# Semi-automated Information Security Risk Assessment Framework for Analyzing Enterprises Security Maturity Level

Blerton Abazi, Andrea Kő

# Semi-automated information security risk assessment framework for analyzing enterprises security maturity level

Blerton Abazi[1][0000-0002-8434-0648] and Andrea Kő[2][0000-0003-0023-1143]

[1,] University for Business and Technology UBT, Prishtina Kosovo
blerton.abazi@ubt-uni.net
[2] Corvinus University of Budapest, Hungary
andrea.ko@uni-corvinus.hu

**Abstract.** While organizations spend millions of dollars on developing security systems at the highest level, one of the most significant areas of weaknesses, and loss remain their employees. Lack of employee training and security expertise, therefore, can cause huge loss, despite other measure being put in place. Cyberattacks are often able to commit cybercrime due to a lack of qualified cyber-security staff and the limited number of IT staff employed to keep pace with continuing security development and advancement. Testing, training and employing staff therefore is a critical measure for all organizations to reduce the vulnerabilities yet seems to be an area still not fully addressed. Businesses and organizations need to provide training to promote understanding for staff at every level, so they are aware of their roles and responsibilities in protecting against security threats. However, this is a colossal undertaking, and until this learning gap is resolved, financial institutions must continue to fight and efficiently manage cybersecurity threats. The aim of the current research paper is to present and propose a semi-automated risk assessment framework and a security maturity model, which can be helpful for auditors, security officers and managers. It is based on the ISO 27001 and utilize the relevant standards as well. The related risk management solution is a web-based software application. The current study targeted information security in Kosovo, specifically in the banking sector, IT industry and insurance field.

**Keywords:** information security and privacy, risk assessment, enterprises, ISO 27001

## 1 Introduction

The violation of information and data breaches is not a new concept and did not first emerge when companies began to convert their protected data digitally. Violations have existed as long as individual, companies or organizations have kept any data, or stored private information. For example, paper-based medical files could be easily shared without authorization and sensitive documents not correctly stored. At these times, many businesses and organizations did not have policies and procedures in place to protect individuals and guide employees in the safe handling of data. According to De

Groot [1] publicly disclosed data breaches increased dramatically in the 1980s, 1990s, and in the early 2000s when public awareness of the potential for data breaches began to grow. The bulk of information regarding data breaches focuses on the period from 2005 to the present day. This is mainly due to the advancement of technology and the spread of electronic data across the globe. The result of this is the threat of data attack regarded as a significant concern for organizations, companies and consumers. Due to the advancement of technology, a violation on today's information can impact on hundreds of thousands, if not millions of individual consumers and even more personal data, all from a single attack on a company. By 2020, over one-third of all data will be stored or pass through the cloud. In 2020, data production is estimated to be forty-four times higher than that in 2009 while experts estimate a four thousand and three hundred percent increase in annual data production by 2020 [1]. While individuals are responsible for the majority of data creation (around seventy percent),eighty percent of all data is stored by companies [1]. Security experts always try to keep up with the changes over time, but with fast-changing technology, it is impossible without external aid as a "third party" to help improving future security.

**Table 1.** Data violations over three years [1]

| Year | Number of records compromised | Violations that are made public |
|---|---|---|
| **2016** | 4,814,941,681 | 823 |
| **2017** | 2,051,572,640 | 853 |
| **2018** | 1,038,130,252 | 699 |
| **Total** | 7,904,644,573 | 2,375 |

In 2005, only one hundred and thirty-six data breaches were reported by the Privacy Rights Clearinghouse. However, more than 8,908 data breaches have been made public since 2005, with more than 11,239,817,282 individual data having been violated up until 2018. In the last three years alone, there have been 7,904,644,573 data breaches, showing a comparatively high value compared to previous years. However, it is essential to note the Privacy Rights Clearinghouse only reports the offenses where the number of documents violated is unknown. Therefore, these figures are not a comprehensive summary of all data violations, with the total violated data likely to be much higher. When it comes to information security and data breaches, the financial aspect of the information must also be considered. Thus, according to the latest IBM and Ponemon Institute report [2], the cost associated with data attacks has increased dramatically since 2013. In the United States, the attack price on data is estimated to average $7.35 million, whereas, worldwide, this attack price is $ 3.62 million on average according to Ponemon Institute [2]. These reported costs data are for the financial year 2017, and a significant increase is further seen according to the 2018 report. It is estimated that the cost has also increased to $ 3.9 million in attack data.

Given these consequences, each business or organization must take the necessary measures to protect itself from such cyber-attacks, improve risk assessment practice.

The aim of this paper is to present and propose a semi-automated risk assessment framework, which can be applied by IT auditors to prepare a security risk assessment report

and by the enterprises to analyze their maturity level in the field of security risk assessment. The framework is based on the ISO 27001 and utilize the related standards. The related risk management solution is a web-based software application and will be validated by companies from banks, IT and insurance companies.

## 2 Literature Review

### 2.1 Information Security Management System and its Integration to the Organization

Diversity of opinions and factors influencing the process of IT adaption to information security needs is emphasized in many papers [3]. The literature has identified several factors affecting this process, and most of them have listed factors such as senior management, government, IT consultants and organizational behavior [4]. Organizations are often affected by the models and standards that are implemented on information security within the same industry, but not all the models and standards are implemented in the same way. For small organizations that operate with small staff and which distribute information with key staff only, the implementation of information security does not seem to be a necessary option. However, companies where information is distributed to more people simultaneously, it is impossible to manage them without a proper system, thus, presenting the problem of data vulnerability. The third group of organizations is on where the main product is information [5].

Information Security Management System is defined by ISO 27001 as a set of policies and procedures for systematically managing an organization's sensitive data. The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach. Organizations have different approaches when deciding to implement an information security system. Some organizations see information security systems as a competitive edge in the market that can provide them with greater credibility in their client relationship, as well as an increase of credibility in their organization and products. Another group of organizations implement information security systems only when they see that their competitors are operating in the same way. The aforementioned views create cultural diversity within organizations of the same industry, and no doubt enables them to improve.

### 2.2 Maturity Models

To ensure security, it is essential to build security in both design phases and adaptation of a security architecture that provides that security rules and connections are set up accurately. Security requirements must relate to business goals through a process-oriented to access. The process should consider many of the factors that affect an organization's goals. There are at least four areas that affect security in an organization. First, governance organizations are a factor that affects the security of an organization. Second, organizational culture affects the implementation of security changes in the organ-

ization. Thirdly, system architecture may pose challenges for enforcing security requirements. Finally, service management is considered as a challenging implementation process. To identify and explore the strength and weaknesses of an organization's security, several maturity models have been developed [6].

We identified several maturity models for risk assessment in information security that could be adapted and implemented in any organization [7]. Large organizations usually have in place several risk assessments processes at the same time. Those risk assessment processes are decentralized from management and led by departments. For this reason, the need to create a centralized system of risk assessment across different processes and in this case, in the field of information security is necessary. The centralization of the process enables the creation of more accurate reports through which potential threats and vulnerabilities within our system can be identified. To evaluate the security of information, various developments have been seen through mechanisms that are adapted from the recognized engineering field. One of these mechanisms is the measurement of information security through the maturity process [8] and based on this maturity process and to elaborate the concepts of information security maturity, three maturity models have been analyzed, respectively: ISM3 (Information Security Management Maturity Model), SSE-CMM (System Security Engineering Capability Maturity Model), COBIT Maturity Model and NIST Maturity Model. Although the aim and scope of coverage for maturity appraisal differ, maturity models are process-oriented standards, which are based on maturity levels. Processes adhere to a quality standard for each maturity level while documenting and document management is required to ensure that the selected processes comply with the standard. The most popular maturity model is Software Engineering Institute's (SEI) Capability Maturity Model (CMM) for software development and the successor Capability Maturity Model Integration (CMMI) [9]. There are several risk assessment systems which help the companies, but these are usually not dedicated for an audit report preparation and they do not provide recommendations according to the risk assessment results. According to the literature [10], there is a gap between the implementation of the information security standards in business sector needs and objectives of the standards.

To determine a maturity level through a risk assessment process [11] influenced the improvement of preconceptions about information security domination as a discipline where "security should be a process rather than a product". Schneier [11] describes this process as a must to understand all the real threats to the system, and by creating security policies tailored to existing threats, through easier mechanisms for data protection can be developed. Maturity models are considered as a standardized approach on driving activities, processes and commitment to the desired destination and goals [12]. In recent years, many maturity models have been developed, with the same aim to improve processes.

## 3 Information Security Risk Assessment

As part of the risk management structure, risk assessment process identifies and evaluates the risk to information security by determining the probability of occurrence and

the resulting impact [13]. Through the risk assessment process, it is possible to identify threats, classify assets and rate the system vulnerabilities, which support effective implementation of controls [14]. According to literature, we can separate risk assessment models into quantitative and qualitative. Quantitative models are those which are based on measurable data to determine the asset value and associated risk to calculate objective numeric values for each of the components that are collected during the risk assessment process. Qualitative methods are based mostly on the descriptive categories such as low, medium, high, or any other method of scaling. This method assesses the impact of the likelihood of the identified risk [14]. Both methods have their advantages and disadvantages to risk management approach, which also depends on the size of organizations. Organizations usually try to adopt the quantitative methods, because it is more easily measurable, but small-sized organizations with limited resources may decide to use qualitative approach as the best methods for their needs.

The deliverable from a qualitative assessment should be a report of which assets and systems are most important to various parts of the business. The assessment team won't necessarily know the financial impact of these systems were compromised, but they will understand which business units would be affected and how much productivity would be lost in different risk scenarios. Additionally, the assessor would understand the impact to the company's reputation and any PR considerations if a risk were realized and became publicly known. When developing the information security risk assessment methodology for an organization, it's essential to realize that both quantitative and qualitative analyses are needed for a well-rounded view on risk management process. Risk management processes require not only understanding impact but creating a risk management framework that sets the acceptable level of risk to enable functioning business operations.

The advancement and complexity of technological networks create opportunities for more attacks and breaches into security systems, causing large direct and side damage such as financial loss, reputation damage, etc. [15]. Adding this to the need for a proper data protection strategy in an organization, information security management is one of the most important area. While organizations are offering their clients access to multiple information systems, the possibility of security threats are growing, and the need to have secure systems gets special and important emphasis [16]. While many researchers and organizations deal with the issue of information security mainly in the technical aspect, respectively its integration into corporate governance, non-technical issues are rarely considered as one of the issues to be included in business strategies [17].

Most of the security information "shakes" are caused by incidents inside the organization, which means that the internal staff is identified as the first and most security threat to information security [18, 19]. Increasing the need for more secure systems and the need for our data to be handled with the utmost security is that the information security study surpasses the technology gap by increasing awareness of the role of management in data security [20, 21]. Also, given the fact that security information systems development is not enough to stop attacks and damages to information, an effective information security system that includes policies and a robust review of information security policies are key factors for a good protection [22]. As a result, management's

role is more focused on the development and execution of information protection policies, training delivery, investment in information infrastructure development and business and IT alignment [23].

### 3.1 Semi-Automated Risk Assessment Solutions

Organizations have a broad set of security requirements. Organizations security and information security management is built from a complex interconnection between business objectives, IT strategy, institutional arrangements and requirements [24] . According to our current research conducted with organizations in Kosovo, completing these requirements is a waste of time and the likelihood of error is large because organizations lack digital, automatic or semi-automatic processes to perform tasks related to information security management. The risk assessment process should be related to what we want to measure, and, in this section, we can interconnect the part of the security controls that we want to evaluate through the risk assessment. Based on the ISO 27001 specification, a total of 133 security controls represent all the areas for information security management. However, not all can be automated through certain tools. A security-control is automated if it can perform the required operations without human intervention in the process. This implies that the best way to automate security controls is through semi-automation. According to Montesino and Fenz [24] and based on the criteria outlined by them, the identification of semi-automated controls can be made through the following criteria:

- Actions and monitoring of audits require only readable and process able resources that cannot be considered as potential training to understand the need to look at and interact with the human factor
- Controls can be automated using one of the relevant security applications.

## 4 Research Overview

This study aims to propose a risk assessment framework and a related workflow that can be utilized in a semi-automated way in the organization to create an audit report and evaluate security risks. The proposed framework is intended to utilize the model of ISO 27001 and its technical implementations. 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.

Our research is based on the evaluation of four maturity model frameworks i.e. ISM3, SSE-CMM, 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 such as ISO 27001 and ISM3 [25]. Another issue is the lack of customization and the attempt to implement one-size fits all standard through which small organizations faces difficulties. In these organizations there are processes offered by the standards which are not used and also the period of implementation takes long time due to many administration procedures until the final

implementation (NIST, ISO 27001, SSE-CMM) [26]. More issues mentioned in literature review, includes the lack of guidance and complex structures of implementation in a case of COBIT 5, while the number of case studies is limited [27].

Additionally, we collected information about the gaps through surveys at the investigated companies in Kosovo. 70 IT managers filled in it mainly from banks and insurance companies in Kosovo. We distributed the survey to all organizations in the region, and got back responses from all of them. Our risk assessment framework was developed using the information gathered in gap analysis based on the survey results. The framework took ISO 27001 as a main framework and the focus is on technical parts of the framework rather than the documentation process. The currently prevailing IT risk management approaches as a good example witnessed through the literature. It is necessary for risk professionals and auditors to have a maturity model through which they can check if the investigated risk management practice meets with the expectations and produce the required results. Many risk management programs have built on risk maturity model which can be broken down into many other sections focusing on core attributes [28]. Recently, there is an increased interest for the maturity models in the research community and its practical implications [29]. In this regard, the current research will try to find the answer for the following research questions:

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 above-mentioned research questions, we developed a software application that apply semi-automated information security risk assessment method and compile a list of recommendations from the assessment findings. The system prototype was 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.

## 5 Risk Assessment Maturity Framework Prototype

With the help of quantitative and qualitative data analysis and through the identification of gaps in the literature, a software application was developed which apply semi-automated information security risk assessment method after the compilation of recommendations from analytical findings. The system prototype is based on the literary findings, comparison of maturity models, and analytical findings from the quantitative and qualitative data collected from participants from companies of IT, banking and insurance sector. Based on studies on risk assessment in information security, we have a wide range of models used in identification, assessment and risk analysis processes: FAIR, OCTAVE, CURF, CRAMM, CORAS, RISK IT, however they have several shortcomings [30].

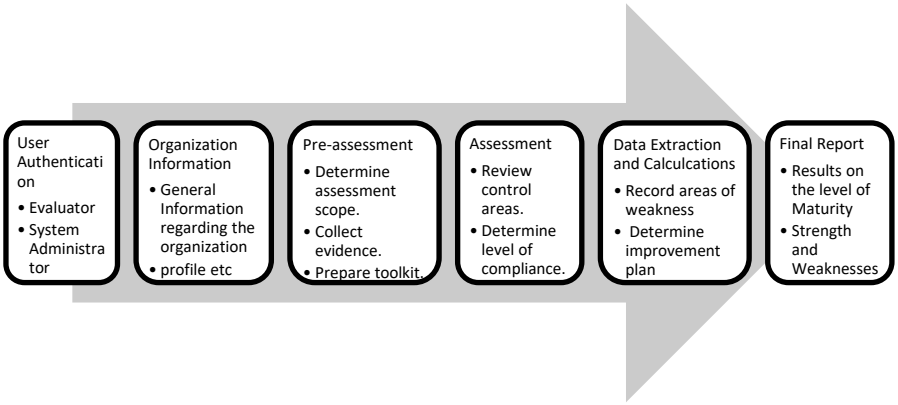


**Fig. 1.** - Risk Assessment Framework - Functional Design

The software is a web-based application developed in PHP programming language and the database is 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 application aims to be user friendly and easy to navigate but the issue of less memory and internet consumption will be 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 has a report generation with the recommendations function.

The current proposal forwards a framework which is more user-friendly easy to be used and adaptable to develop any risk assessment questionnaire. The application is made up of several blocks that represent the respective functions as well as are interconnected with other parts of the system. This is an incremental and iterative development that is implemented as a new concept and is in line with the idea of the on-the-job development. Characteristics of the framework are defined on two levels. The overall level definition establishes the foundation and framework; it indicates particularities and critical issues that need special attention. The detailed level specification defines requirements with full particulars. These documents are prepared simultaneously for the present one. Specifically, the database design will seek to:

- Minimize data redundancy meaning information is not duplicated in several places making it hard to maintain
- Provide easy access to the data including the ability to handle ad-hoc queries
- Provide security for the data
- Allow constraints that ensure data integrity.

Until now the following sections are functioning:
**Companies profile**: This section helps us to obtain data for company profiles (industry, number of employees, annual turnover etc.) subject to the questionnaire.

**Surveys**: This is the main part of application; through this section questionnaires can be managed. In this section, we can add new questions from the database, categorize questions, or even change the type of the questions.
**Assessment**: In this section we can see the list of assessments we have conducted so far. Particularly in this section we can make a comparison between different assessments for the same company. 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.
**Dashboard**: presents visualized data and statistics
**Questions**: through this section we can add new questions, modify the existing ones, or even change the form of the question.
**Accounts:** Is the administration and configuration part that enables us to administer the system by create new users or adding specific roles to the existing users

### 5.1 Vulnerabilities Rating System

To have a qualitative information security risk assessment, we must provide a scoring metric which will be separated for different security controls, this vulnerability rating system is the backend of the proposed solution. The results generated by our proposed framework will be based on a system of estimation of the probabilities that will be calculated in the backend. This system is designed to provide organizations with a better understanding of which identified high-priority vulnerabilities need to be closed. In our research we have analyzed the CVSS (Common Vulnerability Scoring System) which is a risk assessment solution designed to identify the common attributes of several security issues. The reason we choose to analyze CVSS is that it includes standardized vulnerability score that may be meaningful across organization and also it is essential that CVSS is an open framework model and any metric is open and available to all users while also it helps organizations to prioritize the risk. According to the structure and function of CVSS and as well based on our proposed framework, we have created a score-based model 1 to 5 as follows:

**Table 2.** Risk Assessment Proposed Scoring Model

| Level | Score |
|---|---|
| Min Level | 1 |
| Min-mid Level | 2 |
| Mid-Level | 3 |
| Mid-Max Level | 4 |
| Max Level | 5 |

Each of the security control groups have a summarization of their result based on the user selections. The resulting score serves to guide the affected organization in the allocation of resources to address the vulnerability. The higher the severity rating, the more significant the potential impact of an exploit and the higher the urgency in addressing the vulnerability. While not as precise as the numeric CVSS scores, the qualitative labels are very useful for communicating with stakeholders who are unable to relate to the numeric scores.

In the dashboard of the system, statistics present the number of companies that have carried out the risk assessment, the number of questions, how many questionnaires have been conducted and how many questions have been answered are displayed. Further statistics are visualized on the dashboard, such as the most frequent answers, the most prevalent security issues from all questionnaires and so on. Companies can place themselves in this risk assessment landscape, and they get feedback about the fields need improvements from controls aspects.

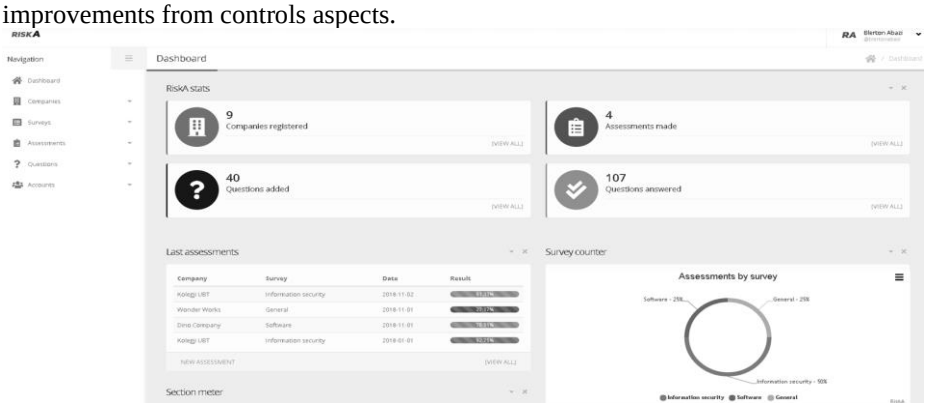


**Fig. 2.** System Dashboard

## 6 Conclusion

In this research paper we presented an approach, model and solution for the information security risk assessment especially for the banking sector, insurance companies and IT industry in Kosovo. This framework can be helpful for auditors, security officers and managers in the investigation of their companies' security maturity level. The model is based on the ISO 27001 and utilize the relevant standards as well. The related risk management solution is a web-based software application, which we presented in section 5. The framework supports the identification some of the biggest gaps that organizations have in security implementation. The use of the questionnaire in the system helped to identify exactly the points in which most organizations encounter problems, while the application helps solving these problems through offering the appropriate controls at the lowest cost. While the dependence of people on different platforms is on the rise, the risk this data will be exposed is likely to increase.

Thus, research data reflects an interesting, current state of information protection. A growing number of companies continue to feel threatened by cyberattacks, and the media frequently report attacks on data being made for larger companies such as Facebook and Google. The more in-depth analysis of these two companies has reflected that regardless of the value of the company, each company continues to struggle with security risks. Therefore, in addition to the above-mentioned risks of data destructions, companies need to consider the reality that such attacks can happen. It is imperative that every company with an online presence considers the need to protect their data, whether due to the protection of the business or its users. Finally, management support plays an essential role in the success of IS. It has been shown the need for management to make

a risk-based decision and support the goals of IS, for it to be successful in the long-term. The current study targeted information security in Kosovo, specifically in the banking sector, IT industry and insurance field, where businesses and organizations face several risks from a range of threat types. Next phase of the research is dedicated to the prototype testing and fine-tuning of the system.

## References


1. Groot, J. De: The History of Data Breaches, https://digitalguardian.com/blog/history-data-breaches
2. Institute, P.: 2018 Cost of Data Breach Study, Global Overview. (2018)
3. Businge, J., Serebrenik, A., van den Brand, M.: An Empirical Study of the Evolution of Eclipse Third-party Plug-ins. In: Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE). pp. 63–72. ACM, New York, NY, USA (2010)
4. Joshi, A., Bollen, L., Hassink, H., De Haes, S., Van Grembergen, W.: Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role. Inf. Manag. 0–1 (2017). https://doi.org/10.1016/j.im.2017.09.003
5. Burgeois, D.T.: Information Systems for Business and Beyond. (2014)
6. Talabis, M., Martin, J.: Information Security Risk Assessment: Risk Assessment. (2012)
7. Ge, X.Y., Yuan, Y.Q., Lu, L.L.: An information security maturity evaluation mode. Procedia Eng. 24, 335–339 (2011). https://doi.org/10.1016/j.proeng.2011.11.2652
8. Dzazali, S., Zolait, A.H.: Assessment of information security maturity: An exploration study of Malaysian public service organizations. J. Syst. Inf. Technol. 14, 23–57 (2012). https://doi.org/10.1108/13287261211221128
9. Poeppelbuss, J., Niehaves, B., Simons, A., Becker, J.: Maturity Models in Information Systems Research: Literature Search and Analysis. Commun. Assoc. Inf. Syst. 29, 506–532 (2011)
10. Von Solms, B., Von Solms, R.: From information security to...business security? Comput. Secur. 24, 271–273 (2005). https://doi.org/10.1016/j.cose.2005.04.004
11. Schneier, B.: Secrets and Lies: Digital Security in a Networked World. (2004)
12. Ngwum, N.I.: Information Security Maturity Model ( ISMM ) Information Security Maturity Model A dissertation submitted to The University of Manchester. 1–136 (2016). https://doi.org/10.13140/RG.2.1.2432.8729
13. Nazareth, D., Choi, J.: Information Security Management: A System Dynamics Approach. In: Americas Conference on Information Systems (2012)
14. Macedo, F.N.R.: Models for Assessing Information Security Risk. 1–64 (2009)
15. Hu, Q., Hart, P., Cooke, D.: The Role of External and Internal Influences on Information Systems Security - a Neo-institutional Perspective. J. Strateg. Inf.

Syst. 16, 153–172 (2007). https://doi.org/10.1016/j.jsis.2007.05.004
16. Nazareth, D.L., Choi, J.: A system dynamics model for information security management. Inf. Manag. 52, 123–134 (2015). https://doi.org/10.1016/j.im.2014.10.009
17. Lapke, M., Dhillon, G.: A semantic analysis of security policy formulation and implementation: A case study. In: Association for Information Systems - 12th Americas Conference On Information Systems, AMCIS 2006 (2006)
18. Gaunt, N.: Practical approaches to creating a security culture. Int. J. Med. Inform. 60, 151—157 (2000). https://doi.org/10.1016/s1386-5056(00)00115-5
19. Singh, A.N., Picot, A., Kranz, J., Gupta, M.P., Ojha, A.: Information Security Management (ISM) practices: Lessons from select cases from India and Germany. Glob. J. Flex. Syst. Manag. (2013). https://doi.org/10.1007/s40171-013-0047-4
20. Stine, K., Barker, W.C., Gulick, J.: Volume I : Guide for Mapping Types of Information and Information Systems to Security Categories. I, (2008)
21. Soomro, Z.A., Shah, M.H., Ahmed, J.: Information security management needs more holistic approach: A literature review. Int. J. Inf. Manage. 36, 215–225 (2016). https://doi.org/10.1016/j.ijinfomgt.2015.11.009
22. Diver, S.: Information Security Policy - A Development Guide for Large and Small Companies. Inf. Secur. SANS Inst. (2007)
23. Radack, S., Kuhn, D.: Managing Security: The Security Content Automation Protocol. IT Prof. 13, 9–11 (2011). https://doi.org/10.1109/MITP.2011.11
24. Montesino, R., Fenz, S.: Automation possibilities in information security management. Proc. - 2011 Eur. Intell. Secur. Informatics Conf. EISIC 2011. 259–262 (2011). https://doi.org/10.1109/EISIC.2011.39
25. Stevanovi, B.: Maturity Models in Information Security. Int. J. Inf. Commun. Technol. Res. 1, 44–47 (2011)
26. Becker, J., Niehaves, B., Poeppelbuss, J., Simons, A.: Association for Information Systems AIS Electronic Library (AISeL) Maturity Models in IS Research. Matur. Model. IS Res. (2010)
27. Zhang, S., Fever, H. Le: An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model. J. Econ. Bus. Manag. (2013). https://doi.org/10.7763/joebm.2013.v1.84
28. Sophia Wright: How Can Risk Maturity Model Benefit Your Risk Management, https://www.riskmethods.net/en/blog/How-Can-Risk-Maturity-Model-Benefit-Your-Risk-Management/112
29. Khaiata, M., Zualkernan, I.A.: A simple instrument to measure IT-Business alignment maturity. Inf. Syst. Manag. 26, 138–152 (2009). https://doi.org/10.1080/10580530902797524
30. Abazi, B.: A novel approach for a risk assessment maturity framework based on ISO 27001, (2019)