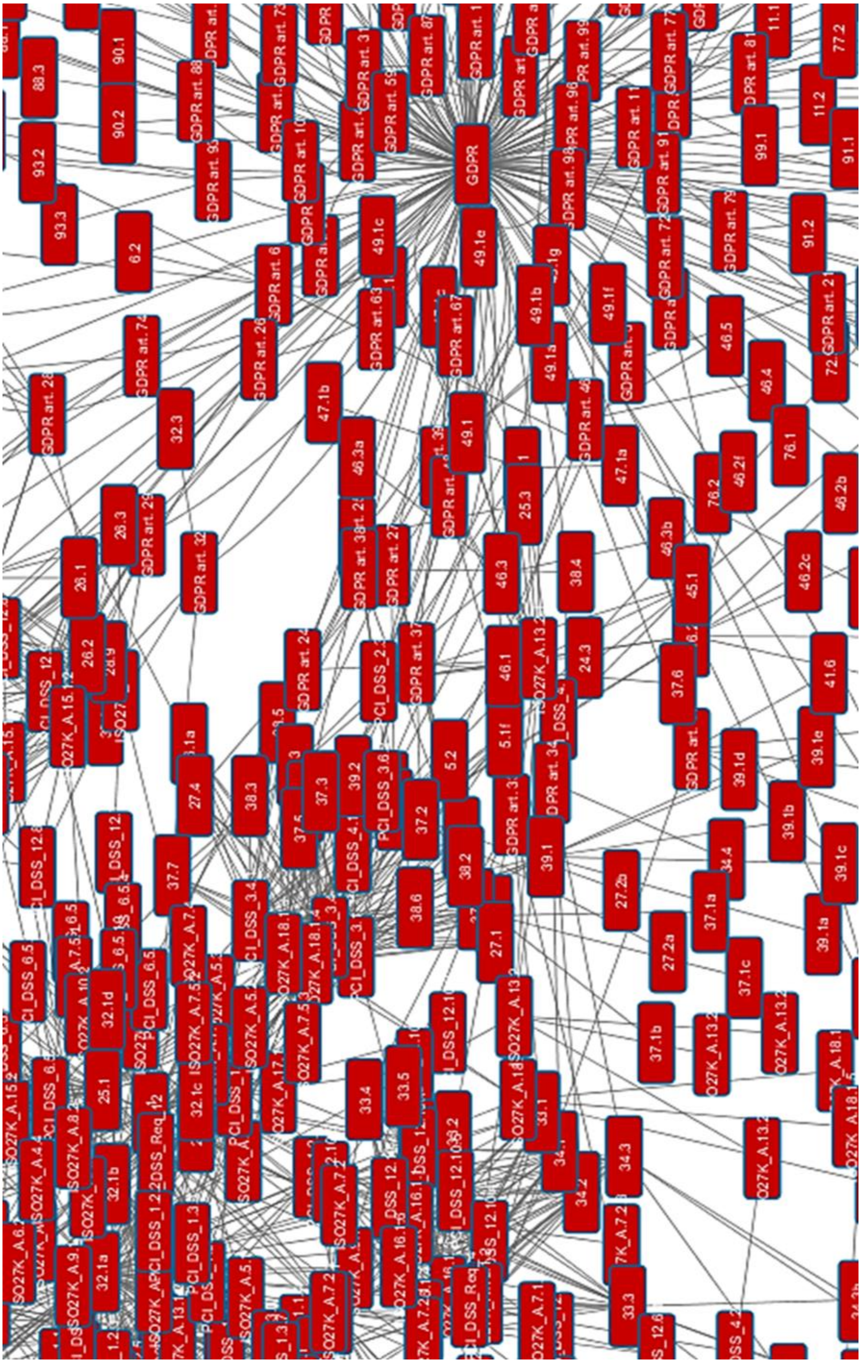
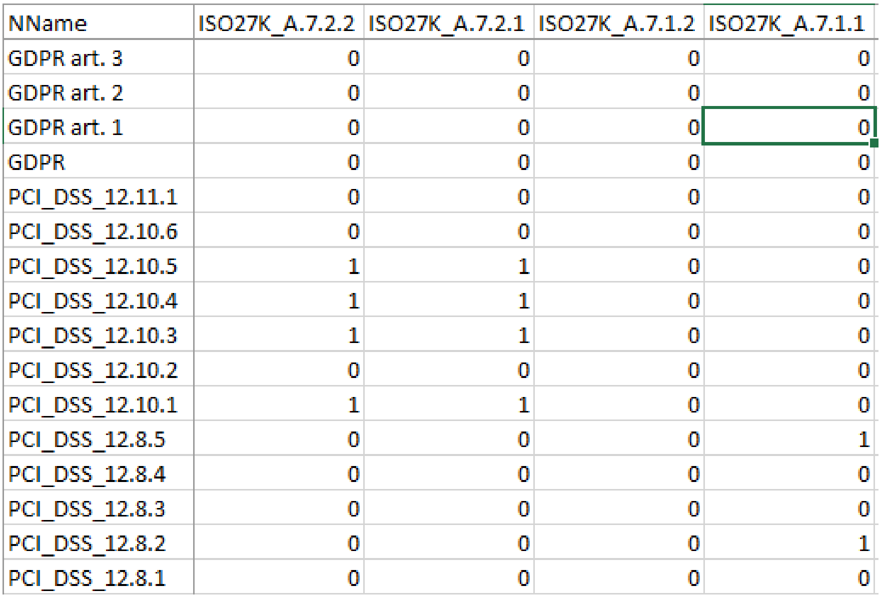


Fig. 3.14. ISO27002–PCI DSS–GDPR mapping graph (Partial view) generated with Cytoscape help (Created by author)

Later, mapping of separately generated graphs from HITRUST CSF 9.1 framework (HITRUST 2018) was performed, although other mapping methods, like the expert-based approach, could be applied. The resulting graph (Fig. 3.14) had 1267 vertexes (150 related to ISO27002 standard, 264 vertexes associated with PCI DSS standard and 853 to GDPR) and 2512 edges.

Null vertexes were added to ensure that vertexes that do not have direct connections with other documents are not removed. Addition of null vertexes has increased the size of the mapping graph by 463 vertexes.

The mapping graph was converted to the adjacency matrix by Cytoscape plug-in “AdjExporter”. The resulting matrix (Fig. 3.15) was saved in *.adj file.

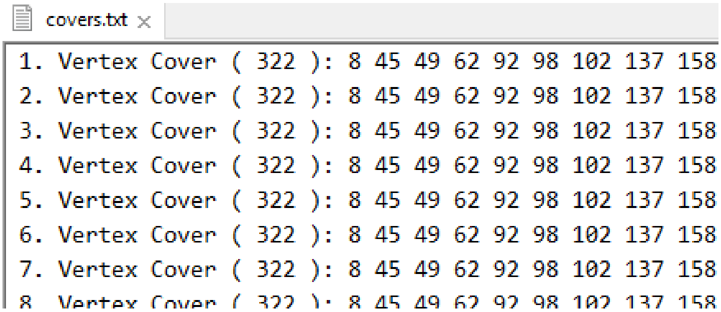


NName	ISO27K_A.7.2.2	ISO27K_A.7.2.1	ISO27K_A.7.1.2	ISO27K_A.7.1.1
GDPR art. 3	0	0	0	0
GDPR art. 2	0	0	0	0
GDPR art. 1	0	0	0	0
GDPR	0	0	0	0
PCI_DSS_12.11.1	0	0	0	0
PCI_DSS_12.10.6	0	0	0	0
PCI_DSS_12.10.5	1	1	0	0
PCI_DSS_12.10.4	1	1	0	0
PCI_DSS_12.10.3	1	1	0	0
PCI_DSS_12.10.2	0	0	0	0
PCI_DSS_12.10.1	1	1	0	0
PCI_DSS_12.8.5	0	0	0	1
PCI_DSS_12.8.4	0	0	0	0
PCI_DSS_12.8.3	0	0	0	0
PCI_DSS_12.8.2	0	0	0	1
PCI_DSS_12.8.1	0	0	0	0

Fig. 3.15. Matrix view of adjacency matrix for the mapping graph generated with TreeView help (Created by author.

Part A of Fig. 3.15 presents a small part of the generated adjacency matrix, and part B presents the whole matrix. Black dots on the screen provide information on graph components and connections between them. Part B view was created by an open source TreeView 3.0 Java application.

After the adjacency matrix is created, the vertex cover algorithm is applied. For our purpose, a C++ application developed by A. Dharwadker (Dharwadker 2011) and implementing his proposed vertex cover algorithm, was used. The application requires specifying the desired size k of the resulting vertex cover. In our case, k was defined as equal to 2 to find all possible vertex covers. The result of vertex cover search is provided in a *.txt file and includes information on the minimum amount of vertexes and provides the list of all vertexes involved in a found vertex cover (Fig. 3.16).



```
1. Vertex Cover ( 322 ): 8 45 49 62 92 98 102 137 158
2. Vertex Cover ( 322 ): 8 45 49 62 92 98 102 137 158
3. Vertex Cover ( 322 ): 8 45 49 62 92 98 102 137 158
4. Vertex Cover ( 322 ): 8 45 49 62 92 98 102 137 158
5. Vertex Cover ( 322 ): 8 45 49 62 92 98 102 137 158
6. Vertex Cover ( 322 ): 8 45 49 62 92 98 102 137 158
7. Vertex Cover ( 322 ): 8 45 49 62 92 98 102 137 158
8. Vertex Cover ( 322 ): 8 45 49 62 92 98 102 137 158
```

Fig. 3.16. List of potential vertex cover (Partial view) (Created by author)

Since all obtained vertex covers with the minimum number of vertexes are equivalent, any of them can be selected for further processing. Based on the chosen vertex cover, unnecessary vertexes are removed from the mapping graph with the help of Cytoscape application. As can be seen, the number of vertexes can be significantly reduced (from 1267 vertexes in the initial graph to 322 vertexes). The resulting MSB graph is presented in Fig. 3.17.

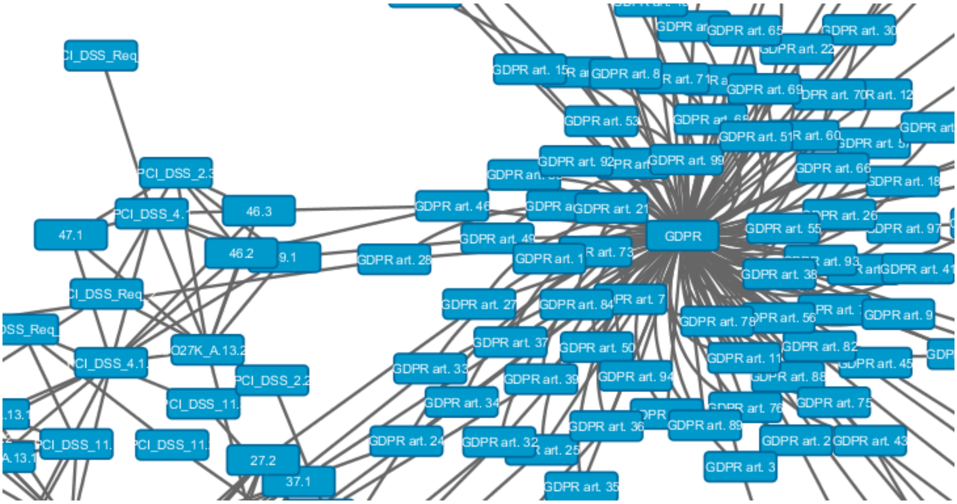


Fig. 3.17. Minimum security baseline graph generated with Cytoscape help (Created by author)

For MSB verification against controls already deployed by the organization, an abstract organization ACME Corporation – was taken. It was assumed that it has already implemented Logging and monitoring and Backup requirements. The DCG graph for ACME Corporation was created in Cytoscape tool (Fig. 3.18). Cytoscape tools are used by researchers for visualizing complex networks and integrating these networks with any type of attribute data (Franz, *et al.* 2016). This tool is widely used in biology (Truong, Tran and Kwon 2016) and bioinformatics (Larsen and Baumbach 2017) .

For identifying subgraph isomorphism between the received MSB graph and created DCG graph for ACME Corporation, Cytoscape plug-in “CyIsomorphism” was used. For isomorphism properties identification CyIsomoprhism plug-in is using VF++ algorithm (Juttneri and Madaras 2018).

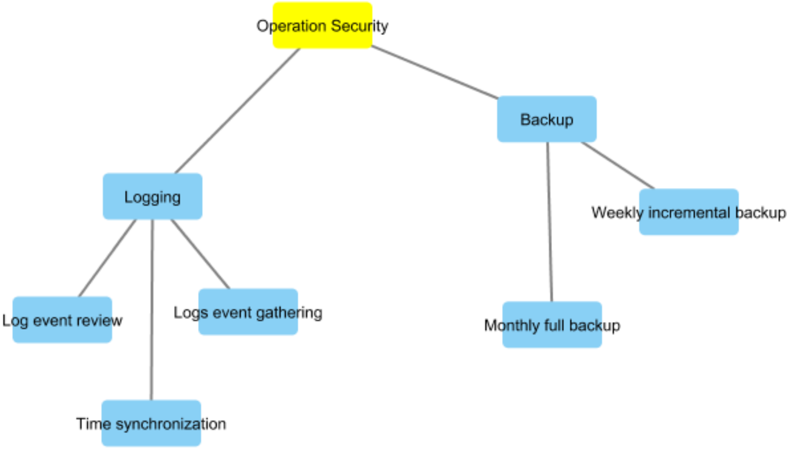
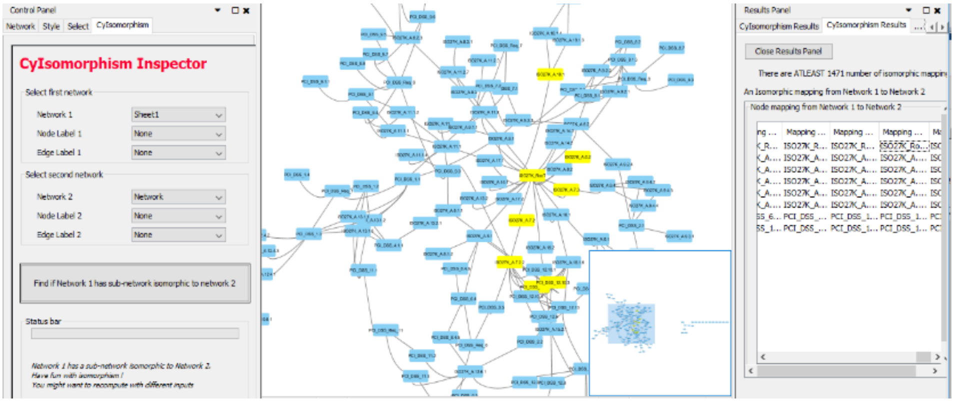


Fig. 3.18. Deployed controls graph for ACME Corporation generated with Cytoscape help (Created by author)

The DCG graph is evaluated against MSB graph to identify pattern similarity. Only information about vertexes and their connections was used in our experiment and because of that, Cytoscape was able to find more than one potential alignment. Use of the additional criteria would allow it to solve this issue. Cytoscape application has the possibility to work with weighted graphs; however for simplification purpose in our experiment, all vertexes have the same weight. In our case, the manual review of adjustments was performed. The final result of DCG verification against MSB is provided in Fig. 3.19.



CyIsomorphism Inspector

Select first network

Network 1: Sheet1
Node Label 1: None
Edge Label 1: None

Select second network

Network 2: Network
Node Label 2: None
Edge Label 2: None

Network 1 has a sub-network isomorphic to Network 2.
Have fun with isomorphism !
You might want to recompute with different inputs

There are ATLEAST 1471 number of isomorphic mappin

An Isomorphic mapping from Network 1 to Network 2

Node mapping from Network 1 to Network 2

ng …	Mapping …	Mapping …	Mapping …	Ma
K_R…	ISO27K_R…	ISO27K_R…	ISO27K_Ro…	ISC
K_A….	ISO27K_A…	ISO27K_A….	ISO27K_A….	ISC
K_A….	ISO27K_A…	ISO27K_A….	ISO27K_A….	ISC
K_A….	ISO27K_A…	ISO27K_A….	ISO27K_A….	ISC
K_A….	ISO27K_A…	ISO27K_A….	ISO27K_A….	ISC
K_A….	ISO27K_A…	ISO27K_A….	ISO27K_A….	ISC
SS_6…	PCI_DSS_…	PCI_DSS_1…	PCI_DSS_1…	PCI
SS_1…	PCI_DSS_…	PCI_DSS_1…	PCI_DSS_1…	PCI

Fig. 3.19. Identified isomorphic parts of Minimum security baseline and Deployed controls graph generated with CyIsomorphism help (Created by author)

The controls already deployed by ACME Corporation are shown on MSB in yellow colour. As can be seen, the presentation of MSB in the form of the graph provides a valuable tool for a security officer for evaluating the current state of ISMS.

3.3. Conclusions of Chapter 3

1. For harmonisation of a set of security documents, adaptive mapping has been chosen, which allows integrating new documents without the need to re-evaluate previous results. Validation of the proposed ontology has shown that it covers more than 90% of controls of used 4 standards.
2. For a harmonized set of security document analysis and their complexity management, several visualisation tools have been used. Chord diagram based approach has been chosen for graphical representation of the affinity of different documents. The graph-based approach is used to present detailed information about the percentage of matching level between different document requirements and relations. System Usability Scale verification reveal, that both appraoches (76.29 and 71.79) are usable.
3. The graph theory based method has been proposed for identifying the minimum set of mandatory security requirements out of the set of harmonized regulatory documents. The proposed methods have been experimentally validated with a set of harmonized security documents

and regulations (ISO 27001, PCI DSS and GDPR). The proposed method allows reducing the original graph (1276 vertexes) of harmonized security regulating documents by 74.76%. Such results are achieved by removing duplicated requirements.

4. The subgraph isomorphism based method has been proposed for comparing of organization’s implemented controls against Minimum Security Baseline. Experiment prove, that method is able to identify similar patterns, however in current state do not verify nodes weight.

General Conclusions

1. The analysis performed has revealed that existing methods for security documents requirements harmonization are not flexible and can be used only with a limited number of documents, while companies are facing the increasing pressure for the deployment of multiple regulatory documents. The following unsolved issues in the area were identified:
   1.1. Implementation of numerous security documents or other governing documents leads to a potential situation of deploying overlapping or contradictory controls, thus causing unnecessary expenditures on duplicated security controls and compliance issues.
   1.2. The existing security implementation costs calculation methods are not oriented to security controls implementation of multiple security documents, do not evaluate the complexity and maturity levels, have complicated calculations process, weak security aspects coverage and a complicated process of new data integration.
   1.3. Existing security document harmonization approaches require re-developing of the harmonized set and are time-consuming, except adaptive mapping methods. The attempts made to implement adaptive mapping and automate the process of information security documents

harmonization via existing ontologies was unsuccessful since used ontologies used were oriented to solve other tasks and didn't ensure quality link with the requirements of security documents.

2. The control-based security implementation costs evaluation method was proposed. The proposed approach is security controls oriented, i.e. controls can be directly linked with security regulating documents requirements. The method introduces the complexity and maturity levels into the calculation process. The proposed method was validated in several test scenarios. The performed experiments have shown that although the first calculation is time-consuming, every next calculation for a newly added document already reuses data from the previous calculation and thus takes much less time (up to 50%) and require smaller amount of new information (up to 32%) . To reduce the calculation time, the method improvement, based on automated data gathering from BPMN and EPC process diagrams, was proposed.
3. The COBIT v5 based ontology was proposed as a basis for adaptive harmonization of information security documents. Validation of the proposed ontology has shown that it covers more than 90% of controls of the set of 4 harmonized documents. For managing the complexity of harmonized regulating documents and their relations, several visualisation tools were used. System Usability Scale (76.29 and 71.79) reveal that both visualization are usable and representing needed information.
4. The graph theory based method for identifying the minimum set of mandatory security requirements out of the set of harmonized regulating documents was proposed. The method utilizes a representation of security documents, harmonized through ontology, in the form of graph. A vertex cover algorithm are used for removing duplicated requirements. The method also includes the possibility for comparing the obtained MSB graph against already deployed controls, by utilizing subgraph isomorphism property for similar structures identification. The proposed method verification has proved the applicability of this practical method for Minimum Security Baseline identification and allowed to reduce the number of vertices in the original graph by 74.76%.

References

Agrawal, V. 2017. A Comparative Study on Information Security Risk Analysis Methods. *Journal of computers, 12*(1), 57–67.

Ahanger, T., Abdullah A. 2018. Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms. *IEEE Access, 7,* 11020–11028.

Ahuja, S., Goldman, J. E. 2009. Integration of COBIT, Balanced Scorecard and SSE-CMM as a strategic Information Security Management (ISM) framework. *Proceeding of the CEUR Workshop on Business/IT alignment and Interoperability – BUSITAL'09,* 456.

Aldin, L., & S. de Cesare. 2009. A Comparative analysis of business process modelling techniques. *Proceeding of Oxford: UK Academy for Information Systems Conference – UKAIS'09,* 2.

ANSI. 2010. Guidelines for the construction, format, and management of monolingual controlled vocabularies. National Information Standards Organization, Baltimore MD, USA, 2010.

Appian. 2017. *About BPM – Business process definition.* Appian, Reston VA, USA, 2017.

Armstrong, C., Brown R., Chaves J., Czerniejewski A., Vecchio J., Perkins T., Rudnicki R., and Tauer G. 2015. Next Generation Data Harmonization. *Proceeding of SPIE, 9499*, 94990D, SPIE.

Arora, A., Hall, D., Pinto, C. A., Ramsey, D., & Telang, R. 2004. An ounce of prevention vs a pound of cure: How can we measure the value of IT security solutions? *Distributed* *by the Office of Scientific and Technical Information*, 1–10, U.S. Dept. of Energy, Washington DC, USA, 2004.

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

Aviad, A., Wecel, K., Abramowicz, W. 2015. The Semantic Approach to Cyber Security. Towards Ontology Based Body of Knowledge. 1*4th European Conference on Cyber Warfare and Security (ECCWS),* 328-336, Hatfield, England.

Avizienis, A., J. C. Laprie, B. Randell, & C. Landwehr. 2004. Basic concepts and taxonomy of dependable and secure computing. *Proceeding of Transactions on Dependable and Secure Computing, 1*(1), 11–33.

Balaban, A. T. 1985. Applications of Graph Theory in Chemistry. *Journal of Chemical Information and Moduling, 25*(3), 334–343.

Balaji, S., V. Swaminathan, & K. Kannan. 2010. Optimization of Unweighted Minimum Vertex Cover. *World Academy of Science, Engineering and Technology, International Journal of Mathematical and Computational Sciences, 4*(7), 941–946.

Bartens, T., S. de Haes, Y. Lamoen, F. Schulte, & S. Voss. 2015. On the Way to a Minimum Baseline in IT Governance: Using Expert Views for Selective Implementation of COBIT 5. *On the 48th Hawaii International Conference on System Sciences (HICSS)*, 4554–4563, Kauai HI, USA, 2015.

Brecht, M., & Nowey, T. 2013. A Closer Look at Information Security Costs. In *Proceeding of the Economics of Information Security and privacy,* 3–24, Springer.

Cai, S., K. Su, C. Luo, and A. Sattar. 2013. NuMVC: An efficient local search algorithm for minimum vertex cover. *Journal of Artificial Intelligence Research, 46*(1), 687–716.

Center for Information Security. 2018. *Cybersecurity Best practices.* CIS, East Greenbush, NY 12061, USA.

CERN Computer Security. 2018. *Mandatory Security Baseline definition.* CERN, Geneva, Switzerland.

Cheng, J., Y. Ke, W. Ng, and A. Lu. 2007. Fg-index: towards verification-free query processing on graph databases. *Proceeding of the 2007 ACM SIGMOD international conference on management of Data – SIGMOD'07,* 857–872, Bejing, China.

Chvatal, V. 1979. A Greedy Heuristic for the Set-Covering Problem. *Mathematics of Operations Research, 4*(3), 233–235.

Cooke, R. 1991. *Experts in uncertainty: opinion and subjective probability in science.* Oxford: Oxford University Press.

Cooke, R. 2008. TU Delft expert judgement data base, *Reliability Engineering & System Safety, 93*(5), 657–674.

Cibran, M. 2009. Translating BPMN Models into UML Activities. *Proceedings of Business Process Management Workshops, 17,* 236–247, Milan, Italy.

Clarkson, K. 1983. A modification to the greedy algorithm for vertex cover problem. *Information Processing Letters, 16*(1), 23–25.

Clemen, R. T., Winkler, R. L. 1999. Combining Probability Distributions from Experts in Risk Analysis. *Risk Analysis*, *19*(2), 187–200.

CMM. 1995. *Capability Maturity Model.* CMMI Institute, Pittsburgh, PA 15222, USA.

Conte D., Foggia, P., Sansone, C., & Vento, M. 2003. Graph matching applications in pattern recognition and image processing. *Proceedings 2003 International Conference on Image Processing (Cat. No. 03H37429),* 21–24.

Cordella, L. P., P. Foggia, C. Sansone, & Vento, M. 2004. A (sub)graph isomorphism algorithm for matching large graphs. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 26*(10), 1367–1372.

Correia, A., Gonçalves, A., Filomena T. 2017. A Model-Driven approach to Information Security. *Proceedings of 1st International Conference on Applied Mathematics and Computer Science (ICAMCS), 1836,* UNSP 020082-1, Rome, Italy.

COSO. 2004. *Enterprise Risk Management – Integrated Framework.* Committee of Sponsoring Organizations of the Treadway, New York, NY 10036, USA.

COSO. 2013. *Internal Control – Integrated Framework.* Committee of Sponsoring Organizations of the Treadway, New York, NY 10036, USA.

Daud, M., Rasiah, R., George M., Asirvatham, D., Thangiah, G. 2018. Bridging the gap between organisational practices and cyber security compliance: can cooperation promote compliance in organisations?. *International Journal of Business and Society, 19*(1), 161–180.

de Bruijn, W., Spruit, M. R., & den Heuvel, M. 2010. Identifying the Cost of Security. *Journal of Information Assurance and Security, 5,* 74–83.

de Haes, S., & van Grembergen, W. 2008. An Exploratory Study into the Design of an IT Governance Minimum Baseline through Delphi Research. *Communications of the Association for Information Systems, 22*(1), 443–459.

Delbot, F., & Laforest, C. 2008. A better list heuristic for vertex covers. *Information Processing Letters, 107*(3–4), 125–127.

Denker, G., L. Kagalb, & Finin, T. 2005. Security in the Semantic Web using OWL. *Information Security Technical Report, 10*(1), 51–58.

Dharwadker, A. 2011. The Vertex Cover Algorithm. *CreateSpace Independent Publishing Platform,* ISBN-13:978-1466384477, 1–44.

Dhillon, G., & Backhouse, J. 2000. Information system security management in the new millennium. *Communications of the ACM, 43*(7), 125–128.

Ding, L., B. Gu, X. Hong, & Dixon, B. 2009. Articulation node based routing in delay tolerant networks. *2009 IEEE International Conference on Pervasive Computing and Communications,* 700–705, Galveston TX, USA.

Dobson, G., Sawyer, P. 2006. Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web. In *Dependable requirements Engineering of Computerised Systems at NPPs,* 1-12.

Donner, M. 2003. Toward a Security Ontology. In *IEEE Security and Privacy, 1*(3), 6–7.

Dudas, P. M., de Jongh, M., Brusilovsky, P. 2013. A semi-supervised approach to visualizing and manipulating overlapping communities. In *17th International Conference on Information Visualization,* 180–185.

E-Government Act. 2002. *Federal Information Security Management Act.* United States of America Government, Washington DC, USA.

E-Government Act. 2014. *Federal Information Security Modernization Act.* United States of America Government, Washington DC, USA.

Elmsallati, A., C. Clark, & Kalita, J. 2007. Global Alignment of Protein-Protein Interaction Networks: A Survey. in *IEEE/ACM Transaction on Computational Biology and Bioinformatics, 13*(4), 689–705.

Eshtay, M., A. Sliet, & Shariah, A. 2016. NMVSA Greedy Solution for Vertex Cover Problem. In *International Journal of Advanced Computer Science and Applications, 7*(3), 60–64.

EU regulation. 2016. General Data Protection Regulation. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,* Brussel, Belgium.

Federal Office for Information Security. 2005. *IT-Grundschutz*. Bundesamt fur Sicherheit in der Informationstechnik, Bonn, Germany.

Fenz, S. 2010. Ontology-based Generation of IT-Security Metrics. In *Proceedings of the 2010 ACM Symposium on Applied Computing – SAC'10,* 1833–1839.

Fenz, S., Ekelhart, A. 2009. Formalizing information security knowledge. In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security,* 183–194.

Fenz, S., Neubauer, T. 2018. Ontology-based information security compliance determination and control selection on the example of ISO 27002. *Information & Computer Security*, *26*(5), 551–567.

Fenz, S., Plieschnegger, S., Hobel, H. 2019. Mapping information security standard ISO 27002 to an ontological structure. *Information & Computer Security, 24*(5), 452–473.

Fernandez-Breis, J., & Martinez-Bejar, R. 2002. A cooperative framework for integrating ontologies. *International Journal of Human-Computer Studies, 56*(6), 665–720.

Franz, M. , Lopes, C., Gerardo, H., Dong, Y., Sumer. O, Bader, G. 2016. Cytoscape.js: a graph theory library for visualisation and analysis. *Bioinformatics, 32*(2), 309–311.

Fung, D. C. Y., Hong, S. H., Koschutzki, D., Schreiber, F., & Xu, K. 2008. 2.5D visualization of overlapping biological networks. In *Journal of Integrative Bioinformatics*, *5*(1), 1–17.

Gaynor, M., Bass, C., Duepner, B. 2015. A tale of two standards: strengthening HIPAA security regulations using the PCI-DSS. *Health Systems, 4*(2), 111–123.

Gajurel, S., & Bielefeld, R. 2012. A Simple NOVCA: Near-Optimal Vertex Cover Algorithm. In *Procedia Computer Science, 9,* 747–753.

Gartner. 2011. *IT Budget: Information Security & Risk Management Spend Metrics.* Gartner Inc., Stamford, CT 06902, USA.

Gaspar, M., Popescu, S. 2018. Integration of the GDPR requirements into the requirements of the SR EN ISO/IEC 27001:2018 standard, integration security management system in a software development company. *Applied Mathematics, Mechanics, and Engineering, 61*(3), 85–96.

Geambasu, C. 2012. BPMN vs. UML Activity Diagram for Business Process Modeling. *Proceedings of the 7th International Conference Accounting and Management Information Systems, AMIS 2012*, 934–945, Bucharest, Romania.

Geneiatakis, D., & Lambrinoudakis, C. 2007. An ontology description for SIP security flaw. In *Computer Communications, 30*(6), 1367–1374.

Giorgini, P., Manson, G., & Mouratidis, H. 2004. Towards the Development of Secure Information Systems: Security Reference Diagrams and Security Attack Scenarios. In *Proceeding of the FORUM at 16th International Conference On Advanced Information Systems Engineering,* 1–10.

Gomez-Perez, A., Fernandez-Lopez, M., & Corcho, O. 2004. Ontological Engineering: With Examples from the Areas of Knowledge Management, E-Commerce and the Semantic Web. *Advanced Information and Knowledge Processing,* Springer-Verlag, ISBN: 1846283965, Berlin.

Griss, M. 2001. CBSE Success Factors: Integrating Architecture, Process and Organization. In *Component-based Software Engineering*, Addison-Wesley, ISBN: 0-201-70485-4, 143–160.

Gruber, T. 1995. Towards Principles for the Design of Ontologies Used for Knowledge Sharing. In *International Journal of Human-Computer Studies, 43*(5–6), 907–928.

Gruninger, M., & Lee, J. 2002. Ontology Applications and Design. *Communications of the ACM, 45*(2), 39–41.

Guan, Hui , Hongji Yang, and Jun Wang. 2016. An Ontology-based Approach to Security Pattern Selection. *International Journal of Automation and Computing*, *13*(2), 168–182.

Han, Z., Yali, L. 2015. Research on the Data Mining Method based on Information Security. *Proceeding of 3rd International Conference on Machinery, Materials and Information Technology Applications, 35,* 251–256, Bejing, China.

Haufe, K., Colomo-Palacios, R., Dzombeta ,S., Brandis, K., Stantchev, V. 2016. ISMS core processes: A study. *Conference on ENTERprise Information Systems, 100,* 339–346, Porto, Portugal.

Haufea, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., Stantchev, V. 2016. Security Management Standards: A Mapping. *Conference on ENTERprise Information Systems, 100, 755*–761, Porto, Portugal.

Herzog, A., Shahmehri, N., & Duma, C. 2007. An Ontology of Information Security. *International Journal of Information Security and Privacy, 1*(4), 1–23.

HIPAA. 2002. Health Insurance Portability and Accountability Act. *United States of America mandatory regulatory requirements for Health Insurance sector*, Washington DC, USA.

HIPAA. 2013. Health Insurance Portability and Accountability Act. *United States of America mandatory regulatory requirements for Health Insurance sector*, Washington DC, USA.

HITRUST. 2018. *HITRUST Cyber Security framework v9.1.* HITRUST, Frisco, TX 75034, USA.

Hofherr, M. 2011. *Mapping ISO27001 <> PCI DSS 2.0.* [online]. [cited 12 April 2015]. available from Internet *<http://www.forinsect.com/downloads/Mapping-ISO27001-PCI_public.pdf>*.

Holik, F., Horalek, J., Neradova, S., Zitta, S., Novak, M. 2015. Methods of deploying security standards in a business environment. In *Proceeding of 25th International Conference Radioelektronika,* 411–414, Pardubice, Czech Republic.

Hora, S. C. 2009. Expert Judgment in Risk Analysis. *Non-published Research Reports,* 120, 1–11.

Horvath, S., Langfelder, P. 2009. WGCNA: an R package for weighted correlation network analysis. In *BMC Bioinformatics, 9*(559), 559.

Humpert-Vrielink, F., Vrielink, N. 2012. A modern Approach on Information Security Measurement. In *ISSE 2012 Securing Electronic Business Processes,* 48-53, Springer.

Information Systems Security Association. 2011. *New standard for SMEs from ISSA UK.* Information Systems Security Association. Vienna, VA, USA.

Yolles, M. 1999. Management Systems: A Viable systems approach. *Financial Times Management,* ISBN-13: 978-0273620181.

ISACA. 2013. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.* ISACA, Schaumburg, IL 60173, USA.

ISACA. 2019. *COBIT 2019 Framework.* ISACA, Schaumburg, IL 60173, USA.

ISO 27000:2014. Information technology – Security techniques – Information security management systems – Overview and vocabulary. International Organization for Standardization, Geneva, Switzerland.

ISO/IEC:27002. 2013. *Code of practice for information security controls.* International organization for Standardization, Geneva, Switzerland.

ISO/IEC:27001. 2013. *Information technology – Security techniques – Information security management systems – Requirements.* International organization for Standardization, Geneva, Switzerland.

ISO/IEC:27001. 2017. *Information technology – Security techniques – Information security management systems – Requirements.* International organization for Standardization, Geneva, Switzerland.

IT Governance Institute. 2008. *Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit.,* ISACA, Schaumburg, IL 60173, USA.

Ivkic, I., Mauthe, A., Tauber, M. 2019. Towards a Security Cost Model for Cyber-Physical Systems. *In Proceeding of 16th IEEE Annual Consumer Communications & Networking Conference (CCNC),* 1–7, Las Vegas NV, USA.

Jacobson, I., Griss, M., & Jonsson P. 1997. Software Reuse: Architecture, Process and Organization for Business Success. *Addison-Wesley-Longman,* ISBN-13: 978–0201924763.

Johansson, L. O., Warja, M., & Carlsson, S. 2012. An evaluation of business process model techniques, using Moody's quality criterion for a good diagram. In *Proceedings of the 11th International Conference on perspectives in business informatics research – BIR'2012, 963*, 56–64.

Johna, A., Wilscy, M. 2015. Vertex Cover Algorithm Based Multi-Document Summarization. In *Proceeding of International Conference on Information and Communication Technologies, 46,* 285–291, Kochi, India.

Juttneri, A., Madaras, P. 2018. VF2++ An Improved Subgraph Isomorphism Algorithm. In *Proceeding of 29th Annual Conference of the European-Chapter-on-Combinatorial-Optimization (ECCO), 242*, 69–81, Dudapest, Hungary.

Karabacak, B., Sogukpinar, I. 2005. ISRAM: Information security risk analysis method. *Computers & Security, 24*(2), 147–159.

Karande, H. 2015. An Ontological Approach to Information. In *Proceeding of International Journal of Innovative Research in Computer, 3*(9), 8087–8092.

Karyda, M., Balopoulos, T., Gymnopoulos, L., Kokolakis, S., Lambrinoudakis, C., Gritzalis S., Dritsas, S. 2006. An ontology for secure e-government applications. *Proceedings of the First International Conference on Availability, Reliability and Security ARES'06,* 1037–1042.

Karp, R. 1972. Reducibility among combinatorial problems. *Complexity of Computer Computations,* 88–103.

Khan, A., Li, N., Yan, X., Guan, Z., Chakraborty, S., & Tao, S. 2011. Neighbourhood-based fast graph search in large networks. *Proceedings of the 2011 ACM SIGMOD International Conference on Management of data - SIGMOD'11,* 901–912.

Khan, I., & Khan, H. 2014. Experimental Comparison of Five Approximation Algorithms for Minimum Vertex Cover. *International Journal of u- and e-Service, Science and Technology, 7*(6), 69–84.

Khan, I., & Khan, H. 2013. Modified Vertex Support Algorithm: A New approach for the approximation of Minimum vertex cover. *Research Journal of Computer and Information Technology Science, 1*(6), 7–11.

Khan, I., Ahmad, I., & Khan, M. 2014. AVSA, Modified Vertex Support Algorithm for Approximation of MVC. *International Journal of Advanced Science and Technology, 64,* 71–78.

Kim, A., Lou, J., & Kang, M. H. 2005. Security Ontology for Annotating Resources. *On the Move to Meaningful Internet Systems, vol. 3761,* 1482–1499.

Kim, B., Won S. 2016. Analytical Study of Cognitive Layered Approach for Understanding Security Requirements using Problem Domain Ontology. In *Proceeding of 23rd Asia-Pacific Software Engineering Conference, APSEC 2016,* 97-104, Hamilton, New Zealand.

Kissel, R. 2013. *NISTIR 7298 revision 2. Glossary of key information security terms.* National Institute of Standards and Technology, Gaithersburg.

Kuo, M. H. 2007. An intelligent agent-based collaborative information security framework. *Expert systems with applications, 32*(2), 585–598.

Landwehr, C. E., Bull, A. R., McDermott, J. P., & Choi, W. S. 1994. A taxonomy of computer program security flaws. *Computing Surveys, 26*(3), 211–254.

Langer, S. 2017. Cyber-Security Issues in Healthcare Information Technology. In *Journal of Digital Imaging, 30*(1)*,* 117–125.

Larsen, S., Baumbach, J. 2017. CytoMCS: A Multiple Maximum Common Subgraph Detection Tool for Cytoscape.In *Journal of Integrative Bioinformatics, 14*(2), Special issue.

Lee, C., Geng, X. Raghunathan, S. 2012. Mandatory Standards and Organizational Information Security. In *Information Systems Research, 27*(1), 70–86.

Lee, J., Kasperovics, R., & Han, W. 2012. An In-depth Comparison of Subgraph Isomorphism Algorithms in Graph Databases. *Proceedings of the VLDB Endowment,6*(2), 133–144.

Li, M., & Tang, M. 2013. Information Security Engineering: a Framework for Research and Practices. *International journal of computers communications & control, 8*(4), 578–587.

Lozano-Tello, A, & Gomez-Perez, A. 2004. ONTOMETRIC: A method to choose the appropriate ontology. *Journal of database management, 15*(2), 1–18.

Lubich, H. P. 2006. IT-Sicherheit: Systematik, Aktuelle Probleme und Kosten-Nutzen-Betrachtung. *HMD. Wirtschaftsinformatik, 248,* 6–15.

Maines, C., Llewellyn-Jones, D., Tang, S., Zhou, B. 2015. A cyber security ontology for BPMN-security extensions. In *Proceeding of 2015 IEEE International Conference on Computer And Information Technology - Ubiquitous Computing and Communications - Dependable, Autonomic and Secure Computing - Pervasive Intelligence and Computing,* 1757–1765, Liverpool, United Kingdom.

Massacci, F., Mylopoulos, J., Paci, F., Tun, T. T., & Yu, Y. 2011. An Extended Ontology for Security Requirements. *In CAiSE 2011: Advanced Information Systems Engineering Workshops, vol. 83,* 622–636.

Mercuri, R. T. 2003. Analyzing Security Costs. *Communications of the ACM - E-services: a cornucopia of digital offering ushers in the Net-based evolution, 46*(6), 15–18.

Mylopoulos, J., Borgida, A., Jarke, M., & Koubarakis, M. 1990. Telos: Representing Knowledge About Information Systems. In *ACM Transactions on Information Systems (TOIS), 8*(4), 325–362.

Mishra, A., Agarwal, M., Asati, A., Raju, K. 2017. Using graph isomorphism for mapping of data flow applications on reconfigurable computing systems. In *Microprocessors and Microsystems, 51*, 343–355.

Mohaghegh, N., Janbozorgi, M., Mirzaeian, M., Malekolkalami, M., Hojatizade, Y. 2018. The status of information security management performance in libraries of state medical sciences universities in Tehran based on ISO/IEC 27002 standards. In *Indo American Journal of Pharmaceutical Science, 5*(8), 7540–7545.

Mongiovi, M., Natale, R. D., Giugno, R., Pulvirenti, A., Ferro, A., & Sharan, R. 2010. Sigma: a set-cover-based inexact graph matching algorithm. *Journal of Bioinformatics and Computational Biology, 8*(2), 199–218.

Mouratidis, H., & Giorgini, P. 2006. Integrating Security and Software Engineering: Advances and Future Visions. *IGI Global,* ISBN-13: 9781599041476.

Mouratidis, H., Giorgini, P., & Manson, G. 2003. An Ontology for Modelling Security: The Tropos Approach. *In Knowledge-Based Intelligent Information and Engineering Systems. KES 2003. Lecture Notes in Artificial Intelligence, vol 2773,*1387–1394.

Nirmala, P., Lekshmi, R., Nadarajan, R. 2016. Vertex cover-based binary tree algorithm to detect all maximum common induced subgraphs in large communication networks. In *Knowledge and Information Systems, 48*(1), 229–252.

NIST SP 800-30. 2012. *Guide for Conducting Risk Assessments - NIST SP 800-30 Rev. 1.* National Institute of Standards and Technology, Gaithersburd, MD 20899, USA.

NISTIR 7621. 2016. *Small Business Information Security - NISTIR 7621 Rev. 1.*, National Institute of Standards and Technology, Gaithersburd, MD 20899, USA

Oliveto, P.S., Yao, X., & He, J. 2008. Analysis of Population-based Evolutionary Algorithms for the Vertex Cover Problem. In *2008 IEEE Congress on Evolutionary Computation (IEEE World Congress on Computational Intelligence)*, 1563–1570.

Pardo, C., Pino, F. J., Garcia, F., Piattini, M., Baldassarre, M. T. 2012. An ontology for the harmonization of multiple standards and models. *Computer Standards & Interfaces, 34*(1), 48–59.

Pardo, C., Pino, F. J., Garcia, F., Piattini, M. 2012. Identifying methods and techniques for the harmonization of multiple process reference models. In *Dyna-Colombia, 79*(172), 85–93.

Patel, K., Patel, J. 2017. Computational Analysis of different Vertex Cover Algorithms of Various Graphs. In *International Conference on Intelligent Computing and Control Systems (ICICCS),* 730–734, Madurai, India..

PCI. 2016. *Payment Card Industry Data Security Standard.* Payment Card Industry, Wakefield, MA 01880, USA.

PricewaterhouseCoopers. 2015. *Information Security Breaches survey.* PricewaterhouseCoopers, London, UK.

Pushpam, L., Suseendran, C. 2018. v. In *Discrete Mathematics Algorithms and Applications, 10*(6), 1850075.

Pushpam, L., Suseendran, C. 2017. Secure vertex cover of a graph. In *Discrete Mathematics Algorithms and Applications, 9*(2), 1750026.

Raymond, J. W., & Willett, P. 2002. Maximum Common Subgraph Isomorphism Algorithms for the Matching of Chemical Structures. *Journal of Computer-Aided Molecular Design, 16*(7), 521–533.

Rajbhandari, L., & Snekkenes, E. 2013. Using the conflicting incentives risk analysis method. *Security and Privacy Protection in Information Processing – SEC'2013, vol. 405,* 315–329.

Rodriguez, A., Fernandez-Medina, E., Trujillo, J., Piattini, M. 2011. Secure business process model specification through a UML 2.0 activity diagram profile. In *Decision Support Systems, 51*(3), 446–465.

Rong, H., Ma, T., Tang, M., Cao, J. 2018. A novel subgraph K+-isomorphism method in social network based on graph similarity detection.In *Soft Computing, 22*(8), 2583–2601.

Sanfeliua, A., Alquézarb, R., Andradea, J., Climentc, J., Serratosad, F., & Vergésa, J. 2002. Graph-based representations and techniques for image processing and image analysis. In *Pattern Recognition, 35*(3), 639–650.

Schilling, A., Doerner, K., Ljubic, I., Pflug, G., Tragler, G. 2017. Robust Optimization of IT Security Safeguards Using Standard Security Data. In *Operations Research Proceedings,* 333-339, Vienna, Austria.

Shang, H., Zhang, Y., Lin, X., & Yu, J. X. 2008. Taming verification hardness: an efficient algorithm for testing subgraph isomorphism. In *Proceedings of the VLDB Endowment, 1*(1), 364–375.

Shasha, D., Wang, J. T. L., & Giugno, R. 2002. Algorithmics and applications of tree and graph searching. In *Proceedings of the twenty-first ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems – PODS'02,* 39–52.

Shojaie, B. 2018. Implementation of Information Security Management Systems based on the ISO/IEC 27001 Standard in different cultures, *Department of Informatics of universitet Hamburg,* 1–147.

Symantec. 2016. *Internet Security Threat Report.* Symantec, Mountain View, CA 94043, USA

Sirisom, P., Payakpate, J., Wongthai, W. 2017. A System Design for the Measurement and Evaluation of the Communications Security Domain in ISO 27001:2013 Using an Ontology. In *Information Science and Applications 2017 (ICISA 2017), 424,* 257–265 .

Siviy, J., Kirwan, P., Marino, L. & Morley, J. 2008. The value of harmonization multiple improvement technologies: A process improvement professional's view. *Published by Software Engineering Institute and Carnegie Mellon Institute.* 1-15, Pittsburg, PA 15213, USA.

Solic, K., Ocevcic, H. Golub, M. 2015. The information systems' security level assessment model based on an ontology and evidential reasoning approach. In *Computers and Security, 55,* 100–112.

Souag, A. 2012. Towards a new generation of security. In *Proceedings of 24th International Conference on Advanced Information Systems Engineering – CAiSE'12, vol. 863,* 1–8.

Souag, A., Salinesi, C., Comyn-Wattiau, I. 2012. Ontologies for security requirements: A literature survey and classification. In *Advanced Information Systems Engineering Workshops Lecture Notes in Business Information Processing, vol. 112,* 61–69.

Souag, A., Salinesi, C., Isabelle, R. 2015. A Security Ontology for Security Requirements Eliction. Proceedings *of Engineering Secure Software and Systems (Essos 2015), 8978*, 157–175.

SOX. 2002. *Sarbanes-Oxley Act.* United States of America law oriented to the financial sector, Washington DC, USA.

Srinivas, J., Das, A., Kumar, N. 2019. Government regulations in cyber security: Framework, standards and recommendations.In *Future Generation Computer Systems, 92*, 178-188.

Stolen, K., den Braber, F., Dimitrakos, T., Fredriksen, R., Gran, B. A., & Houmb, S.-H. 2002. Model-based risk assessment – the coras approach. In *Proceedings of iTrust Workshop.*

Sugiura, M., Suwa, H., Ohta, T. 2015. Improving IT Security Through Security Measures: Using Our Game-Theory-Based Model of IT Security Implementation. In *Proceeeding of 17th International Conference on Human-Computer Interaction (HCI International), 9169*, 82-96.

Suh, B., Han, I. 2003. The IS risk analysis based on a business model. *Information & Management, 41*(2), 149–158.

Telea, A., & Ersoy, O. 2010. Image-based edge bundles: Simplified visualization of large graphs. In *EuroVis'10 Proceedings of the 12th Eurographics / IEEE - VGTC conference on Visualization,* 29(3), 843–852.

Truong, C., Tran, T., Kwon, Y. 2016. MORO: a Cytoscape app for relationship analysis between modularity and robustness in large-scale biological networks. In *BMC Systems Biology, 10*(4), 122.

Tsalis, N., Theoharidou, M., & Gritzalis, D. 2013. Return on Security Investment for Cloud Platforms. In *2013 IEEE 5th International Conference on Cloud Computing Technology and Science,* 132–137.

Tsoumas, B., & Gritzalis, D. 2006. Towards an Ontology-based Security Management. In *20th International Conference on Advanced Information Networking and Applications - Volume 1 (AINA'06),* 985–992.

Tversky, A., & Simonson, I. 1993. Context-dependent preferences. *Management Science*, *39*(10), 1179–1189.

Ullmann, J. R. 1976. An algorithm for subgraph isomorphism. In *Journal of the ACM (JACM), 23*(1), 31–42.

Undercoffer, J., Joshi, A., & Pinkston, J. 2003. Modelling Computer Attacks: An Ontology for Intrusion Detection. In I*nternational Workshop on Recent Advances in Intrusion Detection*, *vol.2820,* 113–135.

Ungureanu, S. 2015. Implementing cost calculation using ABC method. In *Proceeding of 21st International Conference the Knowledge-Based Organization, 21*(2), 360–365.

United States Federal Government. 2004. *Federal Information Processing Standard Publication 199.* United States of America standard, Washington DC, USA.

United States Federal Government. 2006. *Federal Information Processing Standard Publication 200.* United States of America standard, Washington DC, USA.

University of Maryland. 2009. *Hypermedia-based Featherweight OWL Ontology Editor.* University of Maryland, College Park, MD 20742, USA.

Veloudis, S., Paraskakis, I., Petsos, C., Verginadis, Y., Patiniotakis, I., Gouva, P., Mentzas, G. 2019. Achieving security-by-design through ontology-driven attribute-based access control in cloud environments. In *Future Generation Computer Systems-The International Journal of Escience, 93*, 373–391.

Venkata, R., Kamongi, P., Kavi, K. 2018. An Ontology-Driven Framework for Security and Resiliency. In P*roceeding of 13th International Conference on Software Engineering Advances (ICSEA 2018)*, 13-19, Nice, France.

Wang, P., Chao, K., Lo, C., Wang, Y. 2017. Using ontologies to perform threat analysis and develop defensive strategies for mobile security. In *Information Technology Management Journal, 18*, 1–25.

Wang, Z., Wang, S., Wang, L. 2016. Research on the information security audit base on semantic web ontology and improve vector space model. In *International Journal of Security and Applications, 10*(12), 141–152.

Wangwe, C. K., Eloff, M. M., & Venter, L. 2012. A sustainable information security framework for e-government - the case of Tanzania. *Technological and Economic Development of Economy, 18*(1), 117–131.

Wenfei, F. 2012. Graph Pattern Matching Revised for Social Network Analysis. In *ICDT '12 Proceedings of the 15th International Conference on Database Theory,* 8–21.

Wielebski, L., Medynska-Gulij, B. 2018. Graphically sup*ported evaluation of mapping techniques used in presenting spatial accessibility. In Cartography and Geographic Information Science, 46*(4), 311–333.

Zapata-Barra, M., Rodriguez, A., Caro, A., Fernandez, E. 2018. Towards Obtaining UML Class Diagrams from Secure Business Processes Using Security Patterns. In *Journal of Universal Computer Science, 24*(10), 1472–1492.

Zavadskas, E. K., & Vilutiene. T.. 2006. A multiple criteria evaluation of multi-family apartment block's maintenance contractors: I-Model for maintenance contractor evaluation and the determination of its selection criteria. *Building and Environment, 41*(5), 621–632.

Zeng, Y., Wang, D., Liu, W., & Xiong, A. 2009. An approximation algorithm for weak vertex cover problem in IP network traffic measurement. In *2009 IEEE International Conference on Network Infrastructure and Digital Content*, 182–186.

Zeng, W. 2019. A methodology for cost-benefit analysis of information security technologies. In *Concurrency and Computation-Practice & Experience 31*(7), e5004.

Zhao, P., & Han, J. 2010. On graph query optimization in large networks. In *Proceedings of the VLDB Endowment*, *3*(1–2), 340–351.

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

Papers in the Reviewed Scientific Journals

Olifer, D., Goranin, N., Cenys, A., Kaceniauskas, A., Janulevicius, J. 2019. Defining the Minimum Security Baseline in a Multiple Security Standards Environment by Graph Theory Techniques. *MDPI – Applied Sciences 9*(4), 681, 1–16. [Science Citation Index Expanded (Web of Science)], [Index: 1,689 (2017, InCites JCR SCIE)]

Olifer, D., Goranin, N., Kaceniauskas, A., Cenys, A. 2017. Controls-based approach for evaluation of information security standards implementation costs. *Technological and Economic Development 23*(1), 196–219. [Social Sciences Citation Index (Web of Science)], [Index: 3,244 (2017, InCites JCR SSCI)]

Ramanauskaite, S., Olifer, D., Goranin, N., Cenys, A. 2013. Security Ontology for adaptive mapping of Security standards. *International Journal of Computers Communications & Controls, 8*(6), 813–825. [Science Citation Index Expanded (Web of Science)], [Index: 0,694 (2013, InCites JCR SCIE)]

Ramanauskaitė, S., Olifer, D., Goranin, N., Cenys, A., Radvilavičius, L. 2014. Visualization of mapped security standards for analysis and use optimization.

International journal of computer theory and engineering, 6(5), 372–376. [IndexCopernicus]

Ramanauskaitė, S., Radvilė, E., Olifer, D. 2013. Ontologijos naudojimas informacijos saugumo reikalavimams susieti. *Mokslas – Lietuvos ateitis = Science – future of Lithuania: elektronika ir elektrotechnika = Electronics and electrical engineering*. Vilnius: Technika. 88–91.

Papers in other Editions

Olifer, D. Evaluation metrics for ontology-based security standards mapping. In *Electrical, Electronic and Information Sciences (eStream): proceedings of the 2015 Open conference, 21 April 2015, Vilnius, Lithuania,1–4.*

Olifer, D., Goranin, N., Janulevicius, J., Kaceniauskas, A., & Cenys, A. 2017. Improvement of Security Costs Evaluation Process by Using Data Automatically Captured from BPMN and EPC Models. In *International Conference on Business Process Management–Business Process management Workshops – SPBP'17, vol. 308*, 698–709.

Ramanauskaite, S., Goranin, N., Cenys, A., & Olifer, D. 2013. Ontology-based security standards mapping optimization by means of Graph theory. In *Proceedings of International Congress on engineering and technology ICET 2013*, 74–83.

Summary in Lithuanian

Įvadas

Problemos formulavimas

Didėjant kibernetinių atakų kiekiui, valstybės ir komercinės organizacijos taiko vis griežtesnius reikalavimus informacijos ir asmens duomenų apsaugai. Vienas geresnių būdų tai pasiekti yra realizuoti reikalavimus ir taikyti priemones, kurios yra aprašytos informacijos saugos dokumentuose. Atsižvelgiant į tai, organizacijai yra labai svarbu pasirinkti rizikos mažinimo priemones, kurios garantuotų reikiamą apsaugos lygį ir būtų efektyvios kaštų vertinimo prasme.

Esant dabartinėms rinkos sąlygoms ir siekiant įgauti komercinį pranašumą, organizacijos yra priverstos atitikti daugiau negu vieno dokumento reikalavimams. Finansinės organizacijos, kurios dirba su mokėjimo sistemomis, privalo atitikti PCI DSS standarto reikalavimus bei Bendro duomenų apsaugos reglamento reikalavimus, jei organizacija veikia Europos Sąjungoje. Ši situacija dar labiau komplikuojasi, atsižvelgiant į tai, kad egzistuoja skirtingos metodikos, aprašančios būdus atitikti nustatytiems reikalavimams.

Šiuo metu dokumentų susiejimui plačiai naudojamos harmonizavimo metodikos, kurios vėliau naudojamos vizualizuojant gautus rezultatus. Tačiau privalomų reikalavimų nustatymui reikia ekspertinių žinių ir atskiro harmonizuotos informacijos įvertinimo.

Siekiant automatizuoti skirtingų saugos dokumentų reikalavimų harmonizavimą ir jų rezultatų analizę, buvo pasiūlytas adaptyvus susiejimas ir analizė naudojant grafų teorijos algoritmus ir savybes. Saugumo reikalavimai pristatomi, kaip grafo viršūnės, o ryšiai tarp jų pristatomi, kaip grafo briaunos. Toks saugos dokumentų atvaizdavimo būdas leidžia besidubliuojančių reikalavimų ir trūkstamų reikalavimų paieškai pritaikyti Viršūnių dangos radimo (angl. Vertex cover) ir kitus grafų teorijos optimizavimo algoritmus.

Darbo aktualumas

Mokslininkai labiau orientuojasi į specifinių saugumo užtikrinimo klausimų sprendimus, ir mažiau dėmesio skiria problemoms susijusioms su informacijos saugos priemonių įgyvendinimu atsižvelgiant į organizacijoje egzistuojančius procesus. Platesnis požiūris į informacijos saugą leidžia užtikrinti efektyvesnę organizacijos apsaugą, tačiau reikalauja daugiau resursų ir didina informacijos apsaugos sistemos kompleksiškumą.

Tam, kad suvaldyti šiuos iššūkius Informacijos saugos specialistas privalo suprasti skirtingų saugą reglamentuojančių dokumentų reikalavimus, kurie yra taikomi organizacijos sistemoms bei nustatymui efektyviausių būdų, kurie taikomi reikalavimų įgyvendinimui. Automatinis kelių dokumentų susiejimas su tolimesniu nustatymu minimalių saugos gairių ir jų palyginimu su organizacijoje įgyvendintomis saugos priemonėmis, leistų sumažinti subjektyvumo lygį bei padidinti informacijos analizę ir jos pritaikymo efektyvumą. Informacijos saugos dokumentų bei jų harmonizavimo rezultatų atvaizdavimas grafų pavidalu su tolimesniu grafų teorijos optimizavimo algoritmo taikymu, leistų automatizuoti informacijos saugos dokumentų analizės procesą.

Tyrimo objektas

Pagrindinis šio tyrimo objektas yra informacijos saugos dokumentų reikalavimų harmonizavimo ir analizės metodas.

Darbo tikslas

Disertacijos tikslas – padėti identifikuoti minimalius saugos reikalavimus, kai yra įgyvendinami kelių informacijos saugą reguliuojančių dokumentų nustatyti reikalavimai.

Darbo uždaviniai

Nustatyto darbo tikslo pasiekimui, būtina išspręsti žemiau pateiktus darbo tikslus:

1. Atlikti informacijos saugos dokumentų ir juose nustatytų saugumo reikalavimų analizę ir nustatyti informacijos saugos dokumentų ir jų reikalavimų harmonizavimo, analizės bei įvertinimo metodikas.
2. Sukurti informacijos saugos standartų reikalavimų įgyvendinimo kaštų vertinimo metodiką.
3. Sukurti metodiką automatizuotam informacijos saugos dokumentų ir jų reikalavimų harmonizavimui, analizei ir įvertinimui.

4. Atlikti eksperimentinius tyrimus, siekiant įvertinti sukurtas metodikas, įskaitant minimalių saugos gairių nustatymą ir įvertinimą, bei gautus rezultatus palyginti su organizacijoje įgyvendintomis saugumo priemonėmis.

Tyrimų metodika

Tiriant darbo objektą, buvo pasirinkti žemiau aprašyti tyrimo metodai:

- Teorinis (analizės ir sintezės) tyrimas atliktas siekiant nustatyti problemos sprendimo strategiją.
- Klasifikavimas: Literatūroje pateiktų metodikų, privalumų ir trūkumų apibendrinimas, siekiant išgryninti disertacijos tyrimo objekto bei darbo tikslą.
- Patirtis: Problemos sprendimas grindžiamas moksliniais tyrimais bei kitų mokslininkų įžvalgomis bei patirtimi.
- Eksperimentas: Suformuota hipotezė patvirtinta eksperimentiniu tyrimu.
- Įvertinimas: Išvados pateiktos atsižvelgiant į tyrimo metu surinktus išanalizuotus ir išaiškintus duomenis.

Darbo mokslinis naujumas

Darbo mokslinis naujumas pagrįstas šiais rezultatais:

1. Sukurtas informacijos saugos dokumentų reikalavimų įgyvendinimo kaštų įvertinimo metodas, kuris orientuotas į saugos priemonių įgyvendinimo procesą, todėl leidžia detaliai įvertinti visus kaštus susijusius su informacijos saugos priemonėmis bei jų įtaką bendram organizacijos saugumui.
2. Sukurtas minimalių saugos gairių nustatymo metodas. Šis metodas leidžia įvertinti kelių informacijos saugos dokumentų reikalavimus, pateiktus harmonizuotu pavidalu, ir pritaikant grafų teorijos viršūnių dangos radimo algoritmus suformuoti minimalias saugos gaires, pašalinant besidubliuojančius reikalavimus.
3. Sukurtas organizacijos įgyvendintų saugos reikalavimų įvertinimo metodas, kuris grafų izomorfizmo savybės pagalba, leidžia palyginti organizacijoje įgyvendintas saugos priemones su nustatytomis minimaliomis saugos gairėmis.

Darbo rezultatų praktinė reikšmė

Disertacijos pasiūlytų metodų teorinė ir praktinė svarba pasižymi jų pritaikomumu nuolat besikeičiančioje informacijos saugos užtikrinimo srityje, kuri apima technologinius, organizacinius bei fizinius informacijos saugos užtikrinimo aspektus.

Pasiūlyti metodai apima: saugos priemonių įgyvendinimo kaštų įvertinimo metodą; saugos dokumentų harmonizavimo metodą, naudojantį adaptyvų susiejimą per ontologiją;

minimalaus saugos gairių identifikavimo metodą, pritaikant grafų teorijos optimizavimo algoritmus, rodo tarpdisciplininį žinių pritaikymą, kai problemos sprendimui naudojami informatikos inžinerijos technikos ir metodai bei pritaikomos informacijos saugos vadybos procesai ir žinios. Unikaliu galima pavadinti minimalaus saugos gairių nustatymo automatizavimo metodą, kai informacijos saugos dokumentų ir reikalavimų analizei naudojami gerai žinomi grafų teorijos optimizavimo algoritmai, tokie kaip viršūnių dangos radimo algoritmas bei grafų izomorfizmo savybės.

Sukurtas vizualizavimo įrankis, gali būti naudojamas saugos dokumentų reikalavimų ryšių bei tarpusavio priklausomybių atvaizdavimui. Pasiūlytas kaštų vertinimo metodas leistų organizacijoms efektyviai valdyti kaštus susijusius su informacijos saugos įgyvendinimu.

Dalis disertacijos atliktų tyrimų buvo finansuojama ir įgyvendinant „Virtualizavimo, vizualizavimo ir saugos e. paslaugų technologijų kūrimas ir tyrimai“ projektą. Projektas buvo įgyvendinamas 2012–2014 mm. Projekto kodas: VP1-3.1-ŠMM-08-K-01-012.

Ginamieji teiginiai

Išanalizavus tyrimo metu nustatytą informaciją ir įvertinus darbo tikslus bei uždavinius buvo suformuluoti žemiau pateikti ginamieji teiginiai:

1. Kaštų įvertinimas, atliekant skaičiavimus privalo atsižvelgti į įmonės brandos lygį bei organizacijos sistemų kompleksiškumą.
2. Adaptyvus susiejimas su ontologija, paremtas žinomomis metodikomis arba dokumentais, leidžia susieti kelis saugą reglamentuojančius dokumentus ir jų reikalavimus, neatlikus anksčiau pasiektų rezultatų pakartotinio vertinimo.
3. Minimalių saugos gairių nustatymas, nagrinėjant harmonizuotą, kelių susietų informacijos saugos dokumentų atvaizdą, gali būti automatizuotas taikant grafų teorijos viršūnių dangos radimo algoritmus ir grafų izomorfizmo savybes.

Darbo rezultatų aprobavimas

Disertacijos tema paskelbtas 8 mokslinės publikacijos, iš kurių: 3 publikuotos žurnaluose, kurie yra įtraukti į *Clarivate Analytics* (buv. *Thomson Reuters*) *Web of Science* duomenų bazę, 5 – mokslinių konferencijų pranešimų rinkiniuose. Moksliniai rezultatai buvo pristatyti 3 mokslinėse konferencijose:

- *Business Process Management konferencija 2017: Business Process Management Workshops*. 2017 m. rugsėjo 10–11 d., Barselona, Ispanija,
- *Electrical, Electronic and Information Sciences (eStream): proceedings of the 2015 open conference*. 2015 m. balandžio 21 d., Vilnius, Lietuva.
- *2nd International conference on Information Technology and Science (ICITS 2014)*. 2014 m. kovo 27–28 d., Šanchajus, Kinija.

Disertacijos struktūra

Disertacija yra sudaryta iš įvado, trijų pagrindinių skyrių, bendrųjų išvadų, literatūros šaltinių sąrašo, disertacijos autoriaus publikacijų sąrašo bei santraukos lietuvių kalba. Disertacijos apimtis: 138 puslapiai, 35 paveikslai ir 22 lentelės.

1. Informacijos saugos reikalavimų harmonizavimo, analizės ir įvertinimo metodai

Šiame skyriuje apžvelgiami esami informacijos saugos dokumentų bei jų reikalavimų harmonizavimo, analizės ir įvertinimo metodai ir jų aspektai. Taip pat šiame skyriuje apibrėžiamos saugos reikalavimų įgyvendinimo kaštų metodikos.

Pastaruoju metu organizacijos ir jų vadovai vis labiau supranta informacijos ir duomenų apsaugos įtaką jų veiklai. Tai sąlygoja išoriniai faktoriai, tokie kaip išorinių reguliatorių, tokių kaip BDAR (angl. GDPR) reglamento arba PCI DSS standarto, reikalavimai, bei vidiniai faktoriai, tokie kaip noras gauti konkurencinį pranašumą. Vienas iš būdų tai pasiekti – įgyvendinti reikalavimus aprašytus informacijos saugą reglamentuojančiuose dokumentuose.

Nagrinėjant informacijos saugą reglamentuojančius dokumentus, galima išskirti 4 pagrindinius tipus: Informacijos saugos tarptautiniai standartai (ISO27000 serijos standartai, PCI DSS standartas, FIPS standartas); Informacijos saugą reglamentuojantys aktai (FISMA, HIPAA, SOX); Įstatymai ir metodologijos (GDPR, COBIT, COSO); Informacijos saugos specialios publikacijos (NIST SP 800-53, NISTIR 7621). Reikėtų pastebėti, kad kai kurie informacijos saugą reglamentuojantys dokumentai yra taikomi, tik tam tikrose srityse arba reglamentuojantys tam tikrus informacijos saugos aspektus. Tyrimo metu buvo nustatyta, kad dažnai organizacijos reikalauja atitikti daugiau negu vieno informacijos saugos dokumento reikalavimams, tokiu atveju labai svarbu nustatyti, kaip vieno dokumento reikalavimai koreliuoja su kito saugos dokumento reikalavimais.

Išspręsti šią dilemą gali padėti dokumentų harmonizavimo būdai. Mokslininkai išskiria 4 pagrindinius harmonizavimo būdus: semantinis suderinamumas, susiejimas, adaptyvus susiejimas ir integracija. Informacijos saugos srityje plačiausiai paplitęs susiejimo harmonizavimo būdas, kuris taikomas siekiant palyginti tarpusavyje kelis informacijos saugos dokumentus. Dažniausiai jis yra taikomas susieti 2 informacijos saugos dokumentus, retais atvejais jis gali būti panaudotas susieti 3 arba daugiau dokumentų. Pagrindinis šio harmonizavimo metodo trūkumas, kad naujo dokumento pridėjimas reikalauja atlikti naujo dokumento susiejimą su jau susietais dokumentais. Išspręsti šią problemą padeda adaptyvus susiejimas, kuris leidžia panaudoti vieną dokumentą, kaip susiejimo pagrindą ir visus kitus dokumentus sieti per jį.

Taikant adaptyvų susiejimą labai svarbu nustatyti susiejimo pagrindo dokumentą. Šis dokumentas turėtų plačiai padengti visas galimas informacijos saugos sritis, bei apimti kitus organizacijos procesus. Vienas iš būdų taikyti šiam procesui saugumo ontologijas. Šiuo metu egzistuoja kelios saugos ontologijos, tačiau jų formavimo principai yra skirtingi. F. Massacci ontologija orientuota į saugumo reikalavimus, J. Undercoffer orientuota į kompiuterines atakas. Detaliausias saugumo ontologijas pasiūlė A. Herzog ir S. Fenz.

A. Herzog ontologija nukreiptą į informacijos saugos sritis, tuo metu kai S. Fenz ontologija orientuota į ISO27001 ir Grundschutz informacijos saugos standartų konceptus. Tačiau tyrimo metu buvo nustatyta, kad minėtos ontologijos negali efektyviai susieti kelių informacijos saugos dokumentų ir nėra tinkamos naudoti kaip pagrindas adaptyviam susiejimui.

Tyrimo metu buvo išanalizuotos galimybės susiejimo rezultatus atvaizduoti grafiniu pavidalu. Tam buvo įvertinti esami būdai, tokie kaip 2.5D, 3D, HeatMap bei Chord diagramos. Buvo nustatyta, kad išanalizuoti būdai gali atvaizduoti bendrą susiejimo informaciją, tačiau negali pateikti detalios informacijos apie informacijos saugos reikalavimų tarpusavio ryšio bei jų padengiamumo lygį.

Nagrinėjant informacijos saugos įgyvendinimo procesus, buvo nustatyta, kad organizacijoms labai svarbu užtikrinti, kad realizuojamos saugos priemonės būtų efektyvios bei ekonomiškai naudingos. Tai yra ypač svarbu, kaip organizacijos bando įgyvendinti daugiau negu vieną informacijos saugos dokumentą bei juose aprašytus reikalavimus. Tyrimo metu buvo nustatyta, kad daugumos kaštų vertinimo metodai yra taikomi investicijų grąžos vertinimui arba rizikos mažinimo vertinimui ir nėra taikomi saugumo priemonių įgyvendinimo procesų vertinimui.

Organizacijoms, siekiančioms įgyvendinti kelių dokumentų reikalavimus svarbu nustatyti būtinus saugos reikalavimus, aprašytus dokumentuose, kuriems jie stengėsi atitikti ir palyginti jau įgyvendintas saugos priemones su nustatytomis vertinimo metu. Ankščiau aprašyta saugos ontologija leidžia susieti informacijos saugos dokumentus, tačiau neleidžia vienareikšmiškai nustatyti būtinus minimalius saugos reikalavimus. Norint pasiekti šį tikslą galima taikyti grafų teorijos optimizavimo algoritmus, tokius kaip viršūnių dangos radimą bei panaudoti grafų izomorfizmo savybes.

2. Informacijos saugos dokumentų reikalavimų įgyvendinimo kaštų vertinimo metodas, orientuotas į saugos priemonių realizavimo procesą

Literatūros bei esamų mokslinių tyrimų analizės metu buvo nustatyta, kad kaštų vertinimo metodikos yra orientuotos į investicijų grąžą arba kaštų vertinimą per rizikų suvaldymo prizmę. Kalbant apie Informacijos saugos kaštų įvertinimą išskiriami penki pagrindiniai būdai, kurie atsižvelgia į: organizacijos balansą; saugumo priemonių gyvavimo ciklą; informacinių technologijų saugumo procesus; ISO 27001 standartą bei informacijos saugos valdymo sistemos sritį.

Tyrimas parodė, kad egzistuojantys būdai turi savo privalumus ir trūkumus. Vienas iš trūkumų pastebėtas visuose metoduose yra susijęs su sudėtingais metodų pritaikymais, naujo dokumento saugos priemonių įgyvendinimo kaštų vertinimui. Siekiant įvertinti atitikimą naujam dokumentui visus skaičiavimus reikės pakartoti iš naujo. Taip pat buvo pastebėta, kad esami būdai, išskyrus skirtus ISO27001 ir Informacijos saugos valdymo sistemos sričiai, nėra tiesiogiai koreliuojami su informacijos saugos reikalavimus reguliuojančiais dokumentais. Bet ir paminėti 2 būdai yra orientuoti į vieną informacijos saugos standartą – ISO 27001.

Atsižvelgiant į tai ir įvertinus mūsų tikslą, saugos reikalavimų įgyvendinimą organizacijose, kurios siekia atitikti daugiau negu vienam informacijos saugos dokumentui, buvo pasiūlytas naujas informacijos saugos įgyvendinimo kaštų įvertinimo būdas, orientuotas į detalų saugos priemonių įgyvendinimo procesą.

Pasiūlytas metodas į skaičiavimus įtraukia du pagrindinius procesus:

- ✓ Rizikos įvertinimą;
- ✓ Saugos priemonių įgyvendinimą.

Toks požiūris leidžia detaliai įvertinti visus saugos įgyvendinimo kaštų aspektus. Siekiant užtikrinti, kad pasiūlytas kaštų įvertinimas galėtų būti taikomas skirtingų dydžių organizacijoms papildomai buvo įvestas brandos lygio bei sistemų kompleksiškumo koeficientas φ ir pagrindinė kaštų vertinimo formulė priėmė tokį pavidalą:

$$C_{Security} = \varphi(C_{Risk\_assessment} + \sum_{i=1}^{n} C_{Security_{control_{implementation_i}}}(standard)), \qquad \text{(S2.1)}$$

čia φ – brandos lygio bei sistemų kompleksiškumo koeficientas; $C_{Risk\_assessment}$ – Rizikos įvertinimo kaštai; $C_{Security\_control\_implementation_i}(standard)$ – Saugos priemonių įgyvendinimo kaštai.

Siekiant apskaičiuoti rizikos įvertinimo kaštus reikėtų įvertinti visų rizikos procesų sudedamąsias dalis ir tai mes galim padaryti pritaikius tokią formulę:

$$C_{Risk\_assessment} = C_{Asset\_analysis} + C_{Vulnerabilities\_analysis} + C_{Threat\_analysis} + C_{Impact} + C_{Penetration\_testing}(N) + \; C_{Gap\_analysis}\,, \qquad \text{(S2.2)}$$

čia $C_{Asset\_analysis}$ – Kritinio turto įvertinimo kaštai, $C_{Vulnerabilities\_analysis}$ – Pažeidžiamumo vertinimo kaštai, $C_{Threat\_analysis}$ – Grėsmių analizės kaštai, $C_{Gap\_analysis}$ – Trūkumų analizės kaštai ir $C_{Penetration\_testing}(N)$ – Saugos tyrimų kaštai, kur N yra analizuojamų sistemų kiekis, C_{Impact} – Žalos įvertinimo kaštai.

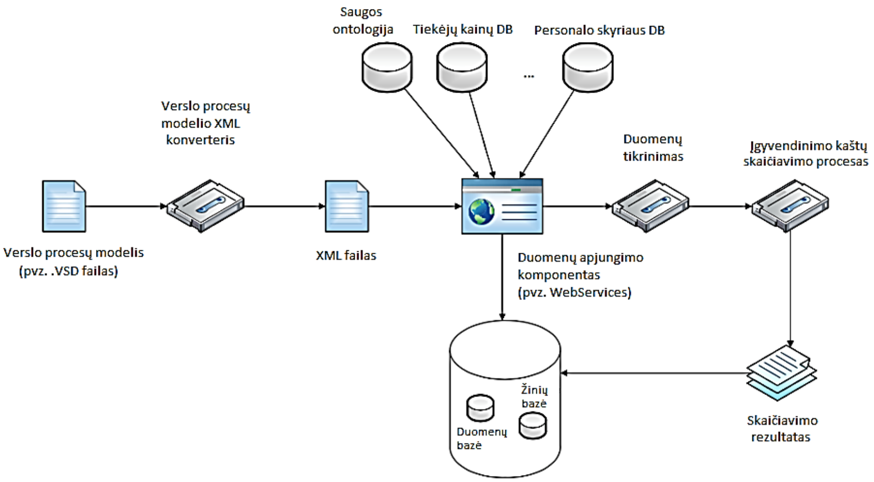
Saugos priemonių įgyvendinimui buvo pasiūlyta taikyti tokius skaičiavimus:

$$C_{Security\_control\_implementation} = \sum_{i=1}^{n}(m_i\,(Risk_i) * (C_{Mitigation\_strategy_i} + C_{Action_i})), \qquad \text{(S2.3)}$$

čia $m_i(Risk_i)$ – saugos priemonės svarbumo koeficientas, $C_{Mitigation\_strategy_i}$ – yra rizikos mažinimo strategijos kaštai ir C_{Action_i} – yra rizikos mažinimo veiksmų kaštai. Reikėtų pastebėti, kad kiekviena rizikos mažinimo strategija (rizikos išvengimas, rizikos mažinimas, rizikos perdavimas ir rizikos priėmimas) turi savo sudėtingus skaičiavimus, susijusius su statistiniais duomenimis ir rizikos priėmimo apetito nustatymais.

Atlikus eksperimentą buvo nustatyta, kad pasiūlytas metodas leidžia atlikti detalesnę kaštų analizę, tačiau pirminiam skaičiavimui reikalauja didelio kiekio duomenų. Ir net esant tokiems apribojimams eksperimento rezultatai parodė, kad pasiūlytas būdas pirminiam skaičiavimui pareikalavo 2 kartus daugiau laiko, negu egzistuojantys kaštų įvertinimo būdai, tačiau visa informacija buvo renkama pirmą kartą.

Siekiant patobulinti ir automatizuoti kaštų įvertinimo metodą, buvo pasiūlytas automatinis duomenų surinkimas iš verslo procesų diagramų, jau egzistuojančių organizacijoje.


Saugos ontologija
Tiekėjų kainų DB
Personalo skyriaus DB
...
Verslo procesų modelio XML konverteris
Duomenų tikrinimas
Įgyvendinimo kaštų skaičiavimo procesas
Verslo procesų modelis (pvz. .VSD failas)
XML failas
Duomenų apjungimo komponentas (pvz. WebServices)
Žinių bazė
Duomenų bazė
Skaičiavimo rezultatas

S2.1 pav. Verslo procesų modelio integravimas su saugos kaštų įvertinimo metodu

Tyrimo metu buvo išanalizuotos verslo procesų diagramos ir juose pateikiama informacija, tolimesniam tyrimui buvo pasirinktos BPMN ir EPC diagramos. Nagrinėjant šias diagramas buvo įvertinta jų pateikiamos informacijos detalizacijos lygis bei kaštų skaičiavime naudojamų komponentų padengiamumas. Buvo nustatyta, kad ne visi komponentai (pvz. brandos lygio bei sistemos kompleksiškumo koeficientas bei saugos tyrimo kaštų įvertinimas) yra atvaizduojami verslo procesuose, o kai kurie komponentai pateikia tik dalinę informaciją reikalingą skaičiavimams.

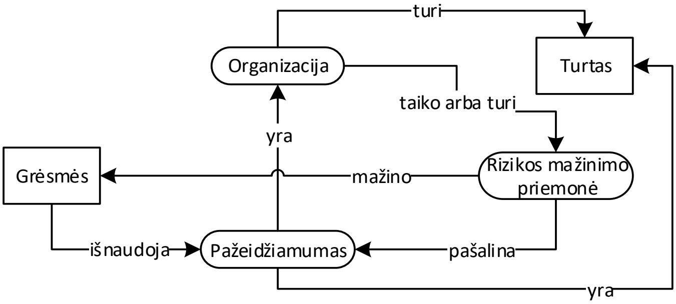
Atliktas eksperimentas parodė, kad pasiūlytas būdas leidžia automatizuoti reikiamos informacijos surinkimą (S2.1 pav.), tačiau siekiant padidinti jo efektyvumą reikėtų papildyti egzistuojančius verslo procesus, pateikiant daugiau papildomos informacijos apie verslo procesų komponentus.

3. Informacijos saugos reikalavimų harmonizavimo, analizės ir įvertinimo automatizavimas

Organizacijoms siekiant įgyvendinti kelių informacijos saugos dokumentų reikalavimus, svarbu suprasti, kaip reikalavimai yra tarpusavyje susieti. Literatūros analizės metu buvo išnagrinėti skirtingi harmonizavimo būdai, tačiau jų taikymas sprendžiant uždavinius kur reikia susieti daugiau negu du informacijos saugos dokumentus yra sudėtingas.

Atsižvelgiant į tai, buvo pasirinktas adaptyvaus susiejimo metodas per vieną bendrą saugą reglamentuojantį dokumentą arba metodiką. Siekiant užtikrinti kokybišką ir efektyvų susiejimą pasirinktas pagrindas turi būti kuo platesnis ir padengti visas saugumo sritis. Įvertinus saugos dokumentus bei ontologijas, buvo nustatyta, kad esami dokumentai bei ontologijos negalės tai padaryti kokybiškai. Iš saugos dokumentų geriausiai tiktų ISO27001 standartas, tačiau jis visiškai neatsižvelgia į kitus organizacijos procesus, kurie irgi gali įtakoti saugos užtikrinimą. Įvertinus egzistuojančias ontologijas, buvo nustatyta, kad jos daugumoje yra siaurai orientuotos, ko pasekoje kai kurie specifiniai skirtingų dokumentų reikalavimai gali nerasti reikiamo atitikmens ontologijoje.

Įvertinus šitas problemas buvo nuspręsta pasiūlyti ontologiją, kurios pagrindu būtų dokumentas arba metodika apimanti visas informacijos saugos užtikrinimo sritis bei leidžianti lengvai integruotis su kitais įmonės procesais, tai pat ontologija turi išnaudoti egzistuojančių ontologijų privalumus. Buvo nuspręsta, kad ontologija aprašys 5 pagrindines informacijos saugos klases: Turtas, Saugos priemonės, Organizacija, Grėsmės ir Pažeidžiamumai (S3.1 pav.). Kaip ontologijos pagrindas buvo paimta COBT v5 metodika, leidžianti aprašyti visus organizacijoje esančius informacinių technologijų bei organizacijos valdymo procesus, įskaitant ir informacijos saugos užtikrinimą. Informacijos saugos užtikrinimo sritis buvo aprašyta detaliai, tuo metu kai kiti procesai buvo pateikti abstrakčiai. Tačiau reikalui esant jie gali būti detalizuoti.



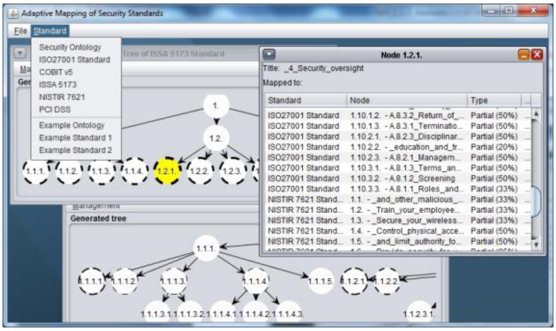
S3.1 pav. Saugumo ontologijos schema

Pasiūlyta ontologija buvo susieta su tais pačiais dokumentais, kurie buvo naudojami S. Fenz ir A. Herzog ontologijų nagrinėjimui. Įvertinimo rezultatai, rodo, kad nauja ontologija leidžia geriau susieti dokumentų reikalavimus su ontologija, ko pasekoje mes galime pasiekti tikslesnius rezultatus, vertinant skirtingų saugos dokumentų tarpusavio padengiamumą, naudojant susiejimą per ontologiją (S3.1 lentelė).

S3.1 lentelė. Standartų ir ontologijų palyginimas

Standartas	Ontologijos / Standarto padengiamumas					
	S. Fenz		A. Herzog		Pasiūlyta ontologija	
	Covered	Covers	Covered	Covers	Covered	Covers
ISO27001	35/311 (11 %)	23/133 (17 %)	26/460 (6 %)	19/133 (14 %)	130/1795 (7 %)	107/133 (80 %)
PCI DSS	42/311 (14 %)	48/165 (29 %)	25/460 (5 %)	32/165 (19 %)	132/1795 (7 %)	165/165 (100 %)
ISSA 5173	31/311 (10 %)	7/12 (58 %)	29/460 (6 %)	6/12 (50 %)	15/1795 (1 %)	12/12 (100 %)
NISTIR 7621	14/311 (5 %)	8/10 (80 %)	21/460 (5 %)	8/10 (80 %)	19/1795 (1 %)	10/10 (100 %)

Standartiniai vizualizavimo būdai neleido vienareikšmiškai nustatyti kaip vieno dokumento saugos reikalavimas koreliuoja su kito dokumento analogišku reikalavimu. Siekiant patobulinti informacijos vizualizavimą buvo pasiūlytas susiejimo padengiamumo atvaizdavimas grafo pagalba (S3.2 pav.), kur kiekvienas reikalavimas yra grafo viršūnė. Viršūnės linijos storumas ir forma leidžia grafiniu pavidalu pateikti informaciją apie padengiamumą, kur linijos nebuvimas rodo, kad kituose dokumentuose, tokio reikalavimo nėra, o linijos storumas bei tarpai tarp linijos nurodo padengiamumo lygį. Detalesnę informaciją galima gauti peržiūrėjus viršūnės detalesnę informaciją. Pilnam adaptyvaus susiejimo atvaizdavimui buvo panaudota Chord diagrama.



Node 1.2.1.

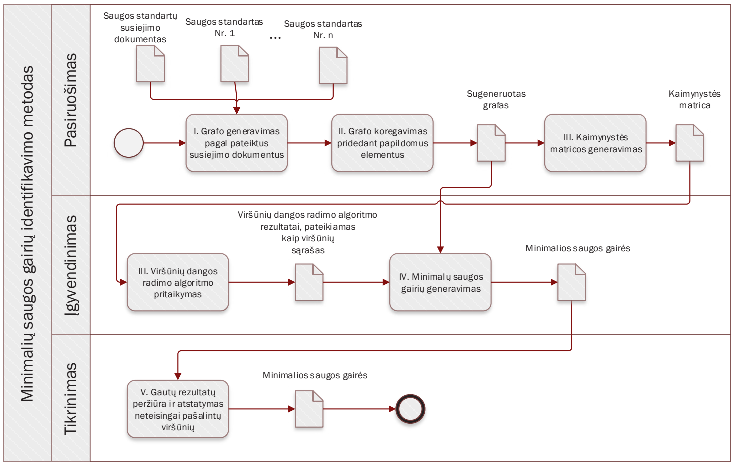
Title: _4_Security_oversight

Mapped to:

Standard	Node	Type
ISO27001 Standard	1.10.1.2. - A.8.3.2_Return_of_...	Partial (50%)
ISO27001 Standard	1.10.1.3. - A.8.3.1_Terminatio...	Partial (50%)
ISO27001 Standard	1.10.2.1. - A.8.2.3_Disciplinar...	Partial (50%)
ISO27001 Standard	1.10.2.2. - _education_and_tr...	Partial (20%)
ISO27001 Standard	1.10.2.3. - A.8.2.1_Managem...	Partial (50%)
ISO27001 Standard	1.10.3.1. - A.8.1.3_Terms_an...	Partial (50%)
ISO27001 Standard	1.10.3.2. - A.8.1.2_Screening	Partial (50%)
ISO27001 Standard	1.10.3.3. - A.8.1.1_Roles_and...	Partial (33%)
NISTIR 7621 Stand...	1.1. - _and_other_malicious_...	Partial (33%)
NISTIR 7621 Stand...	1.2. - _Train_your_employee...	Partial (33%)
NISTIR 7621 Stand...	1.3. - _Secure_your_wireless...	Partial (33%)
NISTIR 7621 Stand...	1.4. - _Control_physical_acce...	Partial (50%)
NISTIR 7621 Stand...	1.5. - _and_limit_authority_to...	Partial (50%)

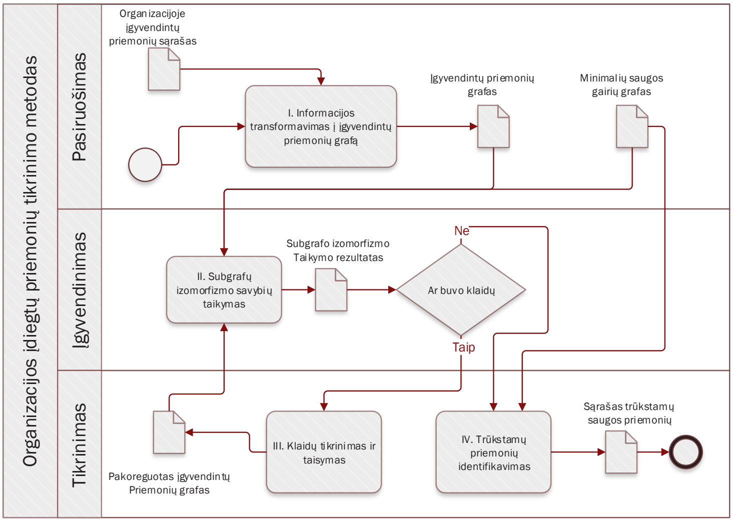
S3.2 pav. Adaptyvaus susiejimo atvaizdavimo būdas

Adaptyvus susiejimas leidžia apjungti daugiau negu du informacijos saugos dokumentus, tačiau neleidžia greitai ir efektyviai nustatyti minimalių būtinų reikalavimų aprašytų keliuose dokumentuose, bei palyginti jų su organizacijos įgyvendintomis saugos priemonėmis.


Minimalių saugos gairių identifikavimo metodas
Pasiruošimas
Įgyvendinimas
Tikrinimas
Saugos standartų susiejimo dokumentas
Saugos standartas Nr. 1
...
Saugos standartas Nr. n
I. Grafo generavimas pagal pateiktus susiejimo dokumentus
II. Grafo koregavimas pridedant papildomus elementus
Sugeneruotas grafas
III. Kaimynystės matricos generavimas
Kaimynystės matrica
III. Viršūnių dangos radimo algoritmo pritaikymas
Viršūnių dangos radimo algoritmo rezultatai, pateikiamas kaip viršūnių sąrašas
IV. Minimalų saugos gairių generavimas
Minimalios saugos gairės
V. Gautų rezultatų peržiūra ir atstatymas neteisingai pašalintų viršūnių
Minimalios saugos gairės

S3.3 pav. Minimalių saugos gairių identifikavimo metodas

Siekiant išspręsti šią problemą mes siūlome panaudoti grafų teoriją ir jos optimizavimo algoritmus. Minimalių saugos gairių nustatymui siūloma naudoti Viršūnių dangos radimo algoritmą, leidžiantį adaptyvaus susiejimo pagalba susietus dokumentus atvaizduoti kaip grafą ir pritaikius algoritmą pašalinti visus besidubliuojančius reikalavimus, taip paliekant tik minimalias saugos gaires. Metodo schema aprašyta aukščiau pateiktoje BPMN diagramoje (S3.3 pav.).


Organizacijos įdiegtų priemonių tikrinimo metodas
Pasiruošimas
Įgyvendinimas
Tikrinimas
Organizacijoje įgyvendintų priemonių sąrašas
I. Informacijos transformavimas į įgyvendintų priemonių grafą
Įgyvendintų priemonių grafas
Minimalių saugos gairių grafas
II. Subgrafų izomorfizmo savybių taikymas
Subgrafo izomorfizmo Taikymo rezultatas
Ar buvo klaidų
Ne
Taip
III. Klaidų tikrinimas ir taisymas
Pakoreguotas įgyvendintų Priemonių grafas
IV. Trūkstamų priemonių identifikavimas
Sąrašas trūkstamų saugos priemonių

S3.4 pav. Būdas įgyvendintų saugos priemonių palyginimui su Minimaliomis saugos gairėmis.

Identifikavus Minimalias saugos gaires, pritaikant grafų izomorfizmo savybes galima palyginti, kaip organizacijoje įgyvendintos saugos priemonės atitinka minimaliems saugos reikalavimams (S3.4 pav.).

Šiam eksperimentui buvo naudojamas HITRUST CSF 9,1 metodikos susiejimas, ko pasekoje buvo gautas grafas su 1267 viršūnėmis ir 2512 briaunomis. Pritaikius pasiūlytą metodą, reikalavimų skaičių pavyko sumažinti iki 322 viršūnių. Pritaikius izomorfizmo savybes gautas grafas buvo palygintas su organizacijos įgyvendintomis priemonėmis.

Bendrosios išvados

1. Atlikta analizė parodė, kad taikomi saugos dokumentų harmonizacijos būdai nėra adaptyvūs ir gali būti taikomi tik ribotam kiekiui dokumentų. Tuo pačiu metu įmonės privalo atitikti kelių saugos dokumentų reikalavimams. Tyrimo metu buvo nustatytos tokios problemos:
   1.1. Kelių informacijos dokumentų reikalavimų įgyvendinimas leidžia įgyvendinti besidubliuojančias arba prieštaraujančias saugos priemones. Tai gali vesti prie išaugusių saugos įgyvendinimo kaštų.

1.2. Esamos saugos priemonių įgyvendinimo kaštų vertinimo metodikos neatsižvelgia į informacijos saugos dokumentus bei neįtraukia organizacijos brandos bei sistemų kompleksiškumo koeficientų į skaičiavimus. Dauguma taikomų skaičiavimo metodų sudėtingi bei nėra adaptyvūs ir neleidžia reikalui esant lengvai į esamus skaičiavimus įtraukti naujų saugos komponentų.

1.3. Esami harmonizacijos metodai leidžia susieti kelis dokumentus, tačiau naujų dokumentų įtraukimas į harmonizacijos procesą reikalauja iš naujo įvertinti prieš tai buvusius rezultatus. Adaptyvus susiejimas per ontologijas parodė, kad egzistuojančios ontologijos buvo sukurtos spręsti kitus uždavinius ir nėra tinkamos saugos dokumentų susiejimui.

2. Buvo pasiūlyta saugos priemonių įgyvendinimo kaštų skaičiavimo metodika leidžianti atsižvelgti į saugos dokumentų reikalavimus. Pateiktas metodas ne tik tiesiogiai susietas su informacijos saugos reikalavimais, bet ir integruoja organizacijos brandos ir sistemų sudėtingumo koeficientus į skaičiavimus. Pasiūlytas metodas buvo patikrintas atliekant eksperimentinius bandymus. Atlikti testavimai parodė, kad pirmas skaičiavimas reikalauja didelio kiekio duomenų (17 formulių ir 32 skirtingų komponentų) ir daug laiko (vieno proceso kaštų apskaičiavimas truko daugiau negu 1 val.), tačiau sekantys skaičiavimai naujiems saugos dokumentams yra 50 % greitesni. Skaičiavimo laikas mažėja, nes metodas naudoja ankstesnius skaičiavimo rezultatus. Siekiant dar sumažinti skaičiavimo laiką, buvo pasiūlytas patobulinimas, leidžiantis dalį skaičiavimams reikalingos informacijos išgauti iš verslo procesų diagramų (BPMN ir EPC).

3. COBIT v5 metodika buvo pasiūlyta kaip pagrindas naujai kuriamai saugos ontologijai. Naujos ontologijos analizė parodo, kad ji leidžia padengti daugiau kaip 90 % su ja susietų keturių saugos dokumentų reikalavimų, naudojamų bandyme. Rezultatų atvaizdavimui buvo sukurti vizualizavimo metodai. Chord diagramos pagrindu sukurta vizualizacija naudojama saugos dokumentų susiejimo atvaizdavimui, o grafais grindžiamas atvaizdavimas naudojamas pateikiant detalesnę informaciją apie reikalavimų padengiamumo laipsnius bei pačius reikalavimus.

4. Buvo pasiūlytas minimalių saugos gairių identifikavimo metodas, kuris leidžia analizuoti harmonizuotus dokumentus ir šalinti besidubliuojančius reikalavimus. Tai pasiekiama atvaizduojant saugos dokumentų reikalavimus grafų pagalba, kur reikalavimai yra viršūnės, o briaunos yra ryšiai tarp reikalavimų. Pritaikius viršūnių dangos radimo algoritmą galima pašalinti identiškus reikalavimus ir tokiu būdu suformuoti naują grafą turintį tik unikalius reikalavimus iš harmonizuotų dokumentų aibės. Pasiūlytas metodas taip pat leidžia, pritaikius grafų izomorfizmo savybes, palyginti organizacijos įgyvendintas saugos priemones su minimaliais saugos gairių reikalavimais. Pateiktas metodas buvo patikrintas pritaikant viršūnių dangos radimo algoritmą harmonizuotų dokumentų grafo analizei. Grafo viršūnių kiekis buvo sumažintas 74,76 %, pašalinant trijų saugos dokumentų besidubliuojančius reikalavimus.

Annexes[1]

Annex A. Control-based Method Experimental Results
Annex B. Experts Knowledge Verification Results
Annex C. System Usability Scale Questionnaire
Annex D. Author's Declaration of Academic Integrity
Annex E. Co-Authors Agreements to Provide the Material of the Joint Publications in the Dissertation
Annex F. Copies of Scientific Publications by the Author on the Topic of the Dissertation.

[1] The annexes are supplied in the enclosed compact disc

Dmitrij OLIFER

AUTOMATION OF HARMONIZATION,
ANALYSIS AND EVALUATION OF
INFORMATION SECURITY REQUIREMENTS

Doctoral Dissertation

Technological Sciences,
Informatics Engineering (T 007)

INFORMACIJOS SAUGOS REIKALAVIMŲ
HARMONIZAVIMO, ANALIZĖS IR
ĮVERTINIMO AUTOMATIZAVIMAS

Daktaro disertacija

Technologijos mokslai,
informatikos inžinerija (T 007)

2019 07 22. 15,75 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