Corvinus University of Budapest

Doctoral School of Business Informatics

Ph.D. Thesis

Summary

Blerton Abazi

A novel approach for information security risk assessment maturity framework based on ISO 27001

Supervisor: Andrea Kő, PhD

Budapest, 2020

Department of Information Systems

A novel approach for information security risk assessment maturity framework based on ISO 27001

Ph.D. Thesis

Summary

@ Blerton Abazi

Supervisor: Andrea Kő, PhD

Budapest, 2020

Contents

I. Background and overview of the Research 4

I.1 Structure of the Thesis 6

I.2 Objectives and Main Questions of the Research 9

II. Method of the Research 16

II.1 Proposed Research Methodology 17

III. The Proposed Framework prototype....... 19

III.2 Framework prototype validation method 23

IV. Results of the Research, Contribution of the Thesis 26

V. References.. 29

VI. References of the Author 30

I. BACKGROUND AND OVERVIEW OF THE RESEARCH

Security risk and metrics monitoring approach and solution should be available to IT and other business leaders, supporting risks identification and assessment quickly and providing recommendations according to that. Data is the key element of most businesses today, and the volume of data continues to grow by fifty percent a year, along with an increase in server numbers by twenty percent each year. According to Gartner (2016) the risk of data manipulation opportunities increases fast as well. The rapid development of IT, the transformation of society and digital businesses results in tremendous growth of the need for data security. Information security within an organization requires information to be protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and no access for unauthoriued users (availability). Businesses and organizations are responsible for information security, and continuously develop systems and update their existing systems to provide secure solutions. The majority of the new software have new and unique features. However, they usually also carry with them several weaknesses that can be harmful. In the majority of the cases the problems cannot be fixed quickly, as the systems are complex. Making changes within the system structure need to be verified, as it can affect some other part of the system, requiring a deep level of knowledge to address and implement.

For this reason, businesses and organizations in the private and public sector must deal with risk management and develop and maintain the related processes for their systems, in a proactive manner.

The main research goal of my thesis is to provide a new framework for a maturity model in the field of security risk assessment. The new framework supports the enterprises analyzing their security maturity level. It is based on the ISO 27001 and utilize the related standards too. As part of the research, I have developed a questionnaire with organizations' experts to identify the current level and practice of security in the above-mentioned sectors and to identify the requirements against my security risk framework and solution. The survey was filled in by organizations from the banking sector, IT industry and insurance organizations and shows a significant difference between sectors in the risk assessment practice. The detailed explanations of the results is discussed in chapter 6 in the thesis – Need Identification – Survey about the current level of security in enterprises.

I.1 Structure of the Thesis

My thesis includes nine chapters. The first chapter deals with introduction, background and problem statement. I detail the main goal and motivation of the research and discuss research questions and statements. The second chapter is about the literature review and theoretical background of my work. I started with information breaks and data referring to breaking security than I continued by listing the main security requirements and controls followed by an overview of the common attacks and threats. In the end I detailed some maturity models. The following part of the second chapter continues with introduction to risk management systems and it is summarizing with a briefly paragraph about the semi-automated risk assessment solutions.

In the third chapter I described the information security standards and models, starting from ISO 27000, NIST, ITIL, COBIT 5, CMMI and ISM 3. The third chapter continues with the outline and comparisons of the above-mentioned standards and models and their role in the development of new framework prototype.

The fourth chapter of the thesis focuses on analyzing existing applications and models in the field of risk assessment in information security. I introduced several models while in particular I presented FAIR, Octave, CURF and CRAMM models. In this chapter, I compared these models based on an online review and their use in practice. The comparision highlighted the gaps of each of the applications. These gaps provided important input to the development of my own framework and solution for risk management.

The fifth chaper deals with research overview, research questions, methodology and research design. The methodology used is described in detail and is relevant to the research questions and the topic of the thesis. The methodology also provides those theoretical principles that lead to a specific research approach to the study of a problem.

The nature of the research required a combined research strategy.

In the sixth chapter I explained the need identification survey though which I investigated the current level of the security and practice in three sectors: ICT Industry, banking sector and insurance companies. I selected the above-mentioned sectors because of the importance of the data that they possess and handle during their work. Besides this, we must take into consideration the ICT sector deals with data from the source code of their applications and the importance of their storage is huge, while the banking and insurance companies mainly deal with personal and financial data which are considered to be very important.

In the seventh chapter I have detailed the proposed Risk Assessment Maturity Framework and prototype which is based on the results of the gap analysis of the current frameworks (detailed in chapter 4). In this chapter I have created a mapping table which helps the reader to understand the link between the information security controls and common vulnerabilities scoring system.

In eights chapter I have followed with the process of validation in order to make it more accurate and functional. I have created five scenarios and I developed the Technological Acceptance Model for my risk assessment solution. The last chapter is summarizing the overall research work with findings and recommendations.

I.2 Objectives and Main Questions of the Research

The main research goal is to provide a new framework for a maturity model in the field of security risk assessment. The new framework supports the enterprises analyzing their security maturity level and is based on the ISO 27001 but also could be further utilized with the related standards. As part of the research, I have developed a questionnaire with organizations' experts to identify the current level of security in the above-mentioned sectors. The survey was filled in by organizations from the banking sector, IT industry and insurance organizations and shows a significant difference between sectors in the risk assessment practice.

The study is aimed to propose a risk assessment framework and a related workflow that can be automated for the organization to create a report and evaluate the security risks. The proposed framework is intended to utilize the model of ISO 27001 and its technical implementations for the current study. The objective of the study is to analyze the assessment methods of vulnerability in information security and to propose an effective model after analyzing the existing maturity models. My research is based on the evaluation of four maturity model frameworks i.e. ISM3 (Information Security Management Maturity Model), SSE-CMM (System Security Engineering Capability Maturity Model), COBIT Maturity Model and NIST Maturity Model. The gaps in the current maturity models identified through the literature review are such as the price of implementation because of the commercial standards (ISO 27001 and ISM3) (Stevanovic, 2011), then lack of customization and the attempt to implement one-size fits all standard through which small organizations faces difficulties because there are processes which are not used on organization and also the period of implementation which takes long time because of many administration procedures until the final implementation (NIST, ISO 27001, SSE-CMM) (Becker *et al.*, 2010).

According to these research challenges, this study posits and answers the following research questions:

Main Research Question: How can we develop the semi-automatic risk assessment system? How risk assessment systems can be extended to provide a list of recommendations by identifying the list of areas with a lack of suitable security measures through an automated risk or semi-automated assessment solution?

For the mentioned research question, a software application is developed that will apply semi-automated information security risk assessment method that will compile a list of recommendations from the assessment findings **(Chapter 7 – Risk Assessment Maturity Framework Prototype)**. The system prototype is created based on the findings from the literature, comparison of maturity models and interviews with individuals of the companies from IT sector, banking sector and insurance companies.

Sub-question 1 (followed by Main Research Question): How is the risk assessment process in the context of the information security management systems' implementation handled within the organizations (specifically on IT sector, banking sector and insurance companies)? What are the key elements of the maturity framework in the field of risk assessment, how can it be described conceptually?

For answering this question, I performed a survey and have interviews to explore how organizations implement information security management systems. Discussion of the answer for this sub-question is available in **chapter 6**. The survey is based on ISO 27001, because that is the main standard of information security management. The other three maturity models, which I reviewed, are counted as well.

Respective factors reviewed i.e. what standard is used, how effective is the usage, and how they determine the level of risk within the organization? Also, at this point, I have reviewed the part of the controls that are applicable in each sector. The questionnaire is divided into several groups of controls, from the ISO 27001, which are analyzed by the control group and the sectors, where after a detailed analysis my aim is to identify the most important controls for each sector, and simultaneously identifying problems and gaps of the mistakes that exist between the sectors.

Sub-question 2 (followed by Main Research Question): How can we map the findings of the risk assessment process for the information security maturity models?

To answer this question, interviews are conducted from the participants employed for the study and data were collected from organizations of IT, banking and insurance. Result of this phase is a conceptual model of the semi-automated risk assessment system describing the information security maturity levels, I detail it in **chapter 7.1**.

I have developed the framework prototype to determine the level of maturity within the organizations **(see chapter 7)**. My framework will not provide only the general maturity about the organization, but also maturity for each sector such according to the information security control objectives of the ISO 27001.

My approach combined ISO 27001 Control Objectives and Common Vulnerability Scoring System in order to offer a unique solution on measuring information security maturity level for the above-mentioned sectors.

Sub-question 3 (followed by Main Research Question): Is it possible to measure the maturity of the risk management practices within a company through a semi-automated risk assessment system according to the literature?

To answer of this research question, first the relevant literature describing the digital maturity models in the context of information security have been reviewed (**see Chapter 3**). In most cases, automated processes have been used mainly by the audit firms. However, the different organizations are represented in the same way as the standardization models are, and the processes are the same as the ones that are in the aspect of time, as well as the financial aspect. A survey was be used in order to identify the customized model needs of auditors in **Chapter 6.**

After a detailed analysis of the literature and the feedback from the survey, the most appropriate approaches are listed that made easy to use and efficient for the identification of audit findings within organizations' systems.

II. METHOD OF THE RESEARCH

In reviewing my thesis research methodology in the process of writing this thesis and carrying out research, I had to follow the pattern of traditional research methodologies which is the requirement of the PhD School as well as explored models to perform the research in the domain of computing. A complete research process in solvable tasks has been defined in this thesis and these tasks are time depended and measurable. In order to achieve these solvable tasks, I had to define the problem statement and research questions instead of devising hypothesis.

The Business Informatics Ph.D. School of Budapest Corvinus University belongs to the doctoral schools of social sciences in the university and has been classified to the IT disciplines well, therefore applying research methods in a kind of ‘hybrid’ way can hopefully be considered to be accepted.

II.1 Proposed Research Methodology

In the process of articulation of research methodology for the study, the design science research method has been adopted. It is a problem-solving approach that has its origins in the engineering disciplines. The design science research combines ideas, practices, technical skills and products (design artifacts) that make the analysis, design, implementation, management and use of information systems more effective and efficient (Hevner *et al.*, 2004). This approach fits on my proposed framework which combines the engineering disciplines but also is based on the existing theories and standards applies on information security. So, the design science research method helped me to make possible the development of my Framework prototype based on scientific and practical criteria's. I perform this research method through the mixed strategy, combining qualitative and quantitative approaches. Data gathering methods include the information obtained from the questionnaire, direct interviews, and literature review. My research strategy is considered as strategy that fits to business informatics field and sometimes it is considers as new discipline. Another important issue on the design science methodology is combining the creation and evaluation of the artifacts to solve and organizational problem, which in my case will be the need for a semi-automated framework in order to measure the level of information security risk in organizations. The artifact represented in my research is the web-based application framework developed. I followed strictly the Design Science Research Model and the process model to present my work in the following steps:

- **Identify Problem & Motivate:**
- **Define Objectives of a Solution**
- **Design & Development**
- **Demonstration & Data Analysis**
- **Evaluation**
- **Communication**

III. THE PROPOSED FRAMEWORK PROTOTYPE

The proposed Risk Assessment Maturity framework is based on the result of the gap analysis of the current frameworks such as Fair, OCTAVE and CRAMM (detailed in chapter 4 of the thesis).

The unique feature of the proposed framework is, that it combines ISO 27001 controls and control objectives with the Common Vulnerability Scoring System. In the framework development, I analyzed each of the control objectives and compared them to the relevant CVSS Scoring Model.

With the help of quantitative and qualitative data analysis and through the identification of gaps in the literature, a software application was developed which applied semi-automated information security risk assessment method after the compilation of recommendations from analytical findings. The development of the software application prototype is the achievement of main research question which states, “How can a risk assessment system be extended to provide a list of recommendations by identifying the list of areas with a lack of suitable security measures through an automated risk or semi-automated assessment solution?” The system prototype is developed on the basis of the findings from the literature, comparison of maturity models, and analytical findings from the quantitative and qualitative data collected from sample participants from companies of IT, banking and insurance sector. The proposed software is the result of comparisons made among the existing models in service sector practices as well as the academic researches.

The software is a web-based application developed on PHP programming language and the database will be based on MySQL. The web-based application is optimized for use on every device ranging from personal computers to smartphones with the technology of auto responsive content. This means that depending upon the resolution and the screen of the device, the software is automatically optimized. This application is user friendly and easy to navigate but the issue of less memory and internet consumption is solved by implementing the backend-oriented layout using the HTML5 and CSS3 mostly for design and very few images. On completion of the questions from the companies and organization, this system will have the opportunity to export the report generated with the recommendations. The prototype will be tested before the organizations can use the software and it will have a period as beta version during which any possible bugs or improvements will be identified.

III.1 Security risk assessment framework and its prototype

The prototype has six main components:

1. Dashboard - which presents visualizes general data and statistics

2. Companies – This section helps us to obtain general data for companies that will be subject to the questionnaire. In this section, we have two subsections, respectively the option to register a new company and the current list of the companies that are already on the system

3. Surveys – This is the main part of application because through this section we manage with questionnaires. In this section, we can add new questions

from the database, categorize questions, or even change the type of questions.

4. Assessment - In this section, we can see the list of assessments we have accomplished so far. Particularly in this section is that we can make a comparison between some assessments. For example, if Company X has conducted the Assessment in 2017 and 2018, then through the Compare Assessment option we can see the progress that the company has made in certain sections.

5. Questions – through this section, we can add new questions, modify the existing ones, or even change the form of the question.

6. Accounts - is the ultimate part that enables us to administer the system or create new users by setting the level of use. For the moment we have two types of users, respectively administrator and user simple.

This tool is designed to assist a skilled and experienced professional in ensuring that the relevant control areas of ISO / IEC 27001:2013 have been addressed.

This tool does not constitute a valid assessment, and the use of this tool does not confer ISO/IEC 27001:2013 certification. The findings here must be confirmed as part of a formal audit/assessment visit.

The application is built on web technology, as it provides easy and fast access from various devices and wherever there is Internet access. The technology used for the user-interacting look is developed with HTML, designed and stylized with CSS and Bootstrap, animations and JavaScript behaviors. To have dynamic content, to display the questionnaire etc., in the background for data manipulation is used PHP and data storage is used by the MySQL database

III.2 Framework prototype validation method

The framework prototype has been validated by companies, IT auditors and IS officers. The process of validation included the key points of the system that are relate to the following 5 key elements:

1. System usefulness
2. Time consuming on completion of assessment
3. Support Information (description of the tools)
4. Information / Report quality
5. Interface Quality (System Navigation)

The aforementioned elements have been part of the validation through the test scenarios that I have developed and distributed to the stakeholders involved on the process to test the framework prototype. Each of the 5 elements has been teste with a specific scenario, in total of 5 use case scenarios. After completing the test scenarios, the validation process has been followed by the ASQ (After-Scenario Questionnaire) model in which system users will evaluated the 5 key elements by answering 5 questions created on the Likert scale model with points 1 to 5 where 1 mean strongly disagree and 5 means strongly agree. After the user has completed the ASQ, the ASQ score is calculated by taking the average (arithmetic mean) of the 5 questions (Lewis, 1995). The ASQ method is a method developed to measure the satisfaction of using technology through questionnaires (Lewis, 1995). I determined this method based on the number of respondents I received and the simplicity of generating results that directly corresponds to our framework development model. I developed the Technology Acceptance Model (TAM) for my prototype, which helps us measure the overall ease of use (overall satisfaction of use of the system). The model suggest that I can measure two main factors namely:

Perceived ease of Use - Ease of completing tasks and the amount of time to complete tasks

Perceived usefulness - The support information

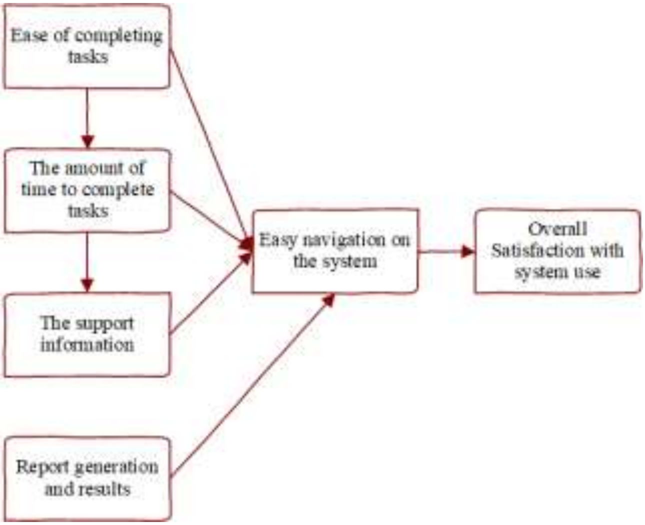
Ease of completing tasks
The amount of time to complete tasks
The support information
Report generation and results
Easy navigation on the system
Overall Satisfaction with system use

Figure 1 - Proposed TAM model for evaluation

IV. RESULTS OF THE RESEARCH, CONTRIBUTION OF THE THESIS

In the dissertation I presented a framework and solution for the information security risk assessment especially for the banking sector, insurance companies and IT industry. Through this model, I've managed to identify some of the biggest gaps that organizations have in implementing security. I could identify the points in which most organizations encounter problems, while my application will help solving these issues.

The current research offers three important contributions for the existing literature such as: 1) maintaining a counter balance and create a semi-automatic framework that would provide facilitation in the risk assessment for the organization by identification of the weaknesses that needs to be improved to bring betterment in the internal processes. This implies that, the framework which will evolve through the conduction of the current study will provide recommendation and suggestion in respect of the educational perspective and identification of the steps that may be taken to bring more work in the field. The second (2) contribution that this research will provide is the identification and similarities between the selected four information security models i.e. ISM3 (Information Security Management Maturity Model), SSE-CMM (System Security Engineering Capability Maturity Model), COBIT Maturity Model and NIST Maturity Model, ISO 27001. This will also ensure that the developed model from the current research don’t repeat any administrative or unnecessary processes. The current research will help in building a model based on the scoreboard and which is validated for functionalization and operations by the most important applications. Lastly, the third (3) contirbution is that the current research provides a unique contribution, because it combined ISO 27001 Control Objectives and Common Vulnerability Scoring System in order to offer a unique solution on measuring information security maturity level. In Kosovo, businesses and organizations need to take the issue of data attacks seriously, put measures in place and make new investments for their customers' security. They need to ensure their measures are tight and report cases of security breaches, so trust in the handling of personal information is restored.

V. REFERENCES

Becker, J. *et al.* (2010) ‘Association for Information Systems AIS Electronic Library (AISeL) Maturity Models in IS Research’, *Maturity Models in IS Research*. Available at: http://aisel.aisnet.org/ecis2010%0Ahttp://aisel.aisnet.org/ecis2010/42.

Hevner *et al.* (2004) ‘Design Science in Information Systems Research’, *MIS Quarterly*. doi: 10.2307/25148625.

Lewis, J. R. (1995) ‘IBM Computer Usability Satisfaction Questionnaires: Psychometric Evaluation and Instructions for Use’, *International Journal of Human-Computer Interaction*. doi: 10.1080/10447319509526110.

Stevanovi, B. (2011) ‘Maturity Models in Information Security’, *International Journal of Information and Communication Technology Research*, 1(2), pp. 44–47.

VI. REFERENCES OF THE AUTHOR

B Abazi, A Kő (2019)
Semi-automated information security risk assessment framework for analyzing enterprises security maturity level. CONFENIS 2019 International Conference on Research and Practical Issues of Enterprise Information Systems, **Lecture Notes in Business Information Processing**

A Luma, B Abazi (2019)
The Importance of Integration of Information Security Management Systemes (ISMS) to the Organization's Enterprise Information System. 42nd International Convention on Information and Communication Technology – **IEEE Conference**

Blerton Abazi, Besnik Qehaja, Edmond Hajrizi (2019)
Application of biometric models of authentication in mobile equipment 19th IFAC Conference on Technology, Culture and International Stability TECIS 2019

Besnik Qehaja, Blerton Abazi, Edmond Hajrizi (2019)
Enterprise Technology Architecture solution for eHealth System and implementation Strategy
19th IFAC Conference on Technology, Culture and International Stability TECIS 2019

B Abazi, E Hajrizi (2018)
Research on the importance of training and professional certification in the field of ICT Case Study in Kosovo. IFAC-PapersOnLine 51 (30), 336-339

A Luma, B Selimi, B Abazi (2018)
Registration and Authentication Cryptosystem Using the Pentor and UltraPentor Operators. International Conference on Engineering Technologies, 97-101

A Luma, B Abazi, B Selimi, M Hamiti (2018)
Comparison of Maturity Model frameworks in Information Security and their implementation. International Conference on Engineering Technologies, 102-104

B Abazi (2018)
An approach to Information Security for SMEs based on the Resource-Based View theory International Journal of Business and Technology 6 (3), 1-5

Abazi, B. (2016)
An approach to the impact of transformation from the traditional use of ICT to the Internet of Things: How smart solutions can transform SMEs. IFAC-PapersOnLine, 49(29), 148-151.

B Abazi (2016)
The adoption of Free/Open Source CRM software to SME-s An approach to low cost oriented solutions. 5th International Conference on Information Systems and Security

B Abazi (2016)
The implications of Information security to the Internet of Things. JOURNAL OF NATURAL SCIENCES AND MATHEMATICS OF UT (JNSM) 3 (2), 86-90