Scientific Research Publishing

Journal of Information Security, 2023, 14, 195-211
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Towards Development of a Security Risk Assessment Model for Saudi Arabian Business Environment Based on the ISO/IEC 27005 ISRM Standard

Wael G. Alheadary

College of Computer Science and Engineering, Taibah University, Medina, KSA
Email: wheadary@taibahu.edu.sa

How to cite this paper: Alheadary, W.G. (2023) Towards Development of a Security Risk Assessment Model for Saudi Arabian Business Environment Based on the ISO/IEC 27005 ISRM Standard. *Journal of Information Security*, **14**, 195-211.
https://doi.org/10.4236/jis.2023.143012

Received: April 6, 2023
Accepted: July 3, 2023
Published: July 6, 2023

Abstract

Security risk assessment refers to the process of identifying, analyzing, and evaluating potential security risks for an organization. An organization's assets, personnel, and operations are protected through it as part of a comprehensive security program. Various security assessments models have been published in the literature to protect the Saudi organization's assets, personnel, and operations. However, these models are redundant and were developed for specific purposes. Hence, the comprehensive security risk assessment model used to safeguard Saudi organizations' assets, personnel, and operations is still omitted. Using a design science methodology, the objective of this study is to develop a comprehensive security risk assessment model called CSRAM to assess security risks in Saudi Arabian organizations based on the International Organization for Standardization and the International Electrotechnical Commission/Information security risk management (ISO/IEC 27005 ISRM) standard. CSRAM is made up of six stages: threat identification, vulnerability assessment, risk analysis, risk evaluation, risk treatment, and monitoring and review of the risk. The stages have many activities and tasks that need to be accomplished at each stage. Based on the results of the validation of the completeness of the CSRAM, we can say that the CSRAM covers the whole ISO/IEC 27005 ISRM standard, and it is complete.

Keywords

Risk Assessment, Risk Analysis, Design Science Research, ISO/IEC 27005 ISRM

1. Introduction

In a security risk assessment, potential security threats or vulnerabilities are identified, analyzed, and evaluated so that the risk level can be determined, and appropriate countermeasures can be developed to mitigate or minimize these risks. Security risk assessments aim to identify and address security risks before they can cause harm or damage to the organization or its assets [1].

For organizations operating in Saudi Arabia, security risk assessment is crucial to identifying, evaluating, and mitigating security risks. Saudi organizations may encounter several challenges and issues related to security risk assessment [2] [3] [4]. **Figure 1** displays these challenges and issues.

As shown in **Figure 2**, the ISO/IEC 27005 ISRM standard presents standards for managing information security risk and enables organizations to select their own risk assessment methodology, depending on their organizational goals and risks [5]. In the article, [6] explained ISO/IEC 27005 provides an overview of the "why", "what", and "how" that an organization can use to successfully discipline its information security risks in accordance with ISO/IEC 27001 requirements.

Alternatively, digital forensics is used to detect and investigate threats in organizations. This type of forensics involves analyzing digital evidence that may include files, networks, and other forms of data [7] [8] [9] [10]. This data can be analyzed to identify malicious activities, such as hacking, malware, or other suspicious activities [11] [12] [13]. Digital forensics can also be used to recover deleted or corrupted data, as well as to track down individuals who have committed cyber-crimes [12] [14].

Thus, the purpose of this study is to develop a comprehensive model for assessing security risks in Saudi organizations based on the ISO/IEC 27005 ISRM. There are several components of developed CSRAM that can be used to identify and analyze security threats, vulnerabilities and risks in Saudi organizations and provide a comprehensive framework for doing so. Additionally, CSRAM provides organizations with recommendations and guidance on how to reduce and

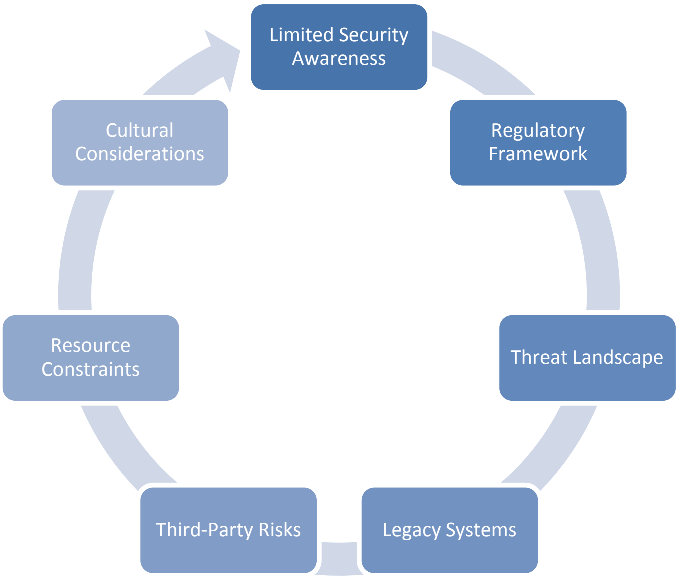

Figure 1. Challenges and issues of Saudi originations.

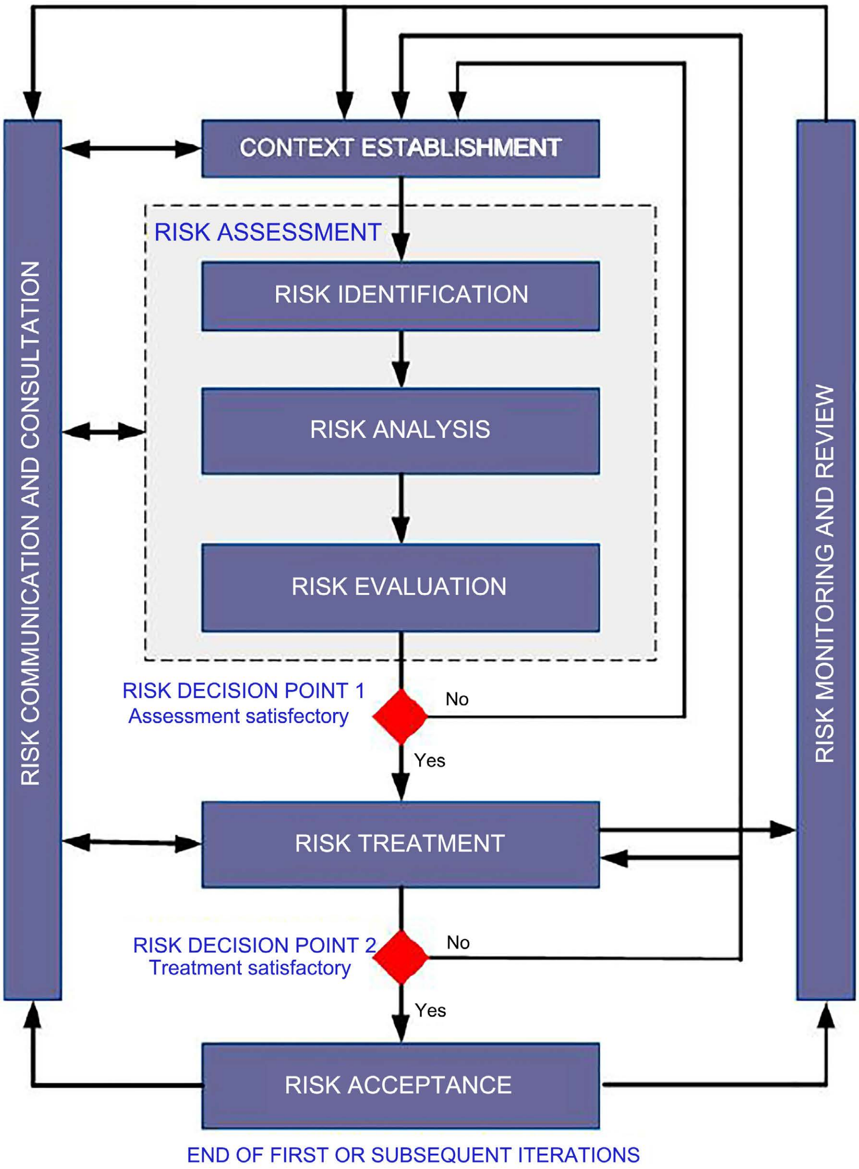

Figure 2. ISO/IEC 27005 ISRM Process [5].

mitigate identified risks and vulnerabilities by providing recommendations and guidance. In this study, researchers used design science methodology to develop the CSRAM.

This article is organized as follows: the related works are discussed in Section II, and the methodology is presented in Section III. Section IV provided the conclusion and future works for this study.

2. Related Works

Several security assessment models and framework have been proposed in the literature. For example, the authors in [15] investigated ANSI/API Security Risk Assessment methods for developing proactive security policies that respect threats. The researchers in [16] proposed a security framework which consists of four stages: risk assessment, implementation of security risk controls, monitoring and review. The researchers in [4] introduced a security risk management model for Saudi organizations. Several factors were proposed in this model such the security policies and process, the size and culture of the organizations. The authors in [17] proposed a model for communicating and implementing information security policies. They examined present information security policy progress and methods from secondary sources. This was to gain a deeper understanding of the processes critical to the development and life cycle of information security policies. As part of the proposed model, the various steps involved in developing, implementing, and evaluating an effective information security policy are described.

The authors in [18] presented an overview of information security policy administration procedures and presented a model based on exercises. It provides comprehensive guidance to experts on what actions security administrators should accept for the development of security policy, and it encourages experts to standardize their current training with the best practices recommended by the model. The authors in [19] developed a model to examine the progress of security policies in higher education institutions as part of an analysis of the security policies that have been implemented. Several security policies and procedures were proposed by them. According to [20] the AHP method can be used for assessing the security of information systems. Based on both qualitative and quantitative methods of analysis, AHP provides decision makers with robust and comprehensive treatment.

The authors in [21] proposed an ontology that will be able to support the implementation of the type of policy suggested. The authors in [22] purposed a model to examine some of the cybersecurity issues that have been faced by the Kingdom of Saudi Arabia over the last couple of years. Moreover, it discussed the concept of cybersecurity in the country and how it is being used to protect the country.

In [23] a model was proposed for exploring employee differences, as well as identifying factors that influence employee perceptions and intentions toward compliance. Using partial least square structural equation models, Saudi Arabian government organizations assessed and validated the model.

The researchers in [24] focused on internet of things in its broader sense, but then narrowed it down to IoT and its risk assessment within that domain so that a more comprehensive overview can be presented. Finally, a framework for systematizing and modularizing information security assessment for smart grids is presented by [25]. The development of an information security index system for smart grids should be informed by authoritative information security standards and the actual situation of the target system.

Additionally, several digital forensic works have been proposed to detect, and investigate the threats and risks of organizations. Organizations can use digital forensics to identify and respond to security incidents, mitigate risks, and improve their overall security posture with the help of digital forensics. Several models, frameworks, and techniques have been proposed and developed by the authors in [26]-[52] to investigate and detect cybercrime, data breaches, and other digital threats to organizations.

3. Methodology

A Design Science Research (DSR) methodology is used in this study to create the CSRAM, which is based on DSR. DSR refers to a method that could be used to create a broad range of objects related to a particular issue to be able to perform analytics on it [53] [54] Hence, this study adopts the metamodeling strategy proposed by [44] [55] [56] for the purpose of this study:

3.1. Recognizing and Choosing Security Risk Assessment Models

Security risk assessment models are identified and selected using the common search engines (e.g., IEEE Explorer, Springer, Scopus, WOS, and Google Scholar) based on the keywords "Risk Assessment", "Security Risk Assessment", "Risk Analysis" and "Risk Evaluations". Table 1 displays the common security risk assessment models which identified and selected from the literature. It is shown in Table 1 that a total of 27 models have been gathered from the literature, but only 15 of those models were considered in the risk assessment component.

An evaluation of risk refers to the process of evaluating the impact and probability of the occurrence of a possible risk or exposure. Consequently, it is necessary to evaluate the difficulty of the potential influence, the likelihood of the risk occurring, and any modifying influences that may reduce the risk. Based on the type of danger and the presented data, the risk may be evaluated qualitatively or in a variable manner. The purpose of risk evaluation is usually to identify the most significant risks and select them for further action.

3.2. Collecting and Merging Common Security Risk Assessment Components

As part of this step, the aim is to collect and merge the common components of the 20 security risk assessment models to construct a single model. Based on the semantic meanings and similarities found among the collected common components, these components will be merged into one. Table 2 displays the collected risk assessment companies from the 15-security risk assessment model.

3.3. Development Process of the CSRAM

This step is a major step towards achieving the main objective of this study. The comprehensive security risk assessment model to safeguard Saudi organizations' assets, personnel, and operations has been developed in this step. Figure 3 displays the developed CSTAM which consists of six components.

1) **Threat Identification**: Threat identification is a critical component of any security risk assessment model, including Saudi Arabian organizations. It involves identifying potential sources of security threats the organization may face.

Table 1. Security risk assessment models.

ID	Year	Ref	Risk Assessment
1	2014	[15]	☑
2	2014	[17]	☑
3	2014	[57]	☒
4	2015	[58]	☒
5	2016	[59]	☒
6	2016	[18]	☑
7	2016	[60]	☒
8	2017	[19]	☑
9	2017	[20]	☑
10	2017	[61]	☒
11	2018	[21]	☑
12	2018	[62]	☒
13	2018	[22]	☑
14	2018	[63]	☒
15	2018	[64]	☒
16	2018	[65]	☑
17	2018	[66]	☒
18	2019	[67]	☒
19	2022	[4]	☑
20	2022	[23]	☑
21	2022	[68]	☒
22	2022	[69]	☒
23	2023	[16]	☑
24	2023	[70]	☑
25	2023	[70]	☑
26	2023	[24]	☑
27	2023	[25]	☑

Table 2. Collected common security risk assessment components.

ID	Year	Ref	Focused	Collected Components
1	2014	[15]	ANSI/API Security Risk Assessment methods were examined for developing proactive security postures by using risk-based performance metrics as part of this study.	Characterization, threat assessment, vulnerability assessment, risk evaluation, risk treatment
2	2014	[17]	In this paper, the authors provided a framework for defining a model for formulating, implementing, and enforcing policies related to information security in an organization.	policy formulation, policy implementation, policy enforcement, and policy monitoring.

Continued

3	2016	[18]	Throughout the study, a comprehensive exploration of management practices of information security policy had been undertaken, and the development of a practice-based model about addressing the four deficiencies noted above was also addressed.	Establish information security policy development team, determine the security needs of the organization, compiling the security policy document, and the implementation and maintenance stage
4	2017	[19]	The purpose of this study was to propose a framework that Institutions of Higher Education can consider during the process of developing and implementing a security policy. As a result of the proposed framework, comprehensive and sustainable information security policies could be developed.	Policy Initiation, Policy Drafting, Policy Implementation, Policy Review, and Policy Maintenance
5	2017	[20]	In this study, the purpose was to examine whether Analytic Hierarchy Process (AHP) can be used as a method to support the analysis of information security decision making in Indonesian e-government systems using the Analytic Hierarchy Process.	information security; policy; decision making
6	2018	[21]	This study aimed at identifying and suggesting a formal, encoded description of the strategic environment of cyber security to establish an ontology of cyber security. In addition, it also proposed to develop an ontology that will be able to support the implementation of the kind of policy that is suggested in this study.	Cyber Security, Cyber Security Policy, Implementation
7	2018	[22]	The purpose of this chapter is to examine some of the cybersecurity issues that have been faced by the Kingdom of Saudi Arabia over the last couple of years. Moreover, it discusses the concept of cybersecurity in the country and how it is being used to protect the country.	Cybersecurity, assess threats
8	2018	[65]	It is the purpose of this study to identify how employees' attitudes toward the information security policies vary in relation to their behavior concerning information security.	Construct, Construct, Compliance, Information Security Practice Behaviors
9	2022	[4]	The purpose of this study was to examine the aspects that affect information security risk management and develop an information security risk management model for large Saudi Arabian companies.	Risk identification, risk assessment, risk control, risk monitoring and response, and risk communication
10	2022	[23]	According to this study, a model was proposed to explore employees' differences as well as identify factors that can influence their perceptions and intentions toward compliance, to identify what drives employee behavior. The model was examined and validated using partial least square structural equation models within a government organization in Saudi Arabia.	Monitoring, Measurement, Compliance, Information security controls
11	2023	[16]	The purpose of this study was to demonstrate an analysis approach based on the current awareness of information security risks in Saudi Arabian non-governmental organizations.	Information security risk assessment, implementation of security controls, monitoring, and review
12	2023	[70]	This research emphasizes the broadening attack surface for threat actors due to IoT firmware security risks. Denial-of-service and brute-force attacks, which are common in diverse smart home environments, can no longer be countered by firewall rules that prevent denial-of-service attacks or brute force attacks.	Internet of Things, Cybersecurity, Firmware, Entropy, Hardcoded, Attack Vector

Continued

13	2023	[70]	The purpose of this paper is to present a strategy for efficiently generating databases that considers the consequences of the COVID-19 outbreak. In the proposed strategy, the information content of the training set will be high, which is compatible with the operating conditions in the field.	Security assessment, Decision tree, Copula functions, Machine learning
14	2023	[24]	The focus of this paper is on IoT in its broader domain and then has been narrowed down to IoMT and its risk assessment within that domain to present a more comprehensive study.	Information security, Policy, Decision making
15	2023	[25]	This paper proposed a framework for systematizing and modularizing information security assessment for smart grids. Expand relevant security indices and develop a smart grid information security index system based on authoritative information security standards and the actual situation of the target system.	Information security assessment, Security assessment, Fuzzy theory, Smart grid

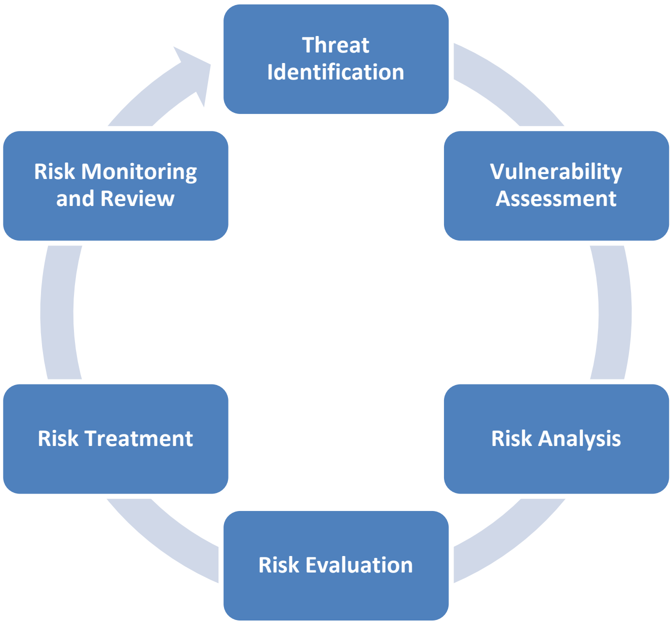

Figure 3. Comprehensive security risk assessment model (CSRAM) for Saudi organizations.

This component has several activities such as gathering data, assessing threats, prioritizing threats, establishing mitigation plan, controlling results.

2) Vulnerability Assessment: This is the second stage of CSRAM. This stage is used to evaluate and assess Saudi organizations' assets. Physical security, network security, and personnel security measures should all be reviewed as part of the vulnerability assessment process. Organization security policies and procedures should be reviewed, security audits and assessments conducted, and penetration testing performed to identify vulnerabilities. Any changes in a company's infrastructure, such as updated software or hardware, or changes in its workforce, should also be considered when conducting the assessment.

3) Risk Analysis: This is the third stage of the proposed CSRAM. In this stage, the detected risks from the second stage are analyzed. An organization's risk analysis identifies and assesses potential threats as well as vulnerabilities and weaknesses that may be exploited by these threats. Based on these results, it is possible to assess the severity of a security breach. It is also important to consider the severity of a security breach's potential impact on the organization.

4) Risk Evaluation: In the context of risk evaluation, this is the procedure of analyzing the results of the risk analysis using the risk principles to determine whether the risk and/or its degree are appropriate or not, based on the results of the risk analysis.

5) Risk Treatment: To reduce the risk of an organization, the risks are treated by means of risk-aware actions, controls, and policies to determine which Risk Mitigation methodology (to avoid, reduce, accept, and transfer) will lead to the reduction of risk to a negligible or profitable level.

6) Risk Monitoring and Review: Lastly, the final step of the proposed framework involves the monitoring of the vital components of risk management which form an essential part of the monitoring and review process. This undertaking marks the final stage of the proposed framework. The process involves monitoring and evaluating the effectiveness of risk treatment strategies on a continuous basis, thus ensuring that they are effective.

4. Results and Discussion

This section introduces the results and discussion of the study. A comprehensive security risk assessment model called CSRAM, which is based on the ISO/IEC 27005 ISRM standard, to assess security risks in Saudi Arabian organizations has been developed. It consists of six stages: threat identification, vulnerability assessment, risk analysis, risk evaluation, risk management, and monitoring and review of risks. It is important to note that each stage has several activities and tasks that need to be accomplished. For example, the first stage threat identification has several activities such as gathering data, assessing threats, prioritizing threats, establishing mitigation plan, controlling results. In the second stage of vulnerability assessment, physical security measures, network security measures, and personal security measures are evaluated. To identify vulnerabilities, security policies and procedures should be reviewed, security audits and assessments should be performed, and penetration testing should be conducted. Assessing a company's infrastructure should also consider changes to its workforce and new software or hardware. The third stage of risk analysis involves identifying and evaluating potential threats, as well as vulnerabilities and weaknesses that may be exploited by these threats to gain control over the system. The fourth stage involves gathering people's opinions through surveys, meetings, or focus groups. In addition, it is equally important to assess the danger's impact on people and the people, as well as its long-term impact on them. A fifth stage of risk management includes several activities such as avoiding, optimizing, transferring, and retaining risk so that it has as little negative impact as possible. A final stage in the process of monitoring and reviewing risks is the ongoing monitoring and evaluation of the effectiveness of the strategies implemented for risk treatment as they are being implemented as part of the monitoring and evaluation process.

The comparison between the CSRAM model and the existing model indicates that CSRAM is sufficient if compared to the existing model. For example, the characterization, threat assessment, vulnerability assessment, risk evaluation, and risk treatment processes which provided by [15] have been covered by the developed CSRAM processes as shown in **Table 3**. Also, the policy formulation, policy implementation, policy enforcement, and policy monitoring processes which introduced by [17] is totally covered by the developed CSRAM processes. A CSRAM also addressed the establishment of the information security policy development team, determining the security needs of the organization, compiling the security policy document, and the implementation and maintenance phases in [18]. Based on the same scenarios conducted for [4] [16] [19]-[25] [65] [70], the developed CSRAM covered all processes for these models from start to finish. **Table 3** compares the CSRAM with the existing studies. It's very

Table 3. Compare the CSRAM with the existing studies.

ID	Year	Ref	Existing Components	CSRAM Components
1	2014	[15]	Characterization, threat assessment, vulnerability assessment, risk evaluation, risk treatment	☑
2	2014	[17]	policy formulation, policy implementation, policy enforcement, and policy monitoring.	☑
3	2016	[18]	Establish information security policy development team, determine the security needs of the organisation, compiling the security policy document, and the implementation and maintenance stage	☑
4	2017	[19]	Policy Initiation, Policy Drafting, Policy Implementation, Policy Review, and Policy Maintenance	☑
5	2017	[20]	information security; policy; decision making	☑
6	2018	[21]	Cyber Security, Cyber Security Policy, Implementation	☑
7	2018	[22]	Cybersecurity, assess threats	☑
8	2018	[65]	Construct, Construct, Compliance, Information Security Practice Behaviours	☑
9	2022	[4]	Risk identification, risk assessment, risk control, risk monitoring and response, and risk communication	☑
10	2022	[23]	Monitoring, Measurement, Compliance, Information security controls	☑
11	2023	[16]	Information security risk assessment, implementation of security controls, monitoring, and review	☑
12	2023	[70]	Internet of Things, Cybersecurity, Firmware, Entropy, Hardcoded, Attack Vector	☑
13	2023	[70]	Security assessment, Decision tree, Copula functions, Machine learning	☑
14	2023	[24]	Information security, Policy, Decision making	☑
15	2023	[25]	Information security assessment, Security assessment, Fuzzy theory, Smart grid	☑

clear that the CSRAM is comprehensive and can cover whole existing security assessment models components. The comparison between the CSRAM model and the existing model specifies that CSRAM is adequate if assessed to the current model. The CSRAM model can offer the same level of execution, while also offering a substantially lower cost. Also, CSRAM can extend a much lesser real footprint, which yields it a best choice for many functions. Furthermore, the CSRAM model can plan a much faster access time than the existing model, making it an ideal selection for efforts that require high speed processing.

5. Conclusion

Organizations conduct Security Risk Assessments to identify, analyze, and evaluate potential security risks. As part of a comprehensive security program, it protects the assets, personnel, and operations of an organization. Various security assessment models have been published in the literature to protect the assets, personnel, and operations of the Saudi organization. Nevertheless, these models are redundant and were developed for specific purposes. As a result, the comprehensive security risk assessment model used by Saudi organizations to safeguard their assets, personnel, and operations is still missing. This study developed a comprehensive security risk assessment model called CSRAM based on the ISO/IEC 27005 ISRM standard to assess security risks in Saudi Arabian organizations. It consists of six main stages: threat identification, vulnerability assessment, risk analysis, risk evaluation, risk treatment, and monitoring and review of risk. The stages have many activities and tasks to accomplish at each stage. Based on the comparison of the CSRAM model to the existing model, it appears that CSRAM is sufficient. The future work of this study involves implementing the effects of a comprehensive security risk assessment model in the real-world environment. This includes collecting and analyzing data from different sources, such as financial institutions, social networks, and other sources of information related to the security risk assessment process. It also involves developing an evaluation framework to assess the model's effectiveness in predicting security risks.

Acknowledgements

No funds have been received for the conduct of this research.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F. (2014) Current Challenges in Information Security Risk Management. *Information Management & Computer Security*, **22**, 410-430. https://doi.org/10.1108/IMCS-07-2013-0053

[2] Murr, P. and Carrera, N. (2022) Institutional Logics and Risk Management Practices in Government Entities: Evidence from Saudi Arabia. *Journal of Accounting & Organizational Change*, **18**, 12-32. https://doi.org/10.1108/JAOC-11-2020-0195

[3] Alshareef, N.M.N. (2022) Information Security Risk Management (ISRM) Model for Saudi Arabian Organisations. Master's Thesis, Curtin University, Curtin.

[4] Shanthamurthy, D. (2011) Leveraging ISO 27005 Standard's Risk Assessment Capabilities. https://www.computerweekly.com/tip/Leveraging-ISO-27005-standards-risk-assessment-capabilities

[5] Alturkistani, F.M. and Emam, A.Z. (2014) A Review of Security Risk Assessment Methods in Cloud Computing. In: Rocha, Á., Correia, A., Tan, F. and Stroetmann, K., Eds., *New Perspectives in Information Systems and Technologies*, Springer, Cham, 443-453. https://doi.org/10.1007/978-3-319-05951-8_42

[6] Al-Dhaqm, A., *et al.* (2017) CDBFIP: Common Database Forensic Investigation Processes for Internet of Things. *IEEE Access*, **5**, 24401-24416. https://doi.org/10.1109/ACCESS.2017.2762693

[7] Al-Dhaqm, A., *et al.* (2020) Categorization and Organization of Database Forensic Investigation Processes. *IEEE Access*, **8**, 112846-112858. https://doi.org/10.1109/ACCESS.2020.3000747

[8] Al-Dhaqm, A., Razak, S., Othman, S.H., Ngadi, A., Ahmed, M.N. and Ali Mohammed, A. (2017) Development and Validation of a Database Forensic Metamodel (DBFM). *PLOS ONE*, **12**, e0170793. https://doi.org/10.1371/journal.pone.0170793

[9] Ali, A., Abd Razak, S., Othman, S.H., Mohammed, A. and Saeed, F. (2017) A Metamodel for Mobile Forensics Investigation Domain. *PLOS ONE*, **12**, e0176223. https://doi.org/10.1371/journal.pone.0176223

[10] Al-Dhaqm, A., Razak, S., Siddique, K., Ikuesan, R.A. and Kebande, V.R. (2020) Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field. *IEEE Access*, **8**, 145018-145032. https://doi.org/10.1109/ACCESS.2020.3008696

[11] Al-Dhaqm, A., *et al.* (2020) Database Forensic Investigation Process Models: A Review. *IEEE Access*, **8**, 48477-48490. https://doi.org/10.1109/ACCESS.2020.2976885

[12] Al-Dhaqm, A., Ikuesan, R.A., Kebande, V.R., Razak, S. and Ghabban, F.M. (2021) Research Challenges and Opportunities in Drone Forensics Models. *Electronics*, **10**, Article 1519. https://doi.org/10.3390/electronics10131519

[13] Kebande, V.R., Ikuesan, R.A., Karie, N.M., Alawadi, S., Choo, K.K.R. and Al-Dhaqm, A. (2020) Quantifying the Need for Supervised Machine Learning in Conducting Live Forensic Analysis of Emergent Configurations (ECO) in IoT Environments. *Forensic Science International*: *Reports*, **2**, Article ID: 100122. https://doi.org/10.1016/j.fsir.2020.100122

[14] Moore, D.A. (2013) Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries. *Journal of Loss Prevention in the Process*, **26**, 1685-1689. https://doi.org/10.1016/j.jlp.2013.10.012

[15] Hassan, M., Saeedi, K., Almagwashi, H. and Alarifi, S. (2023) Information Security Risk Awareness Survey of Non-Governmental Organization in Saudi Arabia. In: Visvizi, A., Troisi, O. and Grimaldi, M., Eds., *Research and Innovation Forum* 2022. *RIIFORUM* 2022, Springer, Cham, 39-71. https://doi.org/10.1007/978-3-031-19560-0_4

[16] Tuyikeze, T. and Flowerday, S. (2014) Information Security Policy Development

and Implementation: A Content Analysis Approach. 8th *International Symposium on Human Aspects of Information Security and Assurance* (*HAISA*), Plymouth, July 2014, 11-20.

[17] Alshaikh, M., Maynard, S.B., Ahmad, A. and Chang, S. (2016) Information Security Policy: A Management Practice Perspective. arXiv: 1606.00890.

[18] Ismail, W.B.W., Widyarto, S., Ahmad, R.A.T.R. and Abd Ghani, K. (2017) A Generic Framework for Information Security Policy Development. 2017 4*th International Conference on Electrical Engineering*, *Computer Science and Informatics* (*EECSI*), Yogyakarta, 19-21 September 2017, 1-6. https://doi.org/10.1109/EECSI.2017.8239132

[19] Irfan, S. and Junseok, H. (2014) The Application of AHP to Evaluate Information Security Policy Decision Making. *International Journal of Simulation*: *Systems*, *Science and Technology*, **10**, 46-50. https://doi.org/10.4135/9781473914643.n11

[20] Talib, A.M., Alomary, F.O., Alwadi, H.F. and Albusayli, R.R. (2018) Ontology-Based Cyber Security Policy Implementation in Saudi Arabia. *Journal of Information Security*, **9**, 315-333. https://doi.org/10.4236/jis.2018.94021

[21] Aljuryyed, A. (2022) Cybersecurity Issues in the Middle East: Case Study of the Kingdom of Saudi Arabia. In: Dawson, M., Tabona, O. and Maupong, T., Eds., *Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security*, IGI Global, Hershey, 62-82. https://doi.org/10.4018/978-1-7998-8693-8.ch004

[22] AlGhamdi, S., Win, K.T. and Vlahu-Gjorgievska, E. (2022) Employees' Intentions toward Complying with Information Security Controls in Saudi Arabia's Public Organisations. *Government Information Quarterly*, **39**, Article ID: 101721. https://doi.org/10.1016/j.giq.2022.101721

[23] Shanmugam, B. and Azam, S. (2023) Risk Assessment of Heterogeneous IoMT Devices: A Review. *Technologies*, **11**, Article 31. https://doi.org/10.3390/technologies11010031

[24] Ma, Y., *et al*. (2022) Smart Grid Information Security Assessment Model Based on Correlation Index. *Advances in Artificial Intelligence and Security*: 8*th International Conference on Artificial Intelligence and Security*, *ICAIS* 2022, Qinghai, 15-20 July 2022, 672-681. https://doi.org/10.1007/978-3-031-06764-8_53

[25] Al-Dhaqm, A.M.R., Othman, S.H., Abd Razak, S. and Ngadi, A. (2014) Towards Adapting Metamodelling Technique for Database Forensics Investigation Domain. 2014 *International Symposium on Biometrics and Security Technologies* (*ISBAST*), Kuala Lumpur, 26-27 August 2014, 322-327. https://doi.org/10.1109/ISBAST.2014.7013142

[26] Al-Dhaqm, A., Razak, S., Ikuesan, R.A., Kebande, V.R. and Othman, S.H. (2021) Face Validation of Database Forensic Investigation Metamodel. *Infrastructures*, **6**, Article 13. https://doi.org/10.3390/infrastructures6020013

[27] Al-Dhaqm, A., *et al*. (2021) Digital Forensics Subdomains: The State of the Art and Future Directions. *IEEE Access*, **9**, 152476-152502. https://doi.org/10.1109/ACCESS.2021.3124262

[28] Aldhaqm, A., Abd Razak, S. and Othman, S.H. (2015) Common Investigation Process Model for Database Forensic Investigation Discipline. 1*st ICRIL-International Conference on Innovation in Science and Technology* (*IICIST* 2015), Kuala Lumpur, 20 April 2015, 297-300.

[29] Alotaibi, F.M., Al-Dhaqm, A. and Al-Otaibi, Y.D. (2022) A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field. *Computational Intelligence and Neuroscience*, **2022**, Article ID: 8002963.

https://doi.org/10.1155/2022/8002963

[30] Ghabban, F.M., Alfadli, I.M., Ameerbakhsh, O., AbuAli, A.N., Al-Dhaqm, A. and Al-Khasawneh, M.A. (2021) Comparative Analysis of Network Forensic Tools and Network Forensics Processes. 2021 2*nd International Conference on Smart Computing and Electronic Enterprise* (*ICSCEE*), Cameron Highlands, 15-17 June 2021, 78-83. https://doi.org/10.1109/ICSCEE50312.2021.9498226

[31] Ameerbakhsh, O., Ghabban, F.M., Alfadli, I.M., AbuAli, A.N., Al-Dhaqm, A. and Al-Khasawneh, M.A. (2021) Digital Forensics Domain and Metamodeling Development Approaches. 2021 2*nd International Conference on Smart Computing and Electronic Enterprise* (*ICSCEE*), Cameron Highlands, 15-17 June 2021, 67-71. https://doi.org/10.1109/ICSCEE50312.2021.9497935

[32] Alhussan, A.A., Al-Dhaqm, A., Yafooz, W., Emara, A.H.M., Bin Abd Razak, S. and Khafaga, D.S. (2022) A Unified Forensic Model Applicable to the Database Forensics Field. *Electronics*, **11**, Article 1347. https://doi.org/10.3390/electronics11091347

[33] Alotaibi, F.M., Al-Dhaqm, A., Al-Otaibi, Y.D. and Alsewari, A.A. (2022) A Comprehensive Collection and Analysis Model for the Drone Forensics Field. *Sensors*, **22**, Article 6486. https://doi.org/10.3390/s22176486

[34] Yafooz, W.M.S., Al-Dhaqm, A. and Alsaeedi, A. (2023) Detecting Kids Cyberbullying Using Transfer Learning Approach: Transformer Fine-Tuning Models. In: Yafooz, W.M.S., Al-Aqrabi, H., Al-Dhaqm, A. and Emara, A., Eds., *Kids Cybersecurity Using Computational Intelligence Techniques. Studies in Computational Intelligence*, Springer, Cham. 255-267. https://doi.org/10.1007/978-3-031-21199-7_18

[35] Alhussan, A.A., Al-Dhaqm, A., Yafooz, W.M.S., Razak, S.B.A., Emara, A.H.M. and Khafaga, D.S. (2022) Towards Development of a High Abstract Model for Drone Forensic Domain. *Electronics*, **11**, Article 1168. https://doi.org/10.3390/electronics11081168

[36] Alfadli, I.M., Ghabban, F.M., Ameerbakhsh, O., AbuAli, A.N., Al-Dhaqm, A. and Al-Khasawneh, M.A. (2021) CIPM: Common Identification Process Model for Database Forensics Field. 2021 2*nd International Conference on Smart Computing and Electronic Enterprise* (*ICSCEE*), Cameron Highlands, 15-17 June 2021, 72-77. https://doi.org/10.1109/ICSCEE50312.2021.9498014

[37] Razak, S.A., Nazari, N.H.M. and Al-Dhaqm, A. (2020) Data Anonymization Using Pseudonym System to Preserve Data Privacy. *IEEE Access*, **8**, 43256-43264. https://doi.org/10.1109/ACCESS.2020.2977117

[38] Al-Dhaqm, A., Othman, S.H., Yafooz, W.M.S. and Ali, A. (2023) Review of Information Security Management Frameworks. In: Yafooz, W.M.S., Al-Aqrabi, H., Al-Dhaqm, A. and Emara, A., Eds., *Kids Cybersecurity Using Computational Intelligence Techniques*, Springer, Cham, 69-80. https://doi.org/10.1007/978-3-031-21199-7_5

[39] Salem, M., Othman, S.H., Al-Dhaqm, A. and Ali, A. (2023) Development of Metamodel for Information Security Risk Management. In: Yafooz, W.M.S., Al-Aqrabi, H., Al-Dhaqm, A. and Emara, A., Eds., *Kids Cybersecurity Using Computational Intelligence Techniques*, Springer, Cham, 243-253. https://doi.org/10.1007/978-3-031-21199-7_17

[40] Al-Dhaqm, A., Yafooz, W.M.S., Othman, S.H. and Ali, A. (2023) Database Forensics Field and Children Crimes. In: Yafooz, W.M.S., Al-Aqrabi, H., Al-Dhaqm, A. and Emara, A., Eds., *Kids Cybersecurity Using Computational Intelligence Techniques*, Springer, Cham, 81-92. https://doi.org/10.1007/978-3-031-21199-7_6

[41] Saleh, M., *et al.* (2023) A Metamodeling Approach for IoT Forensic Investigation.

Electronics, **12**, Article 524. https://doi.org/10.3390/electronics12030524

[42] Ali, A., Razak, S.A., Othman, S.H., Marie, R.R., Al-Dhaqm, A. and Nasser, M. (2022) Validating Mobile Forensic Metamodel Using Tracing Method. In: Saeed, F., Mohammed, F. and Ghaleb, F., Eds., *Advances on Intelligent Informatics and Computing. IRICT* 2021, Springer, Cham, 473-482. https://doi.org/10.1007/978-3-030-98741-1_39

[43] Baras, D.S.A., Othman, S.H., Al-Dhaqm, A. and Radzi, R.Z.R.M. (2021) Information Security Management Metamodel (ISMM) Validation and Verification through Frequency-Based Selection Technique. 2021 *International Conference on Data Science and Its Applications* (*ICoDSA*), Bandung, 6-7 October 2021, 292-297. https://doi.org/10.1109/ICoDSA53588.2021.9617527

[44] Al-Dhaqm, A.M.R. (2019) Simplified Database Forensic Invetigation Using Metamodeling Approach. Master's Thesis, Universiti Teknologi Malaysia, Iskandar Puteri.

[45] Al-Dhaqm, A., Razak, S. and Othman, S.H. (2019) Model Derivation System to Manage Database Forensic Investigation Domain Knowledge. 2018 *IEEE Conference on Application*, *Information and Network Security* (*AINS*), Langkawi, 21-22 November 2018, 75-80. https://doi.org/10.1109/AINS.2018.8631468

[46] Aldhaqm, A., Abd Razak, S., Othman, S.H., Ali, A. and Ngadi, A. (2016) Conceptual Investigation Process Model for Managing Database Forensic Investigation Knowledge. *Research Journal of Applied Sciences*, *Engineering and Technology*, **4**, 386-394. https://doi.org/10.19026/rjaset.12.2377

[47] Ngadi, M., Al-Dhaqm, R. and Mohammed, A. (2012) Detection and Prevention of Malicious Activities on RDBMS Relational Database Management Systems. *International Journal of Scientific & Engineering Research*, **3**, 1-10.

[48] Ali, A., Abd Razak, S., Othman, S.H. and Mohammed, A. (2017) Extraction of Common Concepts for the Mobile Forensics Domain. In: Saeed, F., Gazem, N., Patnaik, S., Saed Balaid, A. and Mohammed, F., Eds., *Recent Trends in Information and Communication Technology. IRICT* 2017, Springer, Cham, 141-154. https://doi.org/10.1007/978-3-319-59427-9_16

[49] Ali, A., Razak, S.A., Othman, S.H. and Mohammed, A. (2015) Towards Adapting Metamodeling Approach for the Mobile Forensics Investigation Domain. 1*st ICRIL International Conference on Innovation in Science and Technology* (*IICIST* 2015), Kuala Lumpur, 20 April 2015, 364-367.

[50] Saleh, M.A., Othman, S.H., Al-Dhaqm, A. and Al-Khasawneh, M.A. (2021) Common Investigation Process Model for Internet of Things Forensics. 2021 2*nd International Conference on Smart Computing and Electronic Enterprise* (*ICSCEE*), Cameron Highlandsc, 15-17 June 2021, 84-89. https://doi.org/10.1109/ICSCEE50312.2021.9498045

[51] Zawali, B., Ikuesan, R.A., Kebande, V.R. and Furnell, S. (2021) Realising a Push Button Modality for Video-Based Forensics. *Infrastructures*, **6**, Article 54. https://doi.org/10.3390/infrastructures6040054

[52] March, S.T. and Smith, G.F. (1995) Design and Natural Science Research on Information Technology. *Decision Support Systems*, **15**, 251-266. https://doi.org/10.1016/0167-9236(94)00041-2

[53] Alaqsam, A. and Ghabban, F.M. (2021) Online Programming Language Learning Using Massive Open Online Courses in Saudi Universities. *International Journal of Emerging Trends in Engineering Research*, **9**, 116-131. https://doi.org/10.30534/ijeter/2021/16922021

[54] Allam, A.A., *et al.* (2022) The Use of M-Government and M-Health Applications during the COVID-19 Pandemic in Saudi Arabia. *Journal of Software Engineering and Applications*, **15**, 406-416. https://doi.org/10.4236/jsea.2022.1511023

[55] Nilashi, M., Fallahpour, A., Wong, K.Y. and Ghabban, F. (2022) Customer Satisfaction Analysis and Preference Prediction in Historic Sites through Electronic Word of Mouth. *Neural Computing and Applications*, **34**, 13867-13881. https://doi.org/10.1007/s00521-022-07186-5

[56] Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J. (2014) Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies. *Information Management & Computer Security*, **22**, 42-75. https://doi.org/10.1108/IMCS-08-2012-0045

[57] Alsaif, M., Aljaafari, N. and Khan, A.R. (2015) Information Security Management in Saudi Arabian Organizations. *Procedia Computer Science*, **56**, 213-216. https://doi.org/10.1016/j.procs.2015.07.201

[58] Thakur, K., Ali, M.L., Gai, K. and Qiu, M. (2016) Information Security Policy for E-Commerce in Saudi Arabia. 2016 *IEEE 2nd International Conference on Big Data Security on Cloud* (*BigDataSecurity*), *IEEE International Conference on High Performance and Smart Computing* (*HPSC*), *and IEEE International Conference on Intelligent Data and Security* (*IDS*), New York, 9-10 April 2016, 187-190. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.14

[59] Safa, N.S., Von Solms, R. and Furnell, S. (2016) Information Security Policy Compliance Model in Organizations. *Computers & Security*, **56**, 70-82. https://doi.org/10.1016/j.cose.2015.10.006

[60] Alqahtani, F.H. (2017) Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science*, **124**, 691-697. https://doi.org/10.1016/j.procs.2017.12.206

[61] Almubayedh, D., Alazman, G., Alabdali, M., Al-Refai, R. and Nagy, N. (2018) Security Related Issues in Saudi Arabia Small Organizations: A Saudi Case Study. 2018 *21st Saudi Computer Society National Computer Conference* (*NCC*), Riyadh, 25-26 April 2018, 1-6. https://doi.org/10.1109/NCG.2018.8593058

[62] Almeida, F., Carvalho, I. and Cruz, F. (2018) Structure and Challenges of a Security Policy on Small and Medium Enterprises. *KSII Transactions on Internet and Information Systems*, **12**, 747-763. https://doi.org/10.3837/tiis.2018.02.012

[63] Moody, G.D., Siponen, M. and Pahnila, S. (2018) Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, **42**, 285-311. https://doi.org/10.25300/MISQ/2018/13853

[64] Park, M. and Chai, S. (2018) Internalization of Information Security Policy and Information Security Practice: A Comparison with Compliance. *Proceedings of the 51st Hawaii International Conference on System Sciences*, Hawaii, 3-6 January 2018, 4723-4731. https://doi.org/10.24251/HICSS.2018.595

[65] Amankwa, E., Loock, M. and Kritzinger, E. (2018) Establishing Information Security Policy Compliance Culture in Organizations. *Information and Computer Security*, **26**, 420-436. https://doi.org/10.1108/ICS-09-2017-0063

[66] Kaušpadienė, L., Ramanauskaitė, S. and Čenys, A. (2019) Information Security Management Framework Suitability Estimation for Small and Medium Enterprise. *Technological and Economic Development of Economy*, **25**, 1-19. https://doi.org/10.20334/2019-027-M

[67] Hengstler, S., Nickerson, R.C. and Trang, S. (2022) Towards a Taxonomy of Information Security Policy Non-Compliance Behavior. *Proceedings of the 55th Hawaii*

International Conference on System Sciences, Hawaii, 4-7 January 2022, 4826-4835. https://doi.org/10.24251/HICSS.2022.588

[68] Kabanda, S. and Mogoane, S.N. (2022) A Conceptual Framework for Exploring the Factors Influencing Information Security Policy Compliance in Emerging Economies. In: Sheikh, Y.H., Rai, I.A. and Bakar, A.D., Eds., *E-Infrastructure and E-Services for Developing Countries*. *AFRICOMM* 2021, Springer, Cham, 203-218. https://doi.org/10.1007/978-3-031-06374-9_13

[69] Bhardwaj, A., Kaushik, K., Alshehri, M., Mohamed, A.A.B. and Keshta, I. (2023) ISF: Security Analysis and Assessment of Smart Home IoT-based Firmware. ACM Transactions on Sensor Networks. https://doi.org/10.1145/3578363

[70] Mollaiee, A., Ameli, M.T., Azad, S., Nazari-Heris, M. and Asadi, S. (2023) Data-Driven Security Assessment Using High Content Database during the COVID-19 Pandemic. *International Journal of Electrical Power & Energy Systems*, **150**, Article ID: 109077. https://doi.org/10.1016/j.ijepes.2023.109077