Egyptian Informatics Journal 22 (2021) 193–199

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Adopting security maturity model to the organizations' capability model

Osamah M.M. Al-Matari [a], Iman M.A. Helal [a,*], Sherif A. Mazen [a], Sherif Elhennawy [b]

[a] Dept. of Information Systems, FCI, Cairo University, Giza, Egypt
[b] Information Systems Auditing Consultant, Egypt

ARTICLE INFO

Article history:
Received 2 October 2019
Revised 28 June 2020
Accepted 9 August 2020
Available online 31 August 2020

Keywords:
Security maturity
Security controls
Maturity assessments
Capability process
Cybersecurity

ABSTRACT

Each organization faces threats and risks in daily operations. One of the main risks is how to assess the security level to protect from the increasing risks associated with technology evolution. So, organizations can specify the required approaches and skills. In this paper, we propose a security maturity model that classifies the organizations into five levels. Each level determines the technologies and process capability used by the organizations. There is a set of factors that can help in determining the security maturity level, such as technology, people, and infrastructure. This paper adopts an Information Security Management model to assess organization's security level. The authors make a correspondence between maturity levels and security levels in an organization. Also, the proposed process capability controls influence both levels. The proposed model helps the organizations bridging the cybersecurity gaps. These gaps relate to talent, technology, organizational units, financial, management and operations gaps. Thus, the model helps the cybersecurity auditors to create a comprehensive plan for measuring the security level of the organization. This plan can manage and develop the organization's automated countermeasures. Also, it can help in applying the suitable standard and framework based on the organization's daily operation. Cybersecurity auditors use cybersecurity techniques and tools to assess the organization's postures. Finally, the authors applied the security maturity controls in two case studies: retirement organization and public telecommunication corporation in the Republic of Yemen.

1. Introduction

A cybersecurity assessment is crucial for every organization developing its business. We need to identify the team who should apply the cybersecurity maturity assessment. The cybersecurity auditing team consists of cybersecurity professionals and IS auditors. They are responsible to determine the organization's posture for stakeholders [1]. They perform four main checks to assess the security maturity levels.

First step specifies a set of processes such as the document management, system, and business audit, design, and evolution. Second step addresses the strategic management. It consists of a group of processes such as stakeholder's report, coordination of information security and physical security, strategic vision, resources allocated for information security. Third check targets the tactical management. It consists of 11 processes such as background checks, service level management, insurance management, security personnel selection and training, and security awareness. Finally, the fourth check states the operational management processes. It consists of 25 processes such as inventory management, environment patching, security measures, change control, access control, information quality, compliance probing, forensics, etc.

These processes govern the level of security maturity. They must be finished before realizing the security standards or framework. They specify the required controls at each level. There are three approaches to perform cybersecurity controls. Either offensive, defensive or mix of both approaches. The offensive approach applies ethical hacking techniques. But, the defensive approach prevents, detects and responds to potential attacks [2]. Moreover, there are three main levels of management in each organization. They are operation management (low-level management), executive management (middle-level management), and higher management (top-level management) [3].

There are various terminologies to state the levels of maturity as defined in organizations and frameworks [4]. Yet, most frameworks express maturity into the following levels: non-existent (level 0), ad hoc (level 1), repeatable (level 2), defined (level 3), managed (level 4) and optimized (level 5) [3]. There are several factors affecting the organization's security vision, such as the different context/environments, a variety of available resources, and

* Corresponding author.
E-mail addresses: osamahalmatari@gmail.com (O.M.M. Al-Matari), i.helal@fci-cu.edu.eg (I.M.A. Helal), s.mazen@fci-cu.edu.eg (S.A. Mazen).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

https://doi.org/10.1016/j.eij.2020.08.001

the specified security targets. The security maturity assessment clarifies the relationship between information systems management, and the identified social and technical factors [4].

The governmental sectors secure their online operations for several e-government services. They use Information Security Maturity Model (ISMM) [5]. ISMM addresses both technical and non-technical security aspects. In [5], the authors presented a comparative study of cybersecurity auditing tools and auditing frameworks. These automated tools can help the cybersecurity auditors to fulfil the auditing process. However, these tools have limitations, such as usage difficulties, a lack of adequate knowledge and insights into relevant practices and parameters [6]. Those missing insights would help in improving business information security. They can assess the current posture and develop the organization's security [7].

In this paper, we propose a security maturity model to assesses an organization based on specific rules specified in the ISM3 model. This model allows dividing the organizations into five levels of security maturity. The classification level depends on the type of controls and the level of automation supported in the organization. These controls can be either *nonexistence*, *ad hoc*, *repeatable*, *defined*, *managed*, or *optimized* [8]. Cybersecurity auditors collect information about the used technology, tools, techniques resources, number of the employees and infrastructure to determine the organization's security maturity level.

Our proposed model is adapted from ISM3 model and applied on two case studies. Our proposed model analyzes ISM3's output reports. Then, it determines whether the organization at a suitable security level or need to develop the security procedures. Moreover, our model takes the ISM3 as a guide to document the security maturity level. This model applies to small, medium, and large organizations. Based on the result of security maturity level, we can perform the cybersecurity methodology such as reconnaissance, footprint, enumeration, scanning and penalties on the organizations.

The proposed model differs from previous security models. It studies the security automation aspects of the organization. Also, it consolidates the security level on organizations with vulnerabilities countermeasures. It determines a set of required documents to perform the suitable controls. Then, it identifies the automated controls instilled through a set of procedures. Finally, it aligns the suitable security maturity level according to the organization's activities. Thus, the maturity level is suitable for the organization's hardware and software capabilities.

The remainder of this paper is organized as follows. An overview of the existing security maturity models and a discussion of related work in Section 2. Section 3 discusses the proposed security maturity model. The proposed security maturity levels are applied on two case studies: retirement department and public telecommunication corporation in Yemen in Section 4. Section 5 discusses the gaps in the existing models and frameworks in comparison to the proposed model. Finally, we conclude the paper in Section 6 with an outlook for the future work.

2. Related work

In [9], the authors have proposed the characterizing Organizations Information Security for Small and medium enterprise (CHOISS) model. They determine measurable organizational characteristics in four categories through 47 parameters. Examples of these parameters are the number of employees, the organization's revenue, the percentage of sourced software development and confidentiality, and availability of critical data. It helps Small and Medium Enterprises (SMEs) distinguish and rank which risks need mitigation. It categorizes the actions associated with the organizational characteristics into: general, in-sourcing and outsourcing, IT dependency, and IT complexity.

CHOISS presents the distinction between a variety of different organizations. To reach a high IS maturity level, an organization must address a tailored set of focus areas and capabilities. Another research considered only the data security associated with Confidential, Integrated, and Availability (CIA) [10]. They ignored digital security process of appraising risks and vulnerabilities for each level of Capability of Maturity Model (CMM).

According to [11], the author presented the Cybersecurity Capability Maturity Model (C2M2) to evaluate an organization's cybersecurity capabilities, communicate its capability levels in meaningful terms, and inform the prioritization of its cybersecurity investments. The model divides cybersecurity for the SMEs in three class Maturity Indicator Levels (MILs) 0 to 3 (MIL0, MIL1, MIL3) and divided by 10 domains. The model uses the evaluation to identify gaps in capability, rank those gaps and develop plans to address them, and to set plans to address the gaps.

In [12], authors classify the organizations into five levels of the capability maturity model. These levels classifies the business governance drive as initial, ad hoc, defined, managed, and optimized. This classification focuses on the architectures of the organization and skips the risks in each of them. According to [13], the organization's capabilities identify the technological maturity and risk. They identify the affordability of each approach using the best data available. Yet, this study ignores the security process to assess the organization's needs and mitigate the risks.

Another study assessing the information security maturity for Malaysian public sectors in [4]. The authors compared three main models System Security Engineering-Capability Maturity Model (SSE-CMM) [14], Control Objectives for Information and related Technology (COBIT) [15], and the Information Security Management Maturity Model (ISM3) [16]. They clarified the relationship between these models. Then, they identified and tested their technical factors.

The authors of COBIT 2019 framework explained the capability levels for processes [15]. These levels are based on process capability schemes ranging from 0 to 5. The capability level is a measure of how well a process is implemented and performing. COBIT framework focuses on the processes of the organization. It tracks these processes based on classifying the organizations into five levels.

Systems Security Engineering Capability Maturity Model (SSE-CMM) is another model presented in [14]. It studies the software design to support the organization's applications. Also, it gives guidance on how to create controls for their processes to develop and maintain software. This model defines five capability rankings which focus on the software performance controls. Information Security Maturity Model version 3 (ISM3) is another model that defines five ranking levels. These levels measure the information security processes in the organizations [16]. The ISM3 standard specifies the required set of processes to achieve every security maturity level. It summarizes these processes to measure the maturity level in four domains as well as the automation requirements.

In [17], the authors assess the master data to derive the main concepts and best practices which called a master data maturity assessment. This assessment uses the maturity matrix that relates to 13 areas. Also, it specified 65 capabilities and validated them. Moreover, the authors developed an assessment questionnaire to assess master data management maturity. They focused on the master data and ignored the security maturity over all the organization. There are some security frameworks that perform the security controls for the organizations such as NIST and ISO (27001, 27002) [18,19].

NIST performs five security controls for the organizations. These controls are identifying, detecting, protecting, responding, and recovering data and assets. ISO information security management

and code of practice perform 13 security domain controls. These controls cover the general security on organizations.

In [20], the authors compared different cybersecurity maturity models applied on network systems. They explored a variety of cybersecurity maturity models to apply in an organization. They described the maturity levels on each model based on the organization's components. Finally, they deduced that each organization identified the suitable model based on its operation's sector. Another research customizes the cybersecurity maturity model in developing health care sectors [21]. They assessed the cloud security maturity model effectiveness for health care organizations. Finally, they deduced the suitable standard to align with the best practices of health information systems.

Authors in [22] addressed the methods to improve the assessment of risk management and cybersecurity maturity. They studied how to integrate them in the software solutions. Their target was governmental sector. They aimed for achieving a suitable information security for internal operations. Another study [23] explained the embodiment ability to include completing a maturity assessment. They identified the vulnerabilities on a computer system by using the risk profile database. The assessment included determining five levels of maturity levels. The authors applied a set of different unique risk scenarios to assess the maturity level.

Furthermore, there are several international corporation's offices located in Yemen. These corporations conduct cybersecurity and IS auditing frameworks. These frameworks assess the level of security on the organizations. As part of our study, we checked Deloitte, KPMG and Moore Stephens offices (Yemen branches). These offices audit the cybersecurity and information systems of the medium-to-large Yemen's organizations. They use models such as COBIT 5 to audit the organizations. Yet, these models do not identify the security maturity for the organizations. Our proposed model aims to bridge this gap. It assesses the organization's applications, hardware and software to ensure its security controls.

As a conclusion, there are no clear procedures to assess the security maturity level in different kinds of enterprises. Moreover, the effectiveness of using automated controls to secure the whole enterprise needs more investigation. Finally, there is no comprehensive cybersecurity maturity model to help cybersecurity auditors in assessing all aspects of the enterprise's security.

3. Proposed cybersecurity maturity model

The proposed cybersecurity maturity model can analyze the current state, with a view towards the desired state. It assesses cybersecurity controls, and realize new technology or process controls. The main advantage of using such a model is to specify the maturity level of the organization. Each level depends on a group of processes. Each process can depend on the infrastructure, resources, operation's automation, and user's knowledge. Hence, cybersecurity maturity models can help to distinguish between organizations [24].

Cybersecurity editors begin to assess the enterprise security level by checking its controls. These controls can be *nonexistence* where the organization lacks or has no controls. They can be *ad hoc* controls which are poor and rarely controlled by the organization. Also, controls can be *repeatable*, where the organization is aware of user controls in the regular processes. Controls are *defined* when the organization automates them on its daily operations. Whenever the organization is developing the automation controls, they become *managed*. Finally, *optimized* controls are automated controls for all operation processes [8].

Fig. 1 illustrates the level of organizations based on the applied controls from the process capability model such as ISM3 [25]. It focuses on five process maturity levels, according to the organization's controls. The *nonexistence* maturity level refers to the absence of security and lack of automated controls in the organization. The *ad hoc* maturity level uses the automated security controls in the exceptional operations only. The *repeatable* maturity level develops automated security controls based on the current cybersecurity awareness. The *defined* maturity level begins to identify the cybersecurity controls, techniques and required technologies to secure the organization. The *managed* maturity level develops the technology needed to automate security controls. The *optimized* maturity level applies the automated security controls to protect the organization from inside and outside threats.

ISM3 specifies the level of organizations based on the controls applied through daily operations. This ranges from lack of controls to fully automated controls. The supported controls reflect the level of security maturity in the organization. It ranges from the *non-existent* to *optimized* maturity. Cybersecurity auditors need to learn how to classify the organizations based on the security maturity model.

The security maturity level is specified based on some factors. These factors can be physical and network infrastructure, the capability of implementing the daily processes, data storage and transfer controls, or quality assurance (policies, standards, and guidance). In this paper, we apply the proposed security maturity model based on ISM3 model to classify the organization's security maturity. Each security need has a set of processes to perform the security maturity levels. We introduce these procedures through the case studies, see Section 4. We assess the security level from four point of views: general, tactical, strategic, and operational. These views help deciding the organization's needs of security skills and standards alignment.

4. Case studies

Cybersecurity auditors must specify the level of security in the organizations to complete the auditing processes. In Sections 4.1 and 4.2, we are studying how to realize and assess the security maturity levels into two types of organizations. The assessment is based on four categories which are general, operational, tactical, and strategy security maturity. Finally, Section 4.3 presents a discussion about all the findings.

4.1. First case study: Retirement organization

Retirement organization is a public service organization in Yemen. It serves more than 100 thousand people. It has four main departments. They are Information Technology, finance, control and audit, and pension administration departments. We studied the security level to fulfill the security gaps according to security maturity model control. It has a limited number of processes that perform the daily operations.

There are several processes in this organization, but it has two main processes: (1) pay the salary for retires every month, and (2) perform the filing procedures to give them a credit card. Yet, there are no standards or frameworks applied in the security domain. Hence, they specify some physical controls and administrative policies for securing the organization.

Physical controls are responsible for implementing hardware-related security controls. An example is isolating the server's room and bio-metrics system to prevent unauthorized people to reach the server's room. Most of the performed processes and procedures controls operate manually. So, the administration categorizes the users based on the levels of authorization and privileges. They try to automate these processes and procedures. But, the security issues are not a priority in the organization.

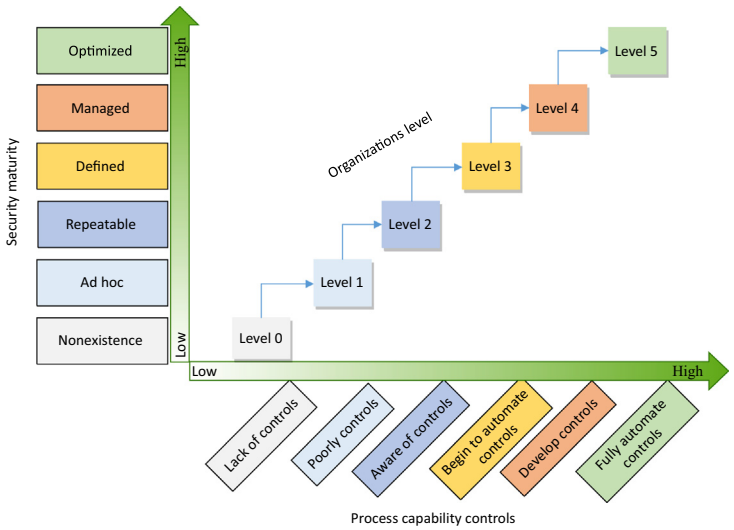

Fig. 1. Proposed Security Maturity Model based on ISM3 [4].

4.2. Second case study: Public Telecommunication Corporation

Public Telecommunication Corporation (PTC)[1] is a Yemeni corporation. It works on telecommunication and executes a complicated process. PTC has 21 branches and more than 50 centers to serve million customers in Yemen. It is a government service provider for Internet and telecommunication to personal and business. Some of their services are pay-for-me (hatfie), internet services (yemennet), training services, information systems, and technology services. The number of internet users in Yemen at the end of the year (2019) has increased to 3 million users. This is in comparison to 2 million users at the previous year (2018) with an increase in the growth by 49.96%.

The PTC daily processes are more complex than the processes of retirement organization. Also, the number of daily processes is increasing to accommodate the customer's needs. The security is a priority for corporation work in the telecommunication domain. Thus, PTC endeavors to enhance its security to attract more customers. The processes and procedures of the PTC corporation are semi-automated as well. Based on the proposed security maturity model, we studied the security maturity level of its departments. So, we recommend complete automation of the security controls to increase the security maturity level.

4.3. Case studies discussions

There are four types of security in the proposed security maturity model: general, strategic, tactical, and operational. Table 1 shows the processes of security maturity assessment of the general processes. These processes are (1) document management, (2) ISM3 system and business audit, and (3) ISM3 design and assess the security level. Note that the two case studies are represented as: (R) for **r**etirement organization and (T) for public **t**elecommunication corporation. The rest of the discussion apply the same notations.

Table 2 shows a set of processes to assess the security maturity of corporations or organizations. These processes focused on security strategic management. They consist of four processes: (1) report to stakeholders, (2) coordinate information security and physical security, (3) strategic vision, and (4) allocate resources for information security.

Table 3 explains the processes to achieve tactical management security maturity. Tactical management assessment consists of eleven processes. These processes are (1) report to strategic management, (2) manage allocated resources, (3) define security targets, (4) service level management, (5) define environments and life-cycles, (6) insurance management, (7) background checks, (8) security personnel selection, (9) security personnel training, (10) disciplinary process, and (11) security awareness. These processes help the IS auditors to assess the level of each organization.

Table 4 shows the operational management processes. They help the cybersecuriy auditors to assess the daily operations' processes. The operational management consists of 23 processes. Each process is vital for assessing the security maturity in the daily operations of the organization.

All tables illustrate the maturity level for both case studies. Both the retirement organization and PTC apply all the functions of general security. The retirement organization accomplishes half the functions of the strategic security management, while PTC covers them all. On the tactical security, the retirement organization fulfills 3 out of its 11 functions, while PTC fulfills them all. On the operational security, the retirement organization achieves 4 out of its 23 functions, while PTC achieves 18 functions.

Finally, we summarize the security maturity results from previous Tables 1–4. Each organization from the case studies can be categorized as follows:

Retirement Organization is on an *ad hoc* level with no regular controls. It does not follow security control standard or framework. The output of security level which complies with ISM3 model is not enough to realize their security goals. It needs clear rules for the separation of duties. These rules can improve the resources usage and reduce the risk of security incidents. Thus, protect the organization from possible internal threats.

PTC corporation is on a *defined* level of maturity. This is a good security control. It begins to automate its processes inside the corporation and its branches. They apply the ISO 27001 standard in the payment card industry (PCI) for its processes and security controls. Thus, the output of their security level complies with ISM3 model. Yet, protecting physical and technical information need alignment with the existing standards.

[1] http://ptc.gov.ye/en/Home.aspx.

Table 1
General Security Maturity.

	Maturity Level				
Process	Level 1	Level 2	Level 3	Level 4	Level 5
Document Management	R		T		
ISM3 System and Business Audit	R		T		
ISM3 Design and Assess Security Levels	R		T		

Table 2
Strategic Management Security Maturity.

	Maturity Level				
Process	Level 1	Level 2	Level 3	Level 4	Level 5
Report to Stakeholders	R		T		
Coordinate information/physical security	R		T		
Strategic vision			T		
Allocate resources for information security			T		

Table 3
Tactical Management Security Maturity.

	Maturity Level				
Process	Level 1	Level 2	Level 3	Level 4	Level 5
Report to strategic management			T		
Manage allocated resources	R		T		
Define Security Targets			T		
Service Level Management			T		
Define environments and life-cycles	R		T		
Insurance Management			T		
Background Checks			T		
Security Personnel Selection	R		T		
Security Personnel Training			T		
Disciplinary Process			T		
Security Awareness			T		

Table 4
Operational Management Security Maturity.

	Maturity Level				
Process	Level 1	Level 2	Level 3	Level 4	Level 5
Report to tactical management	R		T		
Select tools for implementing security measures			T		
Inventory Management	R		T		
Information Systems Environment Change Control			T		
Environment Patching			T		
Segmentation and Filtering Management			T		
Security Measures Change Control					
Software Development Life-cycle Control			T		
Malware Protection Management			T		
Access control	R		T		
User Registration	R		T		
Physical Environment Protection Management			T		
Backup Management					
Enhanced Reliability and Availability Management					
Operations Continuity Management			T		
Archiving Management			T		
Internal Technical Audit			T		
Incident Emulation			T		
Information Quality and Compliance Probing					
Alerts Monitoring			T		
Events Detection and Analysis			T		
Handling of incidents and near-incidents			T		
Forensics					

4.3.1. Retirement organization findings

1. Retirement organization is in level 1 of security maturity.
2. It has a poor implementation of their controls and processes.
3. It uses old technologies to perform the daily operation without updating security patches.
4. It lacks the security professionals. They can handle the threats and detect the vulnerabilities as well as prevent the exploit to reduce the risks.
5. It has a limited number of resources to perform the daily operations.

6. There are no security procedures to protect its assets, so it cannot prevent data from leakage or loss.
7. It lacks the security awareness such as physical, administrative, and technical controls.

4.3.2. PTC findings

1. PTC is in level 3 of security maturity mapping.
2. It detects and responds to the threats and risks with a suitable response.
3. It uses a set of modern technologies (such as firewalls, advanced protection from viruses and malware, intrusion prevention and detection system, and endpoint prevention of assets) to protect their daily data transmissions.
4. It has some security professionals who work in different departments to secure the systems and networks.
5. There is a huge number of resources in PTC which aid in developing the daily operations.
6. It endeavors to back up the data on a monthly-basis to recover them in case of any possible disaster.
7. Its management has a medium level of security awareness and aims for improving its plans to enhance its security maturity level.

As a recommendation, the retirement organization can review its security functions to raise the security awareness. Thus, it can improve its security maturity level to level 2 based on the proposed security maturity model in Fig. 1. Whereas PTC needs to complete the development of its controls to raise its security maturity level to level 4. Due to the risks met on daily operations, it needs to invest in the security controls to face the possible complicated threats. It can also consider the full automation of the security functions to improve its security maturity level to level 5.

5. Discussion of security maturity gaps

Based on previous results, the security maturity level is an important factor in auditing an organization. Yet, there are gaps in the existing tools when determining the required security level per each organization. The maturity level depends on a set of input documents affecting the audit controls. The organization's maturity affects the support level of process capability controls.

Our proposed model can determine the security maturity level of the organization. It can also bridge the gaps in organization's audit controls. There are five organizational levels of maturity. The initial level of security maturity starts with the *lack of controls* in the operations. Thus, it highlights any existence threats. This requires to establish security concepts to protect the assets in general. The first level elevates to *poorly controls* that are performed in emergency cases and lack in the daily operations. It rechecks the unit's controls to secure them.

The differences in security maturity among organizational units is one of the security gaps in an organization. These units rate IT teams as the most secured and the sales teams as the least secured. The second level *aware of the controls* is vital to determine the talent gap. It considers the cybersecurity teams and their struggles. This level have to overcome the gap between the required and the available security talents within the organization. The third level of security maturity is *commence to automate the controls*. It adapts the solutions to cover the technologies gap.

The fourth level *develop controls* expands to new controls. This level addresses the budget gap. There is a disagreement between the amount of budget required to secure the organization and the available funds. The management's main focus can affect the decisions taken to bridge this gap. Meanwhile, the organization's preparation for cyber-attacks and threats is threaten. Finally, the fifth level *fully automated controls* adapts the gaps between the management and operations. This level addresses the perception gap between executive management and security operations management. If this gap is resolved, the organizations can lead the way to close the other gaps.

6. Conclusion and future work

Cybersecurity is becoming one of the raising issues that most organizations aim for. Cyber-attacks have different shapes and targets. Thus, it is difficult for a security staff to manage them without proper and extensive training. The organization's system maturity plays a main factor in providing cybersecurity. Cybersecurity auditing is one of the critical tasks in an organization. It is a difficult and extensive task that needs technical support for performing it. It helps in classifying the level of security in the organization. To assess the organization's security maturity level, cybersecurity auditor can apply the proposed security model according to standards, tools, and techniques.

The proposed security maturity model can assign the organization to a suitable level based on the automated controls. This model uses the resources and requirements process as an indicator of the organization's security levels. Depending on the organization's security maturity level, the cybersecurity auditor can arrange the reports to the organization. Then, the auditor can make recommendations to raise its security level. Thus, the proposed model adapted from ISM3 model corresponds to the maturity levels to bridge the cybersecurity gaps. These gaps relate to talent, technology, organizational units, financial, management and operational gaps.

As a future work, this model can improve and alter these controls according to the generated security reports. This can aid the organization in decreasing possible risks and enhance its security maturity level.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Alles M, Brennan G, Kogan A, Vasarhelyi MA. Continuous monitoring of business process controls: a pilot implementation of a continuous auditing system at Siemens. Int J Acc Inf Syst 2006;7(2):137–61. doi: https://doi.org/10.1016/j.accinf.2005.10.004.
[2] Robinson J. Governance challenges at the intersection of space and cybersecurity. Secur Cyberspace 2016:156.
[3] Josey A. TOGAF® Version 9.1-A Pocket Guide, Van Haren; 2016..
[4] Dzazali S, Hussein Zolait A. Assessment of information security maturity: an exploration study of malaysian public service organizations. J Syst Inf Technol 2012;14(1):23–57.
[5] Karokola G, Kowalski S, Yngström L. Towards an information security maturity model for secure e-government services: a stakeholders view. HAISA 2011:58–73.
[6] Almatari O, Helal I, Mazen S, Elhenawy S. Cybersecurity tools for IS auditing. In: The 6th International Conference on Enterprise Systems. p. 8. Limassol, Cyprus.
[7] Bobbert Y. Improving the maturity of business information security [Ph.D. thesis]. University of Antwerp; 2018..
[8] Karanja E. The role of the chief information security officer in the management of it security. Inf Comput Secur 2017;25(3):300–29.
[9] Mijnhardt F, Baars T, Spruit M. Organizational characteristics influencing SME information security maturity. J Comput Inf Syst 2016;56(2):106–15. doi: https://doi.org/10.1080/08874417.2016.1117369.
[10] Garg D, Jia L, Datta A. Policy auditing over incomplete logs. In: Proceedings of the 18th ACM conference on Computer and communications security – CCS '11. p. 151. doi: https://doi.org/10.1145/2046707.2046726.
[11] Curtis P, Mehravari N, Stevens J. Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services), Version 1.0, Defense Technical Information Center. .
[12] Lankhorst M. Beyond enterprise architecture. In Enterprise Architecture at Work. Springer; 2013. pp. 303–308. .
[13] Sc JKD, Eng C, Massie A. A framework for a systems engineering body of knowledge. In: 11th International Symposium of the INCOSE Melbourne, Australia. p. 1–7.

[14] White GB. The community cyber security maturity model. In Technologies for Homeland Security (HST), 2011 IEEE International Conference on. IEEE; 2011. pp. 173–178. .
[15] Cobit I. COBIT® 2019 framework: governance and management objectives, ISACA; 2019. URL: www.isaca.org/COBITuse. .
[16] Consortium I, et al. Information security management maturity model; 2009. .
[17] Spruit M, Pietzka K. Md3m: the master data management maturity model. Comput. Human Behav. 2015;51:1068–76.
[18] Stouffer K, Stouffer K, Zimmerman T, Tang C, Lubell J, Cichonski J, McCarthy J. Cybersecurity framework manufacturing profile. US Department of Commerce, National Institute of Standards and Technology; 2017.
[19] ISO. ISO/IEC 27002:2013 Information technology – Security techniques – code of practice for information security controls; 2013. URL: https://www.iso.org/standard/54533.html. .
[20] Mohammed I, Bade AM. Cybersecurity capability maturity model for network system. Int J Develop Res 2019;9(07):28637–41.
[21] Akinsanya OO, Papadaki M, Sun L. Current cybersecurity maturity models: how effective in healthcare cloud? In: CERC. p. 211–22.
[22] Heckman RC, Chandler DK. Methods and systems for providing an integrated assessment of risk management and maturity for an organizational cybersecurity/privacy program, uS Patent App. 16/227,109 (Jul. 4 2019). .
[23] Grindstaff IED, Loeb MS, Hood K, Witte G, Conkle T. Cybersecurity maturity assessment, uS Patent App. 16/226,117 (Jul. 25 2019). .
[24] Miron W, Muita K. Cybersecurity capability maturity models for providers of critical infrastructure. Technol Innov Manage Rev 4(10). .
[25] Siponen M, Willison R. Information security management standards: problems and solutions. Inf. Manage. 2009;46(5):267–70.