Scientific Research Publishing

Journal of Software Engineering and Applications, 2023, 16, 695-713
https://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

Developing an Abstraction Framework for Managing and Controlling Saudi Banks' Cybersecurity Threats Based on the NIST Cybersecurity Framework and ISO/IEC 27001

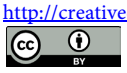
Abdulaziz Saleh Alraddadi

College of Computer Science and Engineering, Taibah University, Yanbu, Kingdom of Saudi Arabia
Email: alraddadi1@yahoo.com

How to cite this paper: Alraddadi, A.S. (2023) Developing an Abstraction Framework for Managing and Controlling Saudi Banks' Cybersecurity Threats Based on the NIST Cybersecurity Framework and ISO/IEC 27001. *Journal of Software Engineering and Applications*, **16**, 695-713.
https://doi.org/10.4236/jsea.2023.1612036

Received: November 12, 2023
Accepted: December 26, 2023
Published: December 29, 2023

Copyright © 2023 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/



Open Access

Abstract

Saudi Arabian banks are deeply concerned about how to effectively monitor and control security threats. In recent years, the country has taken several steps towards restructuring its organizational security and, consequently, protecting financial institutions and their clients. However, there are still several challenges left to be addressed. Accordingly, this article aims to address this problem by proposing an abstract framework based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework and International Organization for Standardization/International Electrotechnical Commission (ISO/IEC 27001). The framework proposed in this paper considers the following factors involved in the security policy of Saudi banks: safety, Saudi information bank, operations and security of Saudi banks, Saudi banks' supplier relationships, risk assessment, risk mitigation, monitoring and detection, incident response, Saudi banks' business continuity, compliance, education, and awareness about all factors contributing to the framework implementation. This way, the proposed framework provides a comprehensive, unified approach to managing bank security threats. Not only does the proposed framework provide effective guidance on how to identify, assess, and mitigate security threats, but it also instructs how to develop policy and procedure documents relating to security issues.

Keywords

Cybersecurity Threats, NIST Cybersecurity Framework, ISO/IEC 27001, Saudi Banks, Design Science Research

1. Introduction

Nowadays, technology is pervasively used across a wide range of sectors such as business, government, and private communication. Technology has appeared as a two-edged sword; it has many benefits, on the one hand, and causes the prevalence of security threats on the other [1] [2]. Such threats could adversely affect the operations, reputation, and customers of an organization. The literature comprises a variety of approaches (including security models, frameworks, policies, procedures, and protocols) to minimize or avoid these risks. There are several frameworks used by Saudi banks to assess and manage the cybersecurity risks they generally face. The NIST Cybersecurity Framework and ISO/IEC 27001 Framework are two frameworks developed in this regard.

In recent years, the National Institute of Standards and Technology (NIST) has established the NIST Cybersecurity Framework (NIST CSF) that permits governments to evaluate the performance of cybersecurity risk administrations and recover them whenever required [3]. An active cybersecurity package is based on a series of rules, best performance, and standards developed by NIST to confirm its real execution and management [4]. NIST CSF comprises five core functions: identifying, protecting, detecting, responding, and recovering. By assessing cybersecurity posture, identifying gaps, and developing plans, the framework guides an organization through the improvement of its security posture [5]. This framework also encourages organizations to create and implement cybersecurity strategies tailored to their own risks profiles and also to work in collaboration with other stakeholders to formulate cybersecurity strategies based on their own risk profiles [6] [7] NIST CSF helps organizations to successfully address threats in a holistic, systematic, and cost-effective manner by improving their overall cybersecurity posture and by addressing threats in a holistic, systematic, and cost-effective manner. The NIST CSF is shown in **Figure 1**.

On the other hand, as an international standard, ISO/IEC 27001 has many capabilities, which include defining, implementing, running, monitoring, evaluating, reviewing, maintaining, and improving information security management systems (ISMS) [8]. It is a standard that belongs to the ISO/IEC 27000 family, which, in turn, is part of the ISO/IEC 27002 standard, described here as a code of practice for information security controls [8]. By adopting this standard, organizations can select appropriate and proportionate security controls to protect their information assets and give their stakeholders a sense of security [9]. The ISO/IEC 27001 framework is displayed in **Figure 2**.

Accordingly, the aim of this study is to develop an abstraction framework for managing and controlling the threats posed to Saudi banks' cybersecurity, based on NIST CSF and ISO/IEC 27001, using design science approach. Regarding the methodology, this study reviews the relevant literature extensively and analyses the existing frameworks and standards such as NIST CSF and ISO/IEC 27001. To validate the efficiency of this framework, a series of tests will be conducted with shareholders from the Saudi banking sector. At the end of the study, some

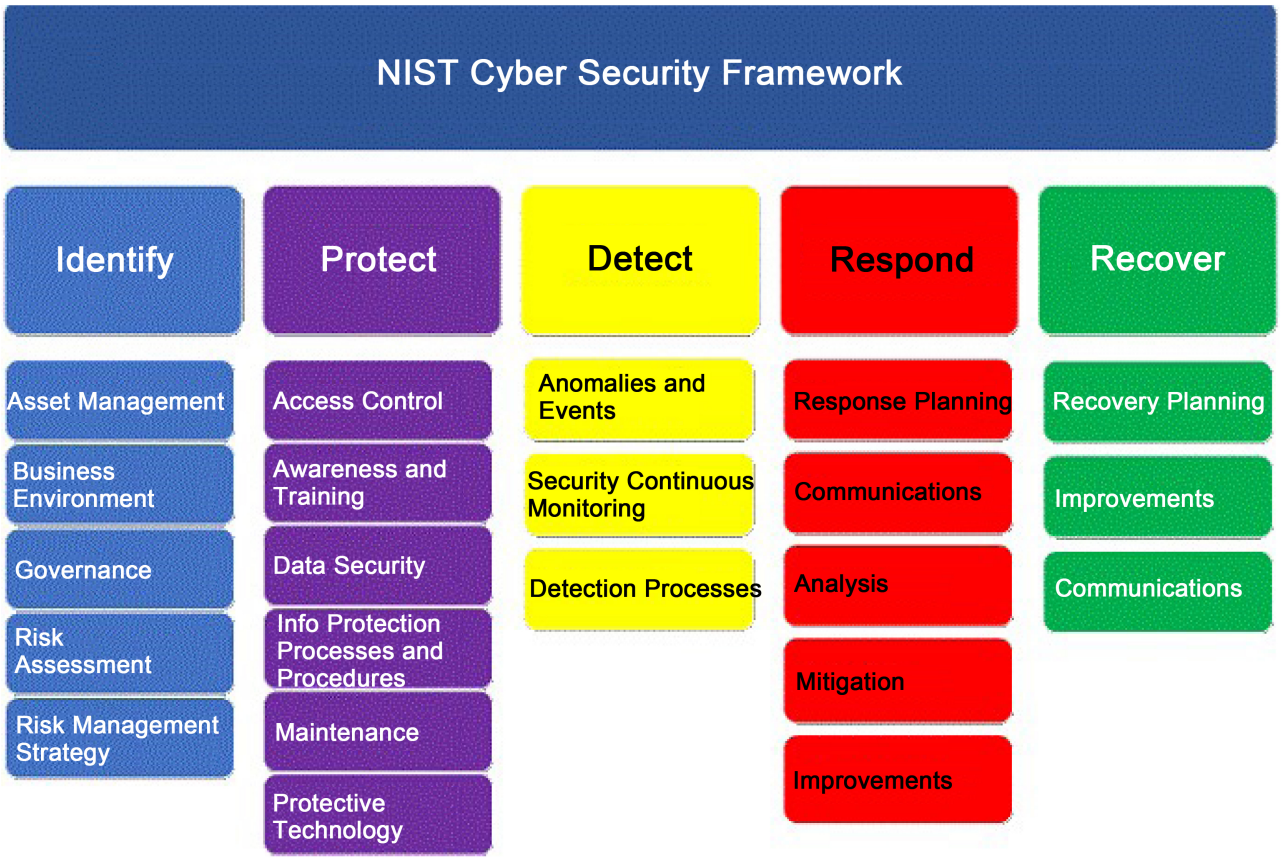


Figure 1. NIST Cybersecurity framework [3].

Figure 2. ISO/IEC 27001: 2005 [8].

recommendations will be made for improving the proposed framework.

The rest of the article is organized as follows: Section 2 discusses the related work. Then, Section 3 explains the methodology used in this study. Next, Section 4 presents the results and discussion. And, finally, Section 5 concludes the paper and offers recommendation for future works.

The literature consists of several security models and frameworks that can be used to ensure that data are confidential, secure, and accessible. The topic of data integrity, confidentiality, and accessibility has attracted a lot of attention in the literature. In the literature, there are various models and frameworks developed for assessing construction risks, which generally address time, cost, quality, security (only physical aspects), safety, etc. [10]-[16]. Nevertheless, the literature lacks cybersecurity-related frameworks. Compared to other industries such as manufacturing, healthcare, and banking has been slow in becoming digitized. The purpose of this section is to briefly review the merits and limitations of relevant studies that have proposed frameworks, models, or methods and incorporated cybersecurity aspects into the construction industry, a topic directly relevant to the present study. For example, as a solution to the challenges associated with cloud-based BIM data breaches, the authors in [17] provided a cybersecurity framework comprising five main components: access control, data encryption, monitoring and detection, continuous training, and education. As a part of the BIM curriculum, researchers in [18] suggested that cybersecurity and blockchain be included as a part of the curriculum. Likewise, the authors in [19] have emphasized that to mitigate the risks associated with the digital built environment, there is a need to develop innovative blockchain technologies.

In two recent studies, it was found that traditional banks become more vulnerable to cyberattacks when they cooperate with fintech firms [20] [21] [22]. Another important factor contributing to the success of the digital transformation process is the growing use of mobile devices. According to a Bain & Company survey of digital clients from 22 countries, mobile banking apps grew 19% between 2013 and 2014, while computer-based banking services remained relatively unchanged [23]. As a result of digitalization, businesses and organizations have been able to create a wide range of business models and structures [24]. The term "threat" refers to actions that may harm the assets of an organization. Cyberattacks damage software, hardware, and data. As part of its threat classification system, Microsoft designed STRIDE [25].

The authors in [26] stated that the banking industry is also affected by digitalization due to a lack of trust. The study found that trust is crucial to customers to commit to online relationship banking. The issue is that most banks still need to get prepared for their clients' changing needs as they migrate to the Internet [27].

The Saudi American Bank (SAMBA), Al-Rajhi Bank, Al-Ahli Bank (CNB), and Al-Riyadh Bank are Saudi Arabia's top four banks [28]. Further, the authors in [29] compared SAMBA with other Saudi banks, and found it, as an e-banking-based and internationally linked institute, to have a key strength that

most other Saudi banks lack.

Meanwhile, there have been several digital forensic studies conducted to detect and investigate the threats and risks faced by organizations. By implementing digital forensics, organizations can better identify and respond to security incidents, reduce risks, and improve the overall security posture of their organization. For example, the authors in [5] [6] [30]-[55] suggested and established various models, frames, and procedures to examine and discover cybercrime, data breaks, and other digital risks that may influence an organization's security and reputation.

During the past few years, Saudi Arabia has taken several steps towards strengthening its organizational security and, as a result, protecting the financial institutions as well as their clients. Despite this, there are still a number of issues that need to be addressed. Therefore, the purpose of this article is to address this problem by proposing an abstract framework that is based on the NIST Cybersecurity Framework as well as ISO/IEC 27001.

2. Methodology

This section provides an overview of the methodology used in this study to achieve the objective defined. The present study uses the design science approach [56] [57] to develop an abstraction framework applicable to managing and controlling the cyber threats that Saudi banks may face in their daily operations. A framework was developed to meet this objective, which is based upon NIST CSF and ISO/IEC 27001:2010. To understand the context and explore the existing solutions to this problem, the research process was started by reviewing the literature on both topics. A requirements analysis was also performed in this study to identify the cybersecurity threats most relevant to Saudi banks and the components that should be included in the framework. Afterwards, the framework design and development process were carried out. This study developed an abstraction framework to enhance the cybersecurity status of Saudi banks in the future. The developed framework provides Saudi banks with the necessary guidance, structure, and tools to identify, assess, and mitigate cyber risks. This framework is also adaptable and applicable to other financial institutions in the region, assisting them with managing and controlling cybersecurity threats that may arise during their operations.

Accordingly, **Figure 3** illustrates the methodology that was applied to this study to conduct it.

1) Identifying search protocols stage: in this stage, the author identifies the search protocols which are:

- Assigning search keywords: in this step, we assign the keywords which govern the search in the search engines which are "NIST Cybersecurity Framework, ISO/IEC 27001; Saudi banks". The period of searching from 2015-2023.
- Identifying search engines: in this step we identify five common search engines which are IEEE explorer, Scopus, Web of Science, Springer Links, and Google Scholar.

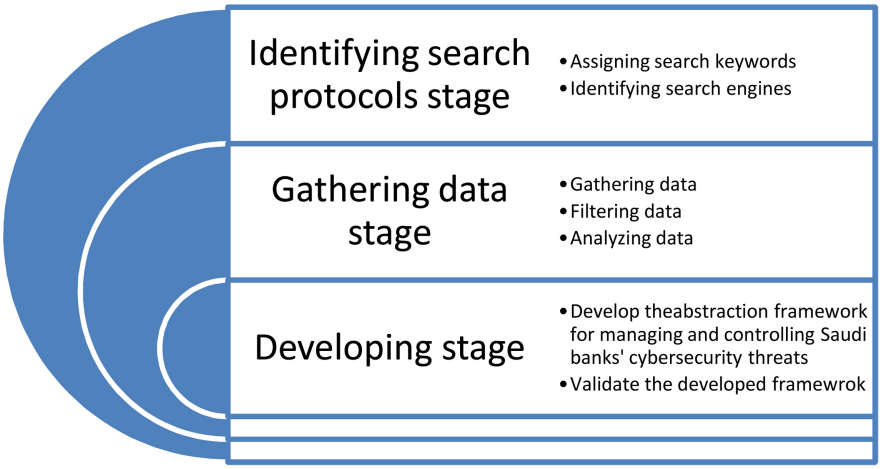


Figure 3. Applied methodology.

2) Gathering data stage: this stage includes three steps:

- Gathering data: in this step we gather whole articles from the identified search engines.
- Filtering data: in this step we filter the data based on these criteria: screening the title, abstract and conclusion. The relevant paper has included in this study.
- Analysing data: in this step, the filtered data has been analysed carefully, the advantages, disadvantages, results, methodology and contributions.

3) Developing stage: in this stage, the author develops and validates the abstraction framework for managing and controlling Saudi banks' cybersecurity threats. It consists of two steps:

- Developing the framework: in this step, the author gathers whole common processes from the analysed models and frameworks and develop the abstraction framework for managing and controlling Saudi banks' cybersecurity threats. The proposed framework comprises 12 components each of which is explained in the following (see **Figure 4**):

1) Security Policy for Saudi Banks: A secure data policy for Saudi banks is a document designed with the aim of protecting sensitive information, ensuring the completion of financial transitions, and maintaining overall data security. In the banking industry, each bank has its own security policy, a policy that differs from one bank to the next.

2) Safety for Saudi banks: As a result of the execution of this procedure, Saudi banks can guarantee the security of their properties. The Saudi banking business implements several measures to guarantee the protection of their physical properties, workers, clients, and financial businesses.

3) Saudi Information Bank: The procedure delivers full information about Saudi banks, containing their names, consultants, locations, websites, types of movement, licenses, etc.

4) The Operations and Security of Saudi Banks: To accomplish this process, critical information needs to be identified about Saudi banks. This way, it will

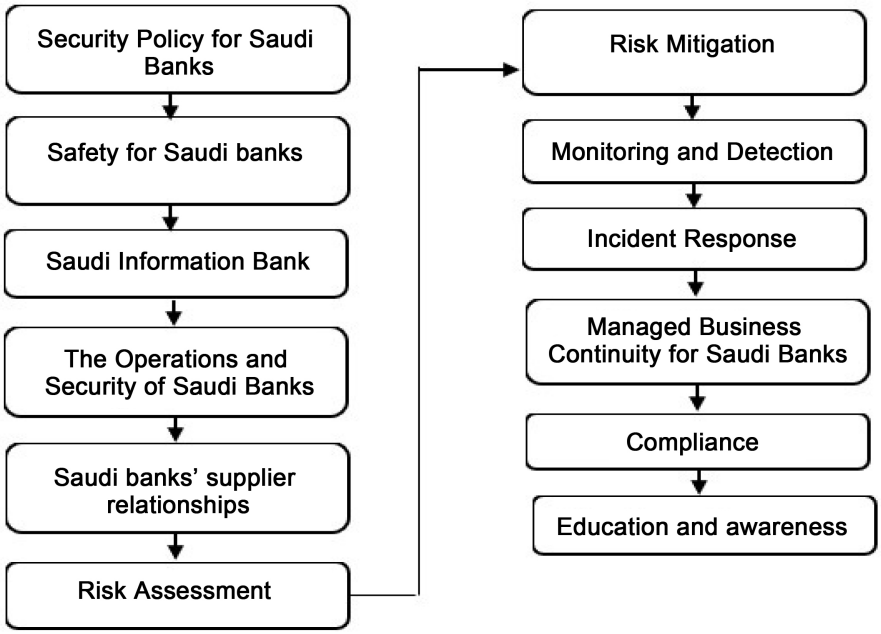


Figure 4. The abstraction framework for managing and controlling Saudi banks' cybersecurity threats.

determine if adversaries' intelligence is able to observe friendly actions and if adversaries can interpret information, they gather to serve their purposes. Then, the bank administrations can select measures which will be designed to reduce or eliminate the adversary exploitation of friendly critical information.

5) Saudi Banks' Supplier Relationships: Supplier relationships refer to the relationships between Saudi banking companies and the suppliers of goods, materials, and services. Supplier contributions to success must be measured and improved to achieve success.

6) Risk Assessment: The Saudi Arabian bank at this stage assesses the security risks that may arise. An assessment of assets, threats, vulnerabilities, and potential impacts will be of crucial importance for the preparation. Thus, it is imperative for the assets of the organization to be protected against the impact of security risks.

7) Risk Mitigation: Assessing risks and developing mitigation methods are part of a risk mitigation strategy. Implementing these strategies requires establishing policies and procedures, improving processes, and creating security controls. Identifying and mitigating risks is key to security plans. These plans are developed and implemented to reduce the damage caused by security breaches in many ways. To mitigate risks, several security controls can be implemented by providing appropriate policies and procedures.

8) Monitoring and Detection: Various tools and techniques, including artificial intelligence, are used by Saudi banks to monitor security incidents. The security of banks systems requires several tools and techniques. Security threats can be identified and prevented through the efficient use of artificial intelligence. This way, anomalies could be detected, threats could be identified, and real-time

monitoring would be possible.

9) Incident Response: Maintaining a safe business environment requires a comprehensive incident response plan. By identifying incidents, containing them, eliminating them, and resuming them in a timely manner, this plan will enable an effective and timely response to incidents. To determine the best response to an incident, it is first necessary to identify it. Unauthorized access to the internal network and suspicious activity on customer accounts should be prevented. Banks must act quickly after discovering a security incident, and make sure it is contained and mitigated. The first step is to limit access to the compromised system. The affected area should be isolated, and the appropriate people informed.

10) Managed Business Continuity for Saudi Banks: Identifying, managing, and preventing potential threats continues to be a priority of the Saudi Arabian banking sector. Disaster resilience is also being developed in the region. Disasters can be handled quickly with frameworks. As a result, the organization's reputation, brand, revenue generation ability, and ability to create value must be maintained. Maintaining high levels of effectiveness requires research and development.

11) Compliance: Compliance is required for regulated banks. The anti-money laundering regulations (AML) require tracking and reporting on compliance. A comprehensive system should integrate policies and procedures tailored to Saudi bank regulations for effective monitoring and reporting. All risks should be addressed in comprehensive policies and procedures. Customers need to be monitored, suspicious activities be reported, and internal controls be implemented to minimize risk.

12) Education and Awareness: Security risks and best practices, policies, and procedures are taught to Saudi banks' employees to maintain the highest level of security. Nevertheless, the threat of cybercrime has exponentially increased. The growing number of cyberattacks in Saudi Arabia has prompted banks to train their staff on cybersecurity risks and best practices, policies, and procedures relating to cyber-attacks. An effective security policy must be developed and maintained to ensure such training is implemented effectively. A bank's asset security policy should summarize its process, controls, and objectives. Additionally, the document should contain information on how the bank's employees are to be trained regarding the importance of maintaining security awareness, providing security training, and taking required steps in order to ensure that the bank's data, systems, and networks are protected. It is also important to train your staff on security policies and best practices as part of the second step, which should be followed by an audit. As a result of this course, students will be able to identify potential security threats, understand the importance of strong passwords, and become familiar with some basic information security concepts. A Saudi bank can ensure that it is protected from cybercrime by providing its employees with ongoing training and education on cybersecurity. As far as this type of training

is concerned, it should be viewed as an investment in the bank's reputation within the industry as well as in the safety and security of its customers and employees secure data policy for Saudi banks is a document designed with the aim of protecting sensitive information, ensuring the completion of financial transitions, and maintaining overall data security. In the banking industry, each bank has its own security policy, a policy that differs from one bank to the next.

- Validation step: This step delivers a validation process for the developed framework. To validate whether the proposed framework is comprehensive and logical, the validation process is required. Thus, frameworks and models should be authenticated before they can be used as a precise representation of the real application domain. The quality of a framework or model is determined by its ability to meet all the requirements during the course of its development [58]. A most-shared question asked when evolving a framework/model is how it can be used in real world situations. There are several factors that must be taken into account when considering whether to choose a specific type of validation technique [59]. For example, the goal of the model should be determined according to the type of framework or model (e.g., agent-based models, semantic models and conceptual models, and mathematical and statistical models). There are a number of validation techniques that can be used in the validation of a simulation model/framework (see **Table 1**) such as Bootstrap Approach [60], Cross-validation [61], and Multistage Validation [62]. The validity of these frameworks and models can only be verified if many samples of subjects are used to verify them and some comparison cycles are conducted, too. These methodologies for validation are not applicable to the present study due to the limited frameworks and models used, as well as the small sample size. Thus, the proposed framework will be validated by comparing it to other models [49], which do not require a large sample size to achieve validity. The blue color in **Table 2** represents the validation method used in the current study.

Therefore, to verify the completeness of the developed framework, ISO/IEC 27001 Security Framework and NIST CSF were selected (see **Table 2**) for comparison purposes. The proposed Security Policy for Saudi Banks protocol in the developed framework covers the Information Security Policies protocol in the ISO/IEC 27001 Security Framework. In addition, the Human Resource Security protocol in the ISO/IEC 27001 Security Framework covers the Security Policy for Saudi Banks protocol. The Risk Mitigation protocol in the developed framework covers two security protocols in the ISO/IEC 27001 Security Framework, *i.e.*, access control and cryptography security controls. On the other hand, the Incident Response protocol in the developed framework covers three security protocols in the ISO/IEC 27001 Security Framework and NIST CSF, *i.e.*, Security Incident Management, Respond, and Recover, respectively.

The developed framework comprises a new protocol, *i.e.*, Education and awareness security protocol, which is included in neither ISO/IEC 27001 framework nor NIST CSF. Consequently, the developed framework could assist

Table 1. The existing validation techniques.

ID	Year	Validation Technique	Description
1	1999	Machine-Aided [63]	In this technique, the multi-graph machine is used for specific purposes.
2	2004	Leave-one-out cross Validation [64]	This application is used to validate loss sensitive data, as well as the mathematical modeling purposes.
3	2015	Multistage Validation [62]	The purpose of this technique is to be able to simulate various systems.
4	2015	Tracing/Traceability [62]	This is a logical consistency checking technique that is used to evaluate the logical consistency of the framework/model against the domain model.
5	2015	Face Validity [62]	This technique was developed to make sure the model or framework is complete, logical, and useful, which is why it is important.
6	2005	Cross-validation [61]	It is a method for evaluating the accuracy of a model, which does not require any further examples to be examined prior to assessing the precision of the model. It is said to be also applicable to mathematical metamodeling.
7	2021	Comparison with other models [49]	By comparing the domain model with the metamodel, its completeness, accuracy, and correctness could be determined.
8	2006	Bootstrap Approach [60]	There are several advantages to bootstrapping over simulation in terms of computational efficiency. This software has been developed for the purpose of modeling simulations.
9	2007	Formal Ontology [65]	This method uses ontological domains as a basis for its operation. During the course, a great deal of emphasis is placed on theories.
10	2007	Subjective Validation [66]	The purpose of this method is to validate the framework, models, or metamodels of analog circuits.
11	2010	Case Study [67]	This technique is used to evaluate the processes through which metamodels are derived.

Table 2. Comparing the proposed framework with the ISO/IEC 27001 Security Protocols and NIST CSF.

Developed Framework Components	ISO/IEC 27001 Security Protocols													NIST Cybersecurity					
	Information Security policies	Organizations of Information Security	Human Resource Security	Asset Management	Access Control	Cryptography	Physical and Environment Security	Operations Security	Communications Security	System Acquisition and Maintenance	Supplier Relationships	Security Incident Management	Business Continuity management	Compliance	Identifying	Protecting	Detecting	Responding	Recovering
Security Policy for Saudi Banks	☑	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Safety for Saudi Banks	☒	☒	☑	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Saudi Information Bank	☒	☑	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
The Operations and Security of Saudi Banks	☒	☒	☒	☒	☒	☒	☒	☑	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Saudi Banks' Supplier Relationships	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☑	☒	☒	☒	☒	☒	☒	☒	☒
Risk Assessment	☒	☒	☒	☒	☒	☒	☑	☒	☒	☒	☒	☒	☒	☒	☑	☒	☒	☒	☒
Risk Mitigation	☒	☒	☒	☒	☑	☑	☒	☒	☒	☒	☒	☒	☒	☒	☒	☑	☒	☒	☒
Monitoring and Detection	☒	☒	☒	☒	☒	☒	☒	☒	☑	☒	☒	☒	☒	☒	☒	☒	☑	☒	☒
Incident Response	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☑	☒	☒	☒	☒	☒	☑	☑
Managed Business Continuity for Saudi Banks	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☑	☒	☒	☒	☒	☒	☒
Compliance	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☑	☒	☒	☒	☒	☒
Education and Awareness	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Saudi banks in developing specific security models, policies, protocols, processes, and procedures in line with their specific needs.

3. Results and Discussion

This study proposes an abstraction framework to be used by Saudi banks to identify, assess, and manage the security risks associated with bank investments in Saudi Arabia. The framework provides Saudi banks with a comprehensive set of tools, guidelines, and procedures for identifying, assessing, and managing security risks. The Saudi banks are advised to follow these high-level guidelines to reduce their risk exposure and to ensure the security of their customers' data to minimize risk. As part of the first stage of the process of identifying and assessing the security risks that Saudi banks face, the proposed framework identifies and assesses the possible security risks that the banks face. As a result, banking institutions can use this methodology to gain a better understanding of the current risk environment in which they operate. This will enable them to take steps toward mitigating the risks they are exposed to. Further, it can identify any potential weaknesses in a company's workplace processes as well as potential threats to those workplace processes if they were to be identified. It is hoped that this framework will enable banks to determine where their resources should be allocated and what strategies they should adopt to mitigate the risk of future security breaches by determining where their resources should be allocated.

In a nutshell, the proposed framework will enable banks, with the help of the framework, to develop their own security incident management standards that are well suited to the banks' requirements, in line with the proposed framework. There is an important issue that banks should follow to ensure that adequate security measures are in place in order for them to be able to effectively respond to security threats. It is imperative that banks follow the guidelines outlined above to ensure that adequate security measures are in place. There are a few steps that need to be followed to achieve this goal. Several steps will need to be taken to prevent future data breaches from occurring in the future, such as developing policies regarding the notification of data breaches and responding to complaints from customers to prevent such a situation from recurring in the future. Since the abstraction framework proposed in this paper allows banks to monitor and manage security risks continuously, banks will be able to monitor and manage security risks for a long time since the framework allows them to perform continuous monitoring and management of security risks for a long time. This security framework is a useful tool that banks can use to be able to continuously assess their security environment to make changes to it in accordance with how it evolves. Moreover, any potential threats or changes that may occur in the future can be reviewed to determine whether any changes need to be made to the security plan in order to address any threats or changes that may occur in the future. Therefore, banks will be able to give their customers the peace of mind to know that they are always keeping up to date with the latest technological ad-

vancements when it comes to their security operations. Thus, they can stay one step ahead of their competition by responding quickly to any emerging security issues, so that they can preserve their competitive advantage.

There are numerous security frameworks today, but they are not as generic as our proposed framework. Despite the fact that their design may differ from one another, they are more universal in nature, meaning they are not tailored to meet the specific challenges that particular countries or regions encounter. Compared with the ISO 27000 series or the NIST 800-53 standards, these standards tend to provide a more granular approach to risk management. This is when compared to the ISO 27000 series or NIST 800-53 standards. These guidelines are based on broader international standards, such as ISO 27000 or NIST 800-53, which are recognized around the world, and are based on broader international standards. Additionally, there's a possibility that they may not contain the specificity and details that each country or region needs when dealing with their own unique security challenges and concerns when it comes to dealing with their own unique security challenges. In fact, it is a similar problem to what Saudi Arabia is facing at the moment. The purpose of this study is therefore to develop an abstraction framework to manage and control risks related to Saudi bank security in order to achieve a better level of risk management and control. Because it is tailored to the country's and region's specific needs, it provides a more detailed and comprehensive approach to risk management that is more comprehensive and detailed as a result of being tailored to its specific needs. As a result of the framework, not only can it offer greater refinement and customization when it comes to risk management, but it can also offer greater granularity and customization when it comes to identifying and minimizing potential hazards that may occur in the future. As a result, Saudi banks must provide innovative programs aimed at educating their customers about security awareness. For them to be able to protect their employees against cyberattacks and cybercrime, they also need to ensure that they receive continuous training and education to ensure that they are prepared for such events. It is highly recommended that Saudi banks consider this type of training as a long-term investment in the safety and security of both their customers and their employees over the long term. In the banking industry, this helps them maintain a well-deserved reputation for providing high-quality service.

4. Conclusion

This study developed an abstraction framework using the NIST Cybersecurity Framework and ISO/IEC 27001. The framework was aimed at managing and controlling the cyber threats Saudi banks are facing. Basically, the framework comprised 12 components, *i.e.*, Saudi banks' security policy, Saudi information bank, Saudi banks' operations and security, Saudi banks' supplier relationships, the risk assessment of Saudi banks, risk mitigation, monitoring and detection, incident response, securing the continuity of Saudi banks, ensuring compliance

with regulations, education, and awareness. The abstraction framework developed in this study helps Saudi banks manage security risks in a comprehensive, unified way. Furthermore, it offers guidance on how to identify, assess, and mitigate security risks in a variety of environments. In future research, we will implement the developed framework in a real-world situation to verify its effectiveness.

Conflicts of Interest

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

References

[1] Tyagi, A.K., Dananjayan, S., Agarwal, D. and Thariq Ahmed, H.F. (2023) Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0. *Sensors*, **23**, Article 947. https://doi.org/10.3390/s23020947

[2] Yafooz, W.M.S., Emara, A.H.M. and Lahby, M. (2022) Detecting Fake News on COVID-19 Vaccine from YouTube Videos Using Advanced Machine Learning Approaches. In: Lahby, M., Pathan, A.S.K., Maleh, Y. and Yafooz, W.M.S., Eds., *Combating Fake News with Computational Intelligence Techniques*, Springer, Cham, 421-435. https://doi.org/10.1007/978-3-030-90087-8_21

[3] Buzdugan, A. and Căpățână, G. (2023) The Trends in Cybersecurity Maturity Models. In: Ciurea, C., Pocatilu, P. and Filip, F.G., Eds., *Education, Research and Business Technologies*, Springer, Singapore, 217-228. https://doi.org/10.1007/978-981-19-6755-9_18

[4] Albarraq, A., Alkayyal, A. and Bawareth, R. (2023) Risk Management Framework Analysis. *Int J Eng Tech Inf*, **4**, 1-8.

[5] 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

[6] 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

[7] Shamshad, H., Ullah, F., Ullah, A., Kebande, V.R., Ullah, S. and Al-Dhaqm, A. (2023) Forecasting and Trading of the Stable Cryptocurrencies with Machine Learning and Deep Learning Algorithms for Market Analytics. *IEEE Access*, **11**, 122205-122220. https://doi.org/10.1109/ACCESS.2023.3327440

[8] Kitsios, F., Chatzidimitriou, E. and Kamariotou, M. (2023) The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability*, **15**, Article 5828. https://doi.org/10.3390/su15075828

[9] 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

[10] Enshassi, M.S.A., Walbridge, S., West, J.S. and Haas, C.T. (2019) Integrated Risk

Management Framework for Tolerance-Based Mitigation Strategy Decision Support in Modular Construction Projects. *Journal of Management in Engineering*, **35**, Article ID: 5019004. https://doi.org/10.1061/(ASCE)ME.1943-5479.0000698

[11] Seifi Azad Mard, H.R., Estiri, A., Hadadi, P. and Seifi Azad Mard, M. (2017) Occupational Risk Assessment in the Construction Industry in Iran. *International Journal of Occupational Safety and Ergonomics*, **23**, 570-577. https://doi.org/10.1080/10803548.2016.1264715

[12] Abootorabi, S.M., Mehrno, H. and Omidvari, M. (2014) Proposing a Model for Safety Risk Assessment in the Construction Industry Using Gray Multi-Criterion Decision-Making. *Journal of Health and Safety at Work*, **4**, 67-74.

[13] Aminbakhsh, S., Gunduz, M. and Sonmez, R. (2013) Safety Risk Assessment Using Analytic Hierarchy Process (AHP) during Planning and Budgeting of Construction Projects. *Journal of Safety Research*, **46**, 99-105. https://doi.org/10.1016/j.jsr.2013.05.003

[14] Pinto, A., Nunes, I.L. and Ribeiro, R.A. (2011) Occupational Risk Assessment in Construction Industry—Overview and Reflection. *Safety Science*, **49**, 616-624. https://doi.org/10.1016/j.ssci.2011.01.003

[15] Gunhan, S. and Arditi, D. (2005) International Expansion Decision for Construction Companies. *Journal of Construction Engineering and Management*, **131**, 928-937. https://doi.org/10.1061/(ASCE)0733-9364(2005)131:8(928)

[16] Yahya, A.E., Gharbi, A., Yafooz, W.M.S. and Al-Dhaqm, A. (2023) A Novel Hybrid Deep Learning Model for Detecting and Classifying Non-Functional Requirements of Mobile Apps Issues. *Electronics*, **12**, Article 1258. https://doi.org/10.3390/electronics12051258

[17] Mutis, I. and Paramashivam, A. (2019) Cybersecurity Management Framework for a Cloud-Based BIM Model. In: Mutis, I. and Hartmann, T., Eds., *Advances in Informatics and Computing in Civil and Construction Engineering*, Springer, Cham, 325-333. https://doi.org/10.1007/978-3-030-00220-6_39

[18] Hammi, A. and Bouras, A. (2018) Towards Safe-BIM Curricula Based on the Integration of Cybersecurity and Blockchains Features. 12*th International Technology, Education and Development Conference*, Valencia, 5-7 March 2018, 2380-2388. https://doi.org/10.21125/inted.2018.0453

[19] Parn, E.A. and Edwards, D. (2019) Cyber Threats Confronting the Digital Built Environment: Common Data Environment Vulnerabilities and Block Chain Deterrence. *Engineering, Construction and Architectural Management*, **26**, 245-266. https://doi.org/10.1108/ECAM-03-2018-0101

[20] Creado, Y. and Ramteke, V. (2020) Active Cyber Defence Strategies and Techniques for Banks and Financial Institutions. *Journal of Financial Crime*, **27**, 771-780. https://doi.org/10.1108/JFC-01-2020-0008

[21] Mok, A. and Saha, R. (2017) Strategic Risk Management in Banking. *Deloitte Insights Magazine*, **1**, 1-16.

[22] Alshammari, A. (2023) A Novel Security Framework to Mitigate and Avoid Unexpected Security Threats in Saudi Arabia. *Engineering, Technology & Applied Science Research*, **13**, 11445-11450. https://doi.org/10.48084/etasr.6091

[23] Du Toit, G., Burns, M., Johnson, B., Sidebottom, P. and De Gooyer, C.H. (2012) Customer Loyalty in Retail Banking: Global Edition. Bain Company.

[24] Patel, K. and McCarthy, M.P. (2000) Digital Transformation: The Essentials of e-Business Leadership. McGraw-Hill, New York.

[25] Kebande, V.R. and Ikuesan, R.A. (2020) Virtual Sensor Forensics. *Proceedings of the 2nd International Conference on Intelligent and Innovative Computing Applications*, Plaine Magnien, 24-25 September 2020, 1-6. https://doi.org/10.1145/3415088.3415117

[26] Mukherjee, A. and Nath, P. (2003) A Model of Trust in Online Relationship Banking. *International Journal of Bank Marketing*, **21**, 5-15. https://doi.org/10.1108/02652320310457767

[27] Olanrewaju, T. (2014) The Rise of the Digital Bank. McKinsey Digital Blue.

[28] Alkhaldi, A.N. (2016) Adoption of Mobile Banking in Saudi Arabia: An Empirical Evaluation Study. *International Journal of Managing Information Technology*, **8**, 1-14. https://doi.org/10.5121/ijmit.2016.8201

[29] Ramady, M.A. (2010) The Saudi Arabian economy: Policies, Achievements, and Challenges. Springer, New York. https://doi.org/10.1007/978-1-4419-5987-4

[30] 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 *2nd International Conference on Smart Computing and Electronic Enterprise* (*ICSCEE*), Cameron Highlands, 15-17 June 2021, 84-89. https://doi.org/10.1109/ICSCEE50312.2021.9498045

[31] 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

[32] 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

[33] Aldhaqm, A., Abd Razak, S. and Othman, S.H. (2018) Common Investigation Process Model for Database Forensic Investigation Discipline. 1*st ICRIL-International Conference on Innovation in Science and Technology*, Kuala Lumpur, 20 April 2015, 297-300.

[34] 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

[35] 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

[36] 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

[37] 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

[38] 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

[39] Yafooz, W.M.S., Al-Dhaqm, A. and Alsaeedi, A. (2023) Detecting Kids Cyberbully-

ing 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*, Springer, Cham, 255-267. https://doi.org/10.1007/978-3-031-21199-7_18

[40] 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

[41] 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

[42] 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

[43] 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

[44] 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

[45] Saleh, M., *et al*. (2023) A Metamodeling Approach for IoT Forensic Investigation. *Electronics*, **12**, Article 524. https://doi.org/10.3390/electronics12030524

[46] 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., *IRICT* 2021: *Advances on Intelligent Informatics and Computing*, Springer, Cham, 473-482. https://doi.org/10.1007/978-3-030-98741-1_39

[47] Al-Dhaqm, A.M.R. (2019) Simplified Database Forensic Invetigation Using Metamodeling Approach. Ph.D. Thesis, University Teknologi Malaysia, Kuala Lumpur.

[48] Alshammari, A. (2023) Detection and Investigation Model for the Hard Disk Drive Attacks Using FTK Imager. *International Journal of Advanced Computer Science and Applications*, **14**, 9. https://doi.org/10.14569/IJACSA.2023.0140784

[49] 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

[50] 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

[51] 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*, Langkawi, 21-22 November 2018, 75-80. https://doi.org/10.1109/AINS.2018.8631468

[52] 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*, **12**, 386-394. https://doi.org/10.19026/rjaset.12.2377

[53] 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.

[54] 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., *IRICT* 2017: *Recent Trends in Information and Communication Technology*, Springer, Cham, 141-154. https://doi.org/10.1007/978-3-319-59427-9_16

[55] 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* (l*ICIST* 2015), Kuala Lumpur, 20 April 2015, 364-367.

[56] 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

[57] Alotaibi, F., Al-Dhaqm, A. and Al-Otaibi, Y.D. (2023) A Conceptual Digital Forensic Investigation Model Applicable to the Drone Forensics Field. *Engineering, Technology & Applied Science Research*, **13**, 11608-11615. https://doi.org/10.48084/etasr.6195

[58] Bermell-Garcia, P. (2007) A Metamodel to Annotate Knowledge Based Engineering Codes as Enterprise Knowledge Resources. PhD Thesis, Cranfield University, Cranfield.

[59] Kott, A. (2023) Autonomous Intelligent Cyber Defense Agent (AICA): A Comprehensive Guide. Springer, Cham. https://doi.org/10.1007/978-3-031-29269-9

[60] Kleijnen, J.P.C. and Deflandre, D. (2006) Validation of Regression Metamodels in Simulation: Bootstrap Approach. *European Journal of Operational Research*, **170**, 120-131. https://doi.org/10.1016/j.ejor.2004.06.018

[61] Biles, W.E., Kleijnen, J.P.C., Van Beers, W.C.M. and Van Nieuwenhuyse, I. (2007) Kriging Metamodeling in Constrained Simulation Optimization: An Explorative Study. 2007 *Winter Simulation Conference*, Washington DC, 9-12 December 2007, 355-362. https://doi.org/10.1109/WSC.2007.4419623

[62] Sargent, R.G. (2015) Model Verification and Validation. In: Loper, M., Ed., *Modeling and Simulation in the Systems Engineering Life Cycle*, Springer, London, 57-65. https://doi.org/10.1007/978-1-4471-5634-5_6

[63] Nordstrom, G., Sztipanovits, J., Karsai, G. and Lédeczi, Á. (1999) Metamodeling-Rapid Design and Evolution of Domain-Specific Modeling Environments. *Proceedings ECBS'*99: *IEEE Conference and Workshop on Engineering of Computer-Based Systems*, Nashville, 7-12 March 1999, 68-74.

[64] Cawley, G.C. and Talbot, N.L.C. (2004) Fast Exact Leave-One-Out Cross-Validation of Sparse Least-Squares Support Vector Machines. *Neural networks*, **17**, 1467-1475. https://doi.org/10.1016/j.neunet.2004.07.002

[65] Ellison, D., Ikuesan, A.R. and Venter, H. (2019) Description Logics and Axiom Formation for a Digital Forensics Ontology. *European Conference on Information Warfare and Security*, *ECCWS*, 2019, Coimbra, 4-5 July 2019, 742-XIII.

[66] Jazzar, M. and Hamad, M. (2022) Comparing HDD to SSD from a Digital Forensic Perspective. In: Agarwal, B., Rahman, A., Patnaik, S. and Poonia, R.C., Eds., *Proceedings of International Conference on Intelligent Cyber-Physical Systems*, Springer, Singapore, 169-181. https://doi.org/10.1007/978-981-16-7136-4_14

[67] Ahmad, M.N., Colomb, R.M. and Sadiq, S.W. (2010) A UML Profile for Perdurant Ontology of Domain Interlocking Institutional Worlds. *International Journal of Internet and Enterprise Management*, **6**, 213-232. https://doi.org/10.1504/IJIEM.2010.032170