Journal of Theoretical and Applied Information Technology
31st July 2025. Vol.103. No.14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CYBERSECURITY ASSESSMENT FRAMEWORK FOR HEALTHCARE INSTITUTIONS PRE-MEDICAL CYBER-PHYSICAL SYSTEM ADOPTION

MOHAMED AWADA ELMAGBARI, MAHEYZAH MD SIRAJ, SITI HAJAR OTHMAN
Universiti Teknologi Malaysia, Jalan Iman, 81310 Skudai, Johore, Malaysia
E-mail: ganbory123@gmail.com, maheyzah@utm.my, hajar@utm.my

ABSTRACT

Medical cyber-physical systems enable the remote monitoring of patients, thereby enhancing accessibility to care. Unfortunately, secure adoption is still difficult, as this remains an unresolved topic that includes cybersecurity and privacy issues. While a number of frameworks exist in the general realm of CPS cybersecurity readiness, few frameworks address the healthcare domain. This study proposes a Cybersecurity Assessment Framework (CAF) together with a quantitative scorecard to assess cybersecurity readiness before healthcare institutions embark on MCPS adoption. Meta-analysis of existing frameworks, coupled with expert interviews, has resulted in five Critical Success Factors (CSFs) being established: reliability, validity, third-party authentication, security, and transparency. Furthermore, a case study approach was adopted with IT managers and healthcare professionals of two Libyan hospitals. Results indicated that the CAF is valid and usable and supports the secure adoption of MCPS, though privacy remains a concern. This work presents a novel, domain-specific CAF for healthcare cybersecurity, followed by tools nurturing IT governance.

Keywords: *Critical Success Factors, Cyber-Physical Systems, Cybersecurity Assessment Framework, Healthcare Industry, Medical Cyber-Physical Systems.*

1. INTRODUCTION

Cyber-physical systems (CPS) comprise software, such as computational applications, and hardware, such as sensing devices, that work together to enable a user to remotely monitor, interact, manipulate, and control tangible items in the real world via a network [1, 2]. As such, it is considered an advancement that could significantly improve intelligent healthcare, traffic, and defence systems among other things. However, there has also been a significant increase in the number of cyber-attacks on CPS [3]. Privacy is another significant issue as the sensitive information being exchanged on these networks can easily be intercepted by unscrupulous third parties [4]. As such, various solutions have been examined to overcome the privacy issues plaguing CPS [5, 6].

In the healthcare industry, at present, patients must be physically present at healthcare institutions for healthcare professionals to assess and treat them. A medical cyber-physical system (MCPS) is a system that uses medical implants and sensors to continuously monitor, measure, and transmit a patient's vitals to healthcare professionals via a network [7]. Under the Health Insurance Portability and Accountability Act (HIPAA), only authorised users can access a patient's health information [8]. However, the data that is being exchanged between these multiple sensor nodes may be intercepted by third parties [9, 10].

Figure 1 provides a detailed layout of a typical MCPS [11]. As seen, it comprises data acquisition, data pre-processing, cloud processing, and action layers. In the data acquisition layer, a wireless body area network collects data from the medical implants and sensors. In the data pre-processing layer, the collected medical data is transmitted to the cloud [12]. In the cloud processing layer, the received data is analysed and stored. Lastly, in the action layer, an actuator (active) or a healthcare professional (passive) will take action based on the results of the analysis. In the present study, the secure adoption of MPCS for both active and passive actions was considered.

Journal of Theoretical and Applied Information Technology
31st July 2025. Vol.103. No.14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

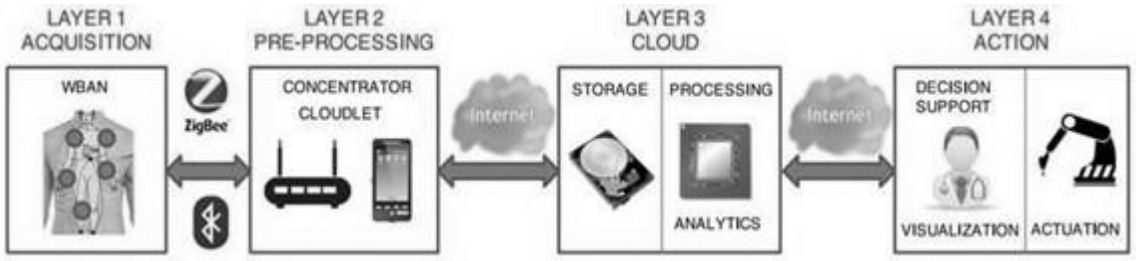

Figure 1. The four layers of a typical medical cyber-physical system (MCPS) [11]

The two most obvious points of failure in MCPS lie in the data acquisition layer and the cloud processing layer. More specifically, the medical implants and sensors in the data acquisition layer have limited computational capabilities and battery life, leading to security and privacy issues during sensor-to-sensor and sensor-to-network communications [13, 14, 15, 16]. Apart from that, storing data in the cloud processing layer enables third parties to exploit data fusion and gain access to valuable information [17].

As such, the present study set out to: (1) identify the critical success factors (CSFs) required to comprehensively assess the cybersecurity readiness of healthcare institutions for MCPS adoption, (2) use the identified CSFs to design a cybersecurity assessment framework (CAF) that healthcare institutions can use to assess their cybersecurity readiness before adopting an MCPS, and (3) develop a scorecard that healthcare institutions can use to assess their cybersecurity readiness against the criteria outlined in the CAF.

The rest of this study is organised as follows. Chapter 2 reviews extant studies on the topic. It reviews existing privacy guidelines as well as tools and techniques that have been used to enhance patient privacy in MCPS. Chapter 3 details the research methodology and the steps taken to identify the CSFs. Chapter 4 details developing the CAF and scorecard as well as discusses the findings of the interviews, which validate the proposed CAF and scorecard. Lastly, the conclusions and recommendations for future studies are provided in Chapter 5.

Even though the MCPS play a vital role in modern healthcare, there are still no tailored frameworks that comprehensively assess the cybersecurity readiness of institutions before adoption. Current cybersecurity frameworks are either generic, industry-specific, or they do not address healthcare-specific risks. This gap poses an urgent question: how can healthcare institutions assess and improve their cybersecurity posture to safely adopt MCPS technology? This study attempts to address the question by developing and validating a healthcare-specific cybersecurity assessment framework and a practical evaluation scorecard.

2. LITERATURE REVIEW

Conventional encryption methods cannot be applied in MCPS as multiple parties, such as the patient, hospital, physician, specialist, pharmacy, and insurance company to name a few, need to be able to access a patient's medical data. As such, role or identity-based access control or attribute-based encryption [18], blockchain [19], and distributed data access control [20] have been proposed to address the security concerns in MCPS, while Health Insurance Portability and Accountability Act (HIPAA)-compatible standards, such as open electronic health records (openEHR) [21] and Health Level Seven International (HL7) [22], have been proposed to increase their resilience. Meanwhile, the American Society for Testing and Materials (ASTM) F2761 proposes a patient-centric architecture for open-source integrated clinical environments (OpenICE) [23, 24].

Other models and frameworks have also been developed to enhance the security of MCPS [14, 25, 26]. Apart from that, solutions have been proposed to prevent cybersecurity attacks on MCPS [27, 28, 29], while others have outlined measures to implement after a security breach has occurred [30]. Schemes that safeguard patient data by allowing patients to give users consent to access their medical data have also been proposed [31, 32, 33].

2.1 Cybersecurity Assessment Frameworks (CAF) for Cyber-Physical Systems (CPS)

A few generic CAFs and models have been developed for CPS, such as the capability maturity

model [34], the Information Systems Audit and Control Association's (ISACA) control objectives for information and related technologies (COBIT) framework [35], the International Standards Organization's (ISO) ISO 27000 and ISO 27001 series for information security management system adoption [36], the European Network and Information Security Agency's (ENISA) guidelines on assessing the security and essential service compliance of digital service providers with the Network and Information Security Directive's (NISD) security requirements [37], the policies, risks, objectives, technology, execute, compliance, and team (PROTECT) information security approach [38], and the National Institute of Standards and Technology's (NIST) special publication (SP) 800-53 on security and privacy controls for federal information systems and organisations [39].

Apart from that, a study presented by [40] proposed a cybersecurity maturity framework for measuring the readiness of higher education institutions in the United Kingdom. In 2017, the researchers [41] published the cybersecurity-culture framework that was developed using seven dimensions: (1) peoples' knowledge, (2) beliefs, (3) attitudes, (4) perceptions, (5) assumptions, (6) values, and (7) norms regarding cybersecurity and how it affects their behaviours with IT. This was, subsequently, developed into a cybersecurity assessment toolkit, which includes the security CLTRe toolkit, which helps organisations assess and graphically represent their security readiness status across these seven dimensions [42]. A study presented by [43] developed a maturity model based on ISO 27001 to improve the implementation of the standard as they found that the standard lacks a detailed plan and may become a burden on organisations. Meanwhile, the researchers [44] proposed a model for assessing the cybersecurity of organisations, which was evaluated and tested against a Canadian cybersecurity model meant for measuring the security awareness of higher education institutions. Apart from that, a study by [45] extended the cybersecurity capacity maturity model proposed by [46] to create a cybersecurity performance evolution management model that enables organisations to create, test, and validate their cybersecurity status. The model of researchers [47], on the other hand, combined the National Institute of Standards and Technology's cybersecurity framework (NIST-CSF), COBIT, and ISO 27001, while the study by [48] reviewed the cybersecurity CMM for providers of critical infrastructure and provided recommendations on employing CMM to measure and communicate readiness.

Meanwhile, the researchers [49] proposed a conceptual model for assessing the cybersecurity readiness of public institutions in Cambodia and other developing countries by measuring their cybersecurity readiness across three dimensions: (1) infrastructure, (2) environment, and (3) human resources. The study by [50] proposed a cybersecurity readiness model that builds a cyber readiness index tool with which to compare the cybersecurity performance of nations in terms of initiatives, policies, and strategies across six factors: (1) economic, (2) culture, (3) legal, (4) infrastructure, (5) institutional, and (6) human development. Lastly, the researcher [51] developed a reference model for measuring the cybersecurity readiness of nations across five dimensions: (1) organisational, (2) legal, (3) cooperation, (4) capacity building, and (5) technical measures and aggregates the results into an overall score [52]. However, these frameworks and models do not focus on healthcare and, therefore, cannot be used to evaluate the cybersecurity readiness of healthcare institutions pre-MCPS adoption.

2.2 Cybersecurity assessment frameworks (CAFs) for medical cyber-physical systems (MCPS)

Only a few CPSs have been developed for the healthcare industry. For example, the study by [53] proposed a secure architecture that yielded an integrated wireless sensor network-cloud-based framework. Meanwhile, [54] offered a modelling analysis of CPS architecture, called CPS-MAS, but failed to examine the privacy and security aspects of the MPCS. Apart from that, the researchers [55] developed a service-oriented MPCS architecture. However, it did not take the security and privacy aspects of healthcare into consideration. Nor did the CPS architecture that was proposed by [56].

Even fewer studies have examined the cybersecurity readiness of healthcare institutions. For instance, the study by [57] developed a framework that comprises an information security control specifications manual and standards and regulations mapping. Although it simplifies compliance efforts of health organisations, there were gaps that were not addressed as healthcare technology improved. Meanwhile, the researchers [58] also developed a framework with which to

determine the current information security maturity level of healthcare institutions. Meanwhile, the Maryland healthcare cybersecurity initiative has a tool that hospitals can use to evaluate their security. However, it is largely manually operated, which is time-consuming and impractical [59]. The cyber readiness index that the Office of the Government Chief Information Officer created to evaluate the cybersecurity readiness of private and public organisations in Hong Kong includes healthcare institutions, but largely focuses on CPS and is meant to be used locally [60].

Apart from that, the global cybersecurity index that the International Telecommunication Union and ABI research developed is mainly for measuring member states' commitment to achieving cybersecurity readiness. As such, it is not intended to be used to measure the cybersecurity readiness of organisations [61]. The Potomac Institute for Policy Studies' cyber readiness index, on the other hand, is generic. As such, it cannot be used to adopt a specific technology. The assessment practices are also ineffective at measuring individual internal security components. As such, they do not depict the overall security level of a healthcare institution. The effects of cloud computing on the healthcare industry were not taken into account either [62]. Lastly, the researchers [63] examined the efficacy of using maturity models to examine the cybersecurity maturity of healthcare institutions that use cloud computing. They concluded that the models were ineffective as they measured individual internal security components, which fails to depict the overall cybersecurity maturity of a healthcare institution. Furthermore, the effects of cloud computing on the healthcare industry were overlooked as well.

2.3 Cybersecurity assessment tools in cyber-physical system (CPS) models

There are three types of existing maturity models with which to assess organisational cybersecurity: (1) progression models, which provide organisation's a simple roadmap with which to measure their improvements as expressed by increasingly better versions of an attribute as the scale progresses; (2) capability models, such as CMM, which measure an organisation's cybersecurity capabilities using a set of characteristics, indicators, attributes, or patterns; and (3) hybrid models, which combine multiple models to simultaneously measure an organisation's maturity attributes and its evolution or progress [34].

Most extant cybersecurity models are simply a set of minimum compliance requirements rather than models that organisations can use to address emerging threats and increase their cybersecurity readiness. Furthermore, the cybersecurity assessment model should allow multiple users, in this case, management teams, security experts, and healthcare professionals, to assess the organisation's overall security level and implement actions to overcome weaknesses. Most extant cybersecurity models do not have this feature.

Lastly, most extant models use qualitative measures to assess cybersecurity readiness. However, quantitative measures are better suited for cybersecurity assessments [63, 64] as they simplify the results and interpretations, facilitating quicker understanding for time-critical decision-making purposes [65]. They also improve cybersecurity capabilities and assure organisations, which increases the confidence of top management in adopting CPS. Therefore, this was used as the basis for developing a scorecard method.

2.4 Scorecard method

A scorecard is a measurement and management system that supports IT governance processes and that can be used to align the organisation with its IT governance processes. Four perspectives are examined in an IT balanced scorecard: (1) organisational value, where the performance and business value of the adopted technology are evaluated from the viewpoint of the chief executive; (2) functionality, where the functionality of the adopted technology is evaluated from the viewpoint of the user; and (3) operational efficacy, where the effectiveness and operational efficiency of the adopted technology and its ability to support processes that run the organisation is evaluated; and (4) future value, where the performance of the adopted technology is evaluated by how it positions itself in the future to address the organisation's needs and continues to evolve with the quality of services provided to support the organisation's business processes [66, 67].

2.6 Problem Statement

Several cybersecurity assessment frameworks that exist for cyber-physical systems do not evolve with respect to various requirements and vulnerabilities specific to medical environments. Several are developed with the goal of maturity

assessment at the national level or for general digital infrastructures, with little application to organization-level healthcare settings. That gives environment handling of privacy a very crucial dimension for MCPS. This creates the need for a domain-specific cybersecurity assessment framework to identify major critical success factors pertinent to healthcare and thus to provide institutions with practical tools through which they may assess and further prepare themselves for MCPS adoption.

2.7 Difference from Prior Work

While several prior frameworks including NIST-CSF, ISO 27001, or COBIT try to present a general set of cybersecurity controls, they don't cover healthcare-specific issues obviously focusing on patient information sharing to third parties and HIPAA compliance, and interoperability of implants, sensors, etc. This research ultimately fills this gap by (1) developing a framework grounded in healthcare-specific CSFs found through meta-analysis and interviews with subject matter experts, (2) conducting validation through actual deployment in two hospitals, and (3) introducing a light, quantitative scorecard for direct institutional use—peculiarities not presented together in existent research studies.

2.5 Critical support factors (CSFs)

The CSFs for integrating MCPS at healthcare institutions with adequate cybersecurity would be most influential if they were explored through the lens of healthcare professionals. A mixed-methods approach, namely, combining qualitative and quantitative methods, is most effective for healthcare institutions [68].

Much of the existing literature provides anecdotal evidence of CSFs and little empirical work appears to have been conducted in this area. To increase certainty, it is important to empirically examine these CSFs by analysing them from multiple perspectives using different techniques, such as experiences and direct data collection, to compare what is believed to what was observed. Questionnaires have been used to identify the CSFs, while others propose conducting interviews to gather data [69].

However, questionnaires alone are not the best method of identifying the CSFs as they provide respondents with a list of possible CSFs, which limits their responses. The respondents may also misunderstand the CSFs listed or lack a sufficient understanding of the concept of the CSF approach. Therefore, interviews should be conducted to better explore the experiences and perceptions of healthcare professionals independently and without the researcher's interference [70].

As such, the researchers [71] used the Delphi Method to identify opportunities and the CSFs of implementing Industry 4.0 on an SME's industrial performance, while [72] first conducted a meta-analysis to identify the CSFs for information security and then evaluated the results with industry experts. Apart from that, the study by [73] conducted a meta-analysis and interviewed experts to identify the CSFs for digital manufacturing in an automotive assembly factory. To identify the CSFs for successfully implementing e-health interventions, the researchers [74] conducted a meta-analysis. Lastly, the study by [75] conducted a meta-analysis to identify the CSFs for IS security management for IoT.

3. METHODOLOGY

3.1 Research Design and Layout

In light of increasing cyberattacks on healthcare institutions, the present study intended to fill the gaps left by existing frameworks by designing a framework and scorecard with which to assess and improve the cybersecurity readiness of healthcare institutions to adopt MCPS by taking into consideration the findings of extant studies and the views of healthcare professionals. The scorecard was developed to evaluate the existing cybersecurity readiness of a healthcare institution, while the framework was developed to help healthcare institutions find solutions with which to address their cybersecurity shortcomings. Therefore, the scorecard determines the existing cybersecurity readiness of a healthcare institution before the framework is implemented.

As such, the present study is a design science study [76, 77, 78]. Information system studies use the design science paradigm for artefact development. It is also a problem-solving approach that creates artefacts, such as models, methods, constructs, and instantiations [79, 80]. Furthermore, developing the scorecard to demonstrate the 'usability' of the framework also makes it fall under the purview of a design science study [77].

Much like the relevance, design, and rigour cycles of design science studies [81, 82], the present study was conducted in three phases. Phase 1 involved developing the cybersecurity assessment framework (CAF) as well as demonstrating its relevance and utility. Phase 2 involved developing and practically discussing the scorecard that embodied the CSFs proposed in the framework. It was put into practice to demonstrate its utility as well. In Phase 3, senior healthcare experts evaluated the results of the scorecard to validate its utility. The framework was analytically evaluated again to glean useful knowledge and determine how to best implement it in healthcare institutions. Figure 2 depicts the framework of the present study.

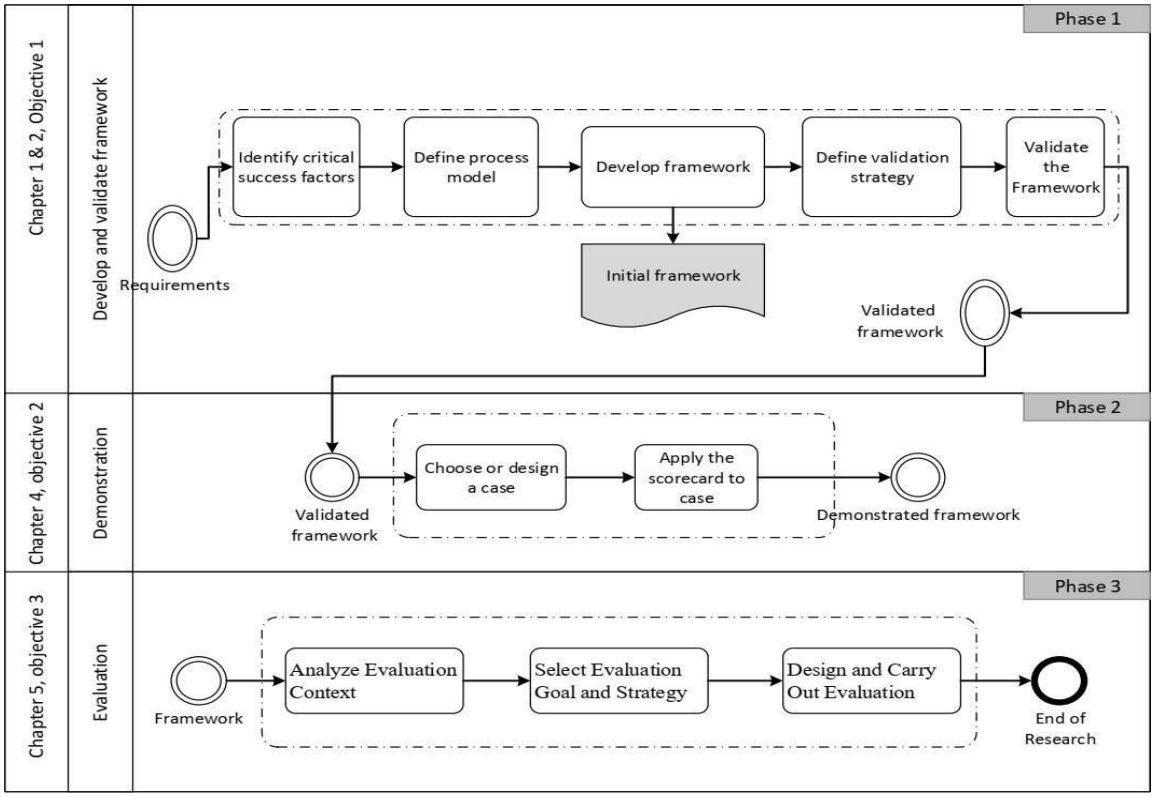

Figure 2. The framework of the present study

3.2 Phase 1: Developing the Cybersecurity Assessment Framework (CAF)

3.2.1 Identifying the constituting and evaluation models

A meta-analysis was conducted to review standards and best-practice frameworks that have been proposed for assessing the cybersecurity readiness of organisations. About 63 cybersecurity assessment process models were collected from diverse sources, such as journals, conference papers, government, non-government, or security agency publications, standards, guidelines, reputable online pages, and books. Furthermore, a total of 22 documents have been chosen specifically for their comprehensive coverage of the cybersecurity assessment domain. The analysis revealed that all the extant methods cannot be used to identify the CSFs. Therefore, inclusion criteria were created to select methods that could be used as the constituting set that would become the base of the CSFs. The models to be used to identify and validate the CSFs were divided into two sets: (1) a set of constituting models, from which the initial set of CSFs was drawn, and (2) a set of evaluation models that had specifically been developed to evaluate the cybersecurity readiness of healthcare institutions, which was used to compare and contrast the initial set of CSFs. The models were collected and categorised into two sets to ensure that whatever was missed in the generic models was included in the final set of CSFs.

The models listed in Tables 1 and 2 were selected because they satisfied the following

inclusion criteria: (A) they had already been used and tested, (B) they provide clear cybersecurity readiness assessment or evaluation procedures that can be adapted into the CSFs required to evaluate organisational cybersecurity readiness, and (C) they provide CSFs that are relevant to both patients' data security and privacy. The models in the constituting set were not included in the evaluation set.

Only 16 models met the inclusion criteria and were, therefore, used as the constituting set of models (Table 1). Meanwhile, all the six models that extant studies have proposed for assessing the cybersecurity readiness of healthcare institutions were taken as the evaluation set (Table 2). They were used to evaluate the completeness of the CSFs extracted from the constituting set and their ability to adequately evaluate the cybersecurity readiness of healthcare institutions. Tables 1 and 2, respectively, list the constituting and evaluation models that were derived from extant studies.

Table 1. The 16 extant constituting models

Model ID	Article Title	Source
M01	ISO/IEC 27000, 27001 and 27002 for information security management.	[36]
M02	COBIT [TM]: A methodology for managing and controlling information and information technology risks and vulnerabilities.	[35]
M03	A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom.	[40]
M04	Information security architecture (PROTECT).	[38]
M05	Summary of NIST SP 800-53, Revision 4: Security and privacy controls for federal information systems and organizations.	[39]
M06	Working from home during COVID-19 crisis: A cyber security culture assessment survey.	[41]
M07	To measure security culture: A scientific approach.	[42]
M08	Maturity models for data and information management.	[43]
M09	A comprehensive cybersecurity assess model to improve cybersecurity assurance: The cybersecurity assess model (CAPMM)	[44]
M10	A dynamic capability maturity model for improving cyber security.	[45]
M11	Information security maturity model for NIST cyber security framework.	[47]
M12	Cybersecurity capability maturity models for providers of critical infrastructure.	[48]
M13	Manage risks to achieve an appropriate level of security: To what extent does security requirements imposed on critical sectors align with a high common level of security on network and information systems?	[37]
M14	Conceptual model for cybersecurity readiness assessment for public institutions in developing country: Cambodia.	[49]
M15	A conceptual model for the development of a national cybersecurity index: An integrated framework.	[50]
M16	Cybersecurity indices and cybercrime annual loss and economic impacts.	[52]

Table 2. The six extant evaluation models

Model ID	Article Title	Source
M17	Cyber readiness index 2.0.	[62]
M18	Health care data breaches: A changing landscape.	[59]
M19	Smart city development in Hong Kong.	[60]
M20	Global cybersecurity index & cyberwellness profiles.	[61]
M21	A survey of security standards applicable to health information systems.	[57]
M22	ISFAM: the information security focus area maturity model.	[58]

3.2.2 Identifying the critical success factors (CSFs)

A set theory (Equation 1) was then used to remove redundant CSFs, leaving 500 CSFs in the initial list. This involved identifying popular CSFs and then identifying models that did not contain these popular CSFs. The descriptions of the CSFs from the models that did not contain the popular CSFs were studied to determine if any were similar to the popular CSFs. If any were identified, the CSF was removed from the list. If none were identified, the CSF was retained. This was repeated until the descriptions of all the CSFs had been examined. The

following set theory demonstrates the reduction process:

If
α and β are two sets of models. (1)
$x \in \alpha$; *and* $y \in \beta$
then $\alpha \setminus \beta$, *therefore* $x \equiv y$.

The common terms used to label the CSFs in the models were not altered so as to maintain their scientific representations and ensure that they would be understood and easily recognised by the security community.

The 89 CSFs shortlisted from the 16 constituting models (M01-M16) were then grouped into five dimensions that most commonly appeared in the constituting set: (1) assets, (2) access and trust, (3) operations, (4) governance, and (5) human resources. Tables 3 to 8 list the initial set of 89 CSFs and from which of the 16 constituting models they had been extracted.

Journal of Theoretical and Applied Information Technology
31st July 2025. Vol.103. No.14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3. The 20 assets-based critical success factors (CSFs)

Dimension	CSF	M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12	M13	M14	M15	M16
Assets	Do you only use up-to-date and trusted third-party components for the software developed by the organisation?	✓			✓		✓		✓			✓	✓		✓	✓	✓
	Do you apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software?		✓	✓		✓		✓			✓	✓	✓	✓			✓
	Do you maintain an inventory of all sensitive information stored, processed, or transmitted by the organisation's technology systems, including those located on-site or at a remote service provider?	✓		✓	✓	✓	✓			✓		✓		✓	✓		✓
	Have you ensured that sensitive data or systems are not regularly accessed by the organisation from the network?	✓	✓		✓		✓	✓			✓	✓	✓			✓	✓
	Do you employ integrity checking mechanisms to verify hardware integrity?	✓	✓	✓		✓			✓	✓			✓	✓	✓		
	Do you maintain an accurate and up-to-date inventory of all assets with the potential to store or process information?	✓		✓	✓		✓		✓		✓	✓		✓	✓	✓	
	Have you established and do you maintain secure configuration management processes (e.g., when servicing field devices or updating their firmware)?		✓	✓	✓			✓		✓	✓	✓		✓		✓	
	Do you store master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorised changes to the images are possible?	✓	✓	✓	✓			✓		✓		✓	✓		✓	✓	✓
	Do you properly label all relevant assets, depending on their classification?	✓	✓	✓		✓	✓		✓		✓			✓	✓	✓	✓
	Are the classification schemes and labelling procedures properly communicated to all relevant parties?	✓			✓	✓		✓		✓		✓	✓		✓	✓	✓
	Do you maintain documented security configuration standards for all authorised network devices?	✓	✓	✓		✓	✓		✓	✓		✓	✓	✓		✓	
	Have you compared all network device configurations against approved security configurations defined for each network device in use, and do you alert when any deviations are discovered?	✓	✓	✓			✓		✓	✓	✓	✓	✓			✓	✓
	Have you associated active ports, services, and protocols to the hardware assets in the asset inventory?		✓	✓	✓			✓			✓				✓		✓

Dimension	CSF	M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12	M13	M14	M15	M16
Assets	Do you perform automated port scans on a regular basis against all systems and alert if unauthorised ports are detected on a system?	✓	✓	✓		✓			✓		✓		✓		✓		✓
	Have you utilised software inventory tools throughout the organisation to automate the documentation of all software on business systems?			✓	✓		✓		✓	✓	✓	✓	✓				✓
	Is the software inventory system tied into the hardware asset inventory so that all devices and associated software are tracked from a single location?	✓		✓	✓			✓			✓		✓		✓		✓
	Does your staff wear ID badges?	✓	✓		✓		✓		✓		✓		✓		✓	✓	✓
	Are authorised access levels and type (employee, contractor, visitor) identified on the badge?	✓		✓	✓		✓	✓	✓	✓			✓		✓	✓	
	Is access to all your computing area controlled (single point, reception or security desk, sign-in/sign-out log, temporary/visitor badges)?	✓	✓	✓		✓	✓	✓		✓		✓	✓	✓			
	Do you have an emergency evacuation plan and is it current?	✓	✓		✓		✓	✓			✓			✓		✓	

Table 4. The 18 access and trust-based critical success factors (CSFs)

Dimension	CSF	M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12	M13	M14	M15	M16
Access and trust	Have you enabled firewall filtering between VLANs to ensure that only authorised systems are able to communicate with other systems necessary to fulfil their specific responsibilities?	✓		✓	✓		✓	✓	✓			✓	✓	✓		✓	✓
	Have you implemented physical or logical access controls for the isolation of sensitive applications, application data, or systems?	✓	✓		✓	✓	✓		✓		✓	✓	✓		✓	✓	✓
	Do you automatically disable dormant accounts after a set period of inactivity?		✓	✓	✓	✓			✓	✓			✓	✓	✓	✓	✓
	Do you maintain an inventory of each of the organisation's authentication systems, including those located on - site or at a remote service provider?	✓	✓	✓			✓	✓	✓	✓			✓	✓	✓		
	Do you have documentation of the mapping of organisational communication flows?	✓		✓		✓					✓	✓				✓	
	Do users acknowledge receipts of secret authentication information?	✓			✓		✓		✓		✓		✓		✓		✓
	Do you policies and procedure ensure the flexibility of your organisation by defining ways of adapting to changes in the sector and the environment?	✓	✓	✓		✓	✓	✓	✓	✓	✓					✓	✓
	Have you established a good cooperation level with other sectoral organisations (inter-organisational strategic ties)?	✓			✓	✓	✓		✓		✓			✓	✓	✓	✓

Dimension	CSF	M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12	M13	M14	M15	M16
Access and trust	Does your log-on procedure avoid displaying a password being entered?	✓	✓			✓		✓				✓		✓	✓		
	Are your computers set up so that others cannot view staff entering passwords?	✓	✓		✓		✓		✓		✓						
	Do you identify the privileged access rights associated with each system or process and the users to whom they need to be allocated?	✓	✓					✓			✓	✓				✓	✓
	Do you log changes to privileged accounts?	✓				✓				✓		✓		✓		✓	
	Do you properly inform employees about his responsibilities that remain valid after termination or change of employment?	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
	Are access permissions and authorisations managed according to the principles of least privilege and separation of duties?	✓		✓	✓	✓		✓		✓		✓		✓	✓		
	Have you formalised contractual relationships with partners and suppliers regarding information security?	✓			✓		✓	✓								✓	✓
	Do you identify and define the necessary requirements a third party should have to be considered trusty?		✓	✓		✓			✓	✓	✓	✓					
	Do you maintain an inventory of authorised wireless access points connected to the wired network?	✓	✓		✓		✓	✓					✓	✓	✓		
	Have you created a separate wireless network for personal and untrusted devices?		✓				✓	✓		✓	✓			✓	✓		✓

Table 5. The 12 operations-based critical success factors (CSFs)

Dimension	CSF	M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12	M13	M14	M15	M16
Operations	Do you audit your processes and procedures for compliance with established policies and standards?	✓	✓		✓		✓		✓	✓	✓		✓	✓	✓	✓	
	Do you review and revise your security documents, such as: policies, standards, procedures, and guidelines, on a regular basis?		✓	✓	✓		✓	✓	✓	✓		✓	✓			✓	✓
	Do you have all the necessary policies and procedures properly documented?	✓	✓	✓		✓	✓		✓		✓	✓		✓	✓	✓	✓
	Do you have all the necessary records properly documented?	✓		✓			✓	✓		✓		✓		✓		✓	✓
	Do users have different user profiles for operational and testing systems?	✓		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
	Do you maintain separate environments for production and non-production systems?	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓			✓	✓
	Do you specify the operational instructions of the installation and configuration of the systems?	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓		

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Dimension	CSF	M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12	M13	M14	M15	M16
Operations	Do you specify the operational instructions of the scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times?	✓	✓		✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓
	Is your leadership actively and continuously involved in information security planning?	✓	✓		✓	✓	✓	✓	✓	✓	✓		✓	✓			
	Do you pursue the principles of efficiency in information security – economy/cost optimisation?		✓		✓	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓
	Do you receive threat and vulnerability information from information sharing forums and sources?		✓		✓	✓	✓	✓	✓	✓	✓	✓				✓	✓
	Is the organisational risk tolerance determined and clearly expressed?	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓

Table 6. The 12 defence-based critical success factors (CSFs)

Dimension	CSF	M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12	M13	M14	M15	M16
Defence	Do you maintain an up-to-date inventory of all the organisation's network boundaries?	✓		✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓
	Do you decrypt all encrypted network traffic at the boundary proxy prior to analysing the content?	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓
	Do you encrypt all data stored in cloud services?	✓	✓	✓		✓	✓	✓	✓	✓	✓			✓	✓	✓	✓
	Do you encrypt event files locally and in transit?	✓			✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		
	What is the percentage from your total received emails that are detected as spam?		✓	✓		✓		✓		✓		✓	✓			✓	✓
	What is the percentage of your SSL certificates that are configured incorrectly?	✓	✓	✓	✓		✓	✓	✓		✓		✓		✓	✓	✓
	Have you properly broken-down information security policies into sub-areas and orderly documented them?	✓			✓	✓				✓	✓	✓	✓	✓	✓		
	Do your policies and procedures comply with relevant regional legislation?		✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓
	What percentage of your systems (workstations, laptops, servers) are covered by antivirus/antispyware software?			✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
	Do you send all malware detection events to enterprise antimalware administration tools and event log servers for analysis and alerting?	✓			✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		
	Do you perform a skill gap analysis to understand the skills and behaviours workforce members are not adhering to, using this information to build a baselines education roadmap?	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓

Dimension	CSF	M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12	M13	M14	M15	M16
Defence	Do you deliver training to address this skills gap identified to positively impact workforce members' security behaviour?	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓

Journal of Theoretical and Applied Information Technology
31st July 2025. Vol.103. No.14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 7. The 10 governance-based critical success factors (CSFs)

Dimension	CSF	M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12	M13	M14	M15	M16
Governance	Have you ensured that local logging has been enabled on all systems and networking devices?	✓	✓	✓	✓	✓			✓	✓	✓	✓		✓	✓	✓	✓
	Do you protect logs from unauthorised alterations and deletions?	✓			✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	
	What percentage of your security incidents cause service interruption or reduced availability?	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓			
	Do you have established processes to receive, analyse, and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g., internal testing, security bulletins, or security researchers)?		✓	✓			✓	✓	✓			✓	✓	✓	✓	✓	✓
	Have you tested that you gracefully handle denial of service attempts (from compromised metres)?	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓
	Do you apply a qualified third-party security penetration testing to test all hardware and software components prior to live deployment?	✓		✓	✓	✓	✓			✓	✓	✓			✓	✓	
	Do you provide your employees with a channel in order to report violations of information security policies or procedures?	✓	✓		✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	
	How much time does the organisation take in order to respond to a report?	✓			✓	✓	✓	✓	✓	✓					✓	✓	✓
	Are critical security tasks handled based on team decision making techniques?	✓	✓	✓	✓	✓					✓	✓	✓	✓	✓		
	Do you organise vertical and horizontal security meetings on a regular basis?		✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	

Table 8. The 17 human resources-based critical success factors (CSFs)

Dimension	CSF	M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12	M13	M14	M15	M16
Human resources	I believe that cyber criminals are more advanced than the people who are supposed to be protecting us.	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	✓	✓
	I worry that if I report a cyber-attack to the police, it might damage the reputation of the company.	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
	I am pleased with my organisation's approach towards information security.	✓	✓		✓	✓			✓	✓	✓	✓		✓	✓	✓	✓

Dimension	CSF	M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12	M13	M14	M15	M16
Human resources	I am happy to conform to the security guidance offered by our security experts.	✓	✓	✓			✓	✓	✓	✓	✓		✓		✓		
	Are you aware of the organisation's communication flows?	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓		✓	
	Are you aware of the organisation's role?	✓		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓
	Are you aware of all the devices and systems you are responsible for?	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓	
	Are you aware of all the external information systems they come in contact with?	✓		✓	✓	✓	✓	✓		✓	✓		✓	✓		✓	✓
	Do you make sure your mobile devices are not left exposed?	✓	✓		✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	
	Do you efficiently protect mobile devices from physical hazards?			✓		✓		✓	✓	✓	✓	✓	✓		✓	✓	
	What would you do if you saw a colleague not wearing their security pass around the office?	✓		✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓
	What would you do if you overheard a discussion, which you knew to be about some highly sensitive and confidential information, being held in a corridor where external visitors often pass through?	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓
	How many of your security incidents stem from non-secure behaviour?	✓		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓
	I get into the office wearing my security pass.	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓			✓	✓
	What is necessary for a person to turn a plain text message into an encrypted message?		✓	✓	✓	✓			✓	✓	✓	✓	✓		✓		✓
	My achievement score at the last security training programme I participated in was around.	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓		
	How many self-security assessments do you normally attempt per year?	✓		✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	

3.2.3 Evaluating the Critical Success Factors (CSFs)

To evaluate the completeness of the initial list of CSFs, each domain's CSFs, which had been derived from the constituting set (M01-M16), were validated by comparing them to the six models in the evaluation set (M17-M22): (1) to ensure their completeness and generalisability, (2) to ensure the structure, logic, and causal correlations between the CSFs agreed with those in the healthcare industry, and (3) to identify any CSFs that may have been overlooked.

Assets-based critical success factors (CSFs)

Although M17 and M18 contained security-related CSFs, they did not contain specific assets-based CSFs. Meanwhile, M19 contained three assets-related CSFs, namely, threat detection technology, patch management, and security hardening factors, which were all selected for inclusion in the assets-based CSFs. Apart from that, although M20 assessed five dimensions, none of them were assets- or technology-related. Similarly, although M21 assessed asset management, it failed to list clear evaluation factors or indicators. Lastly, as the asset management dimension of M22 contained 13 CSFs, all 13 were included in the present study's assets-based dimension. Therefore, the CSFs selected were generic and additional CSFs were not required.

Access and trust-based critical success factors (CSFs)

M17 considered various access control mechanisms and the policies that govern them. However, it did not delve into trust-based CSFs at a much-disaggregated level. M18, similarly, addressed secure authentication mechanisms and discussed trust-based frameworks for risk mitigation. However, it did not elaborate on any specific CSF for continuous trust validation. M19 proposed an access control system built on public-private trust partnerships. Trust policies over multi-factor authentication, as well as access to public data, were described and correlated to key access-based CSFs. M20, on the other hand, acknowledged the factors involved in measures of cybersecurity maturity. However, it does not delineate trust-related individual CSFs. M21 commented on asset management but failed to evaluate trust-based access factors properly. Furthermore, it stressed the security of sensitive information, but no framework for measuring trust was given.

Operations-based critical success factors (CSFs)

M17 contained continuity-related CSFs, which were already included in the initial list of CSFs. Model M18 did not specify specific operations-related CSFs. Lastly, M19 to M22 did not contain operations-related CSFs.

Defence-based critical success factors (CSFs)

M17 contained defence- and crisis response-related CSFs, such as the establishment of cyber defence policies, cyber defence mission statements, and articulating a cyber defence statement. These three CSFs were included in the initial list of CSFs. Meanwhile, the defence-related CSFs that M18 to M20 were developed for a national level and, therefore, not very suited for organisations. Lastly, M21 and M22 did not contain defence-related CSFs.

Governance-based critical success factors (CSFs)

M17 contained knowledge management- and crisis management-related CSFs that ought to be taken under consideration. Meanwhile, M18 contained establishing policies and procedures for governing strategies, which were already included in the initial list of CSFs. The CSFs in the remaining models only marginally assessed the governance aspects of cybersecurity.

Human resources-based critical success factors (CSFs)

Although M17 to M20 contained many human- or people-related CSFs, most of the CSFs in the initial list already addressed them. On the other hand, M21 and M22 contained an education for cybersecurity awareness domain, however, these, too, had already been included in the initial list of CSFs. Figure 3 depicts the process of identifying and customising the CSFs.

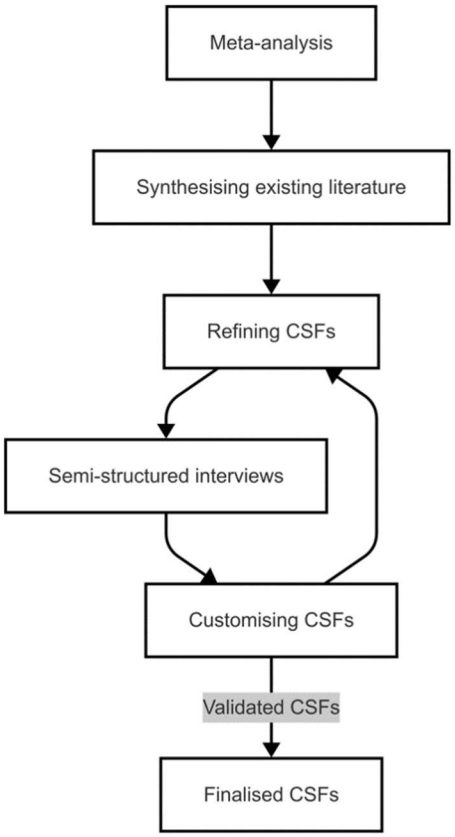

Figure 3. The process of identifying the critical success factors (CSFs)

In conclusion, only a few of the initial CSFs addressed privacy as most of the models in the constituting set did not prioritise the data privacy aspect of cybersecurity. As data privacy is important in the healthcare industry, some models that prioritise data privacy in the healthcare industry will be taken into consideration to fill the gap.

3.2.4 Designing and developing the cybersecurity assessment framework (CAF)

The 1st iteration of the framework was developed using the identified CSFs. The CSF list underwent numerous cycles to yield a framework that was reliable. The CSFs in the framework were then validated by a group of IT managers and

healthcare professionals who were selected based on their years of experience in their respective fields. A questionnaire was used to conduct the initial evaluation followed by an analysis conducted via interviews. Figure 4 depicts Phase 1 of the present study.

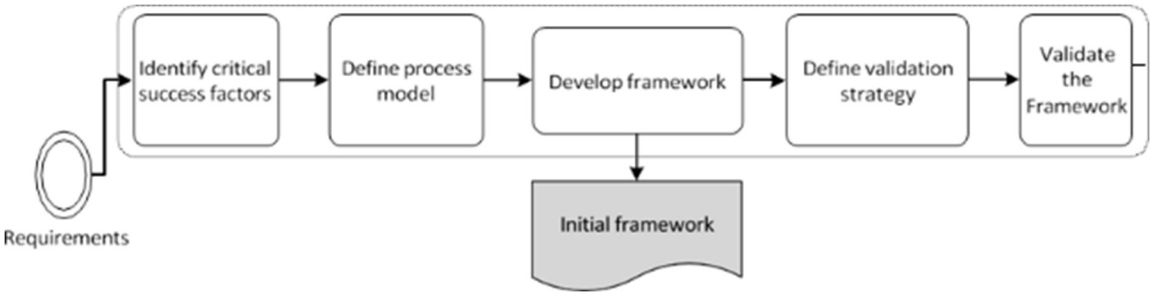

Figure 4. Phase 1

The final CAF was developed by (1) assessing the theoretical and technical aspects of security and privacy readiness that healthcare institutions require to adopt an MCPS; (2) ensuring that it aligns with the strategies of healthcare institutions, under the purview of the top management, and adopted at an organisational and individual level; and (3) ensuring that it does not contradict to the main reason the healthcare institution is adopting an MCPS in the first place. As such, the framework was, largely, based on the best practices used to securely implement, manage, and govern cloud computing, IoT technologies, edge computing, fog computing and such in the healthcare industry, as well as extant studies listing what is required to protect patient privacy when adopting cutting-edge technologies in the healthcare industry. Figure 5 depicts the CAF that was developed.

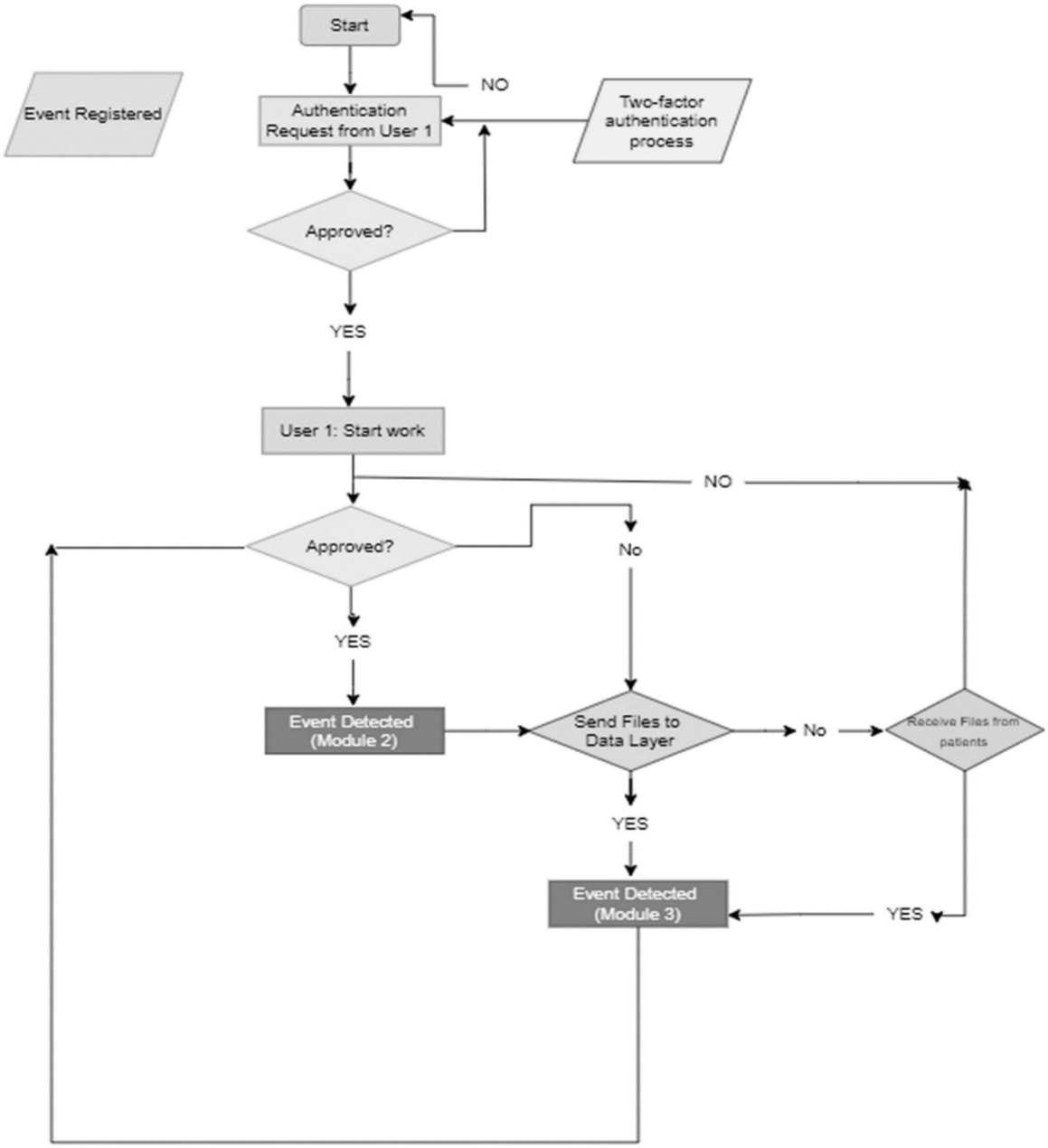

Figure 5. The proposed cybersecurity assessment framework (CAF)

The framework begins with a two-factor authentication system against fraud authentication requests from a user. A two-factor authentication system enhances security by adding an additional layer of security to personal information [83]. Once the user is granted access, they can begin working with the patient's data. The user's access to the data is registered as an event and sent to the data layer, where information related to the patient's treatment procedures can be received and sent. In the data layer, information from multiple devices and sensors is received, which is of a heterogeneous nature [84]. After receiving information in multiple formats, the data is converted into a common format that is understandable by all users.

3.3 Phase 2: Developing the Scorecard

A scorecard that IT managers could use as a template for gathering data about the MCPS adoption readiness of their healthcare institution pre-MCPS adoption was developed to test the

usability of the proposed MCPS framework (Table 9). The required data was collected via structured interviews with relevant members of the institution. The scorecard also provides a mechanism with which to report the aggregated data back to the decision-makers at the institution. Apart from that, the scorecard and the framework were theoretically tested on two case study healthcare institutions in Libya. Figure 6 depicts Phase 2 of the present study.

Table 9. The proposed scorecard

CSF	High (%)	Medium (%)	Low (%)	Negligible (%)
Reliability				
Validity				
Third-party Authentication				
Security				
Transparency				

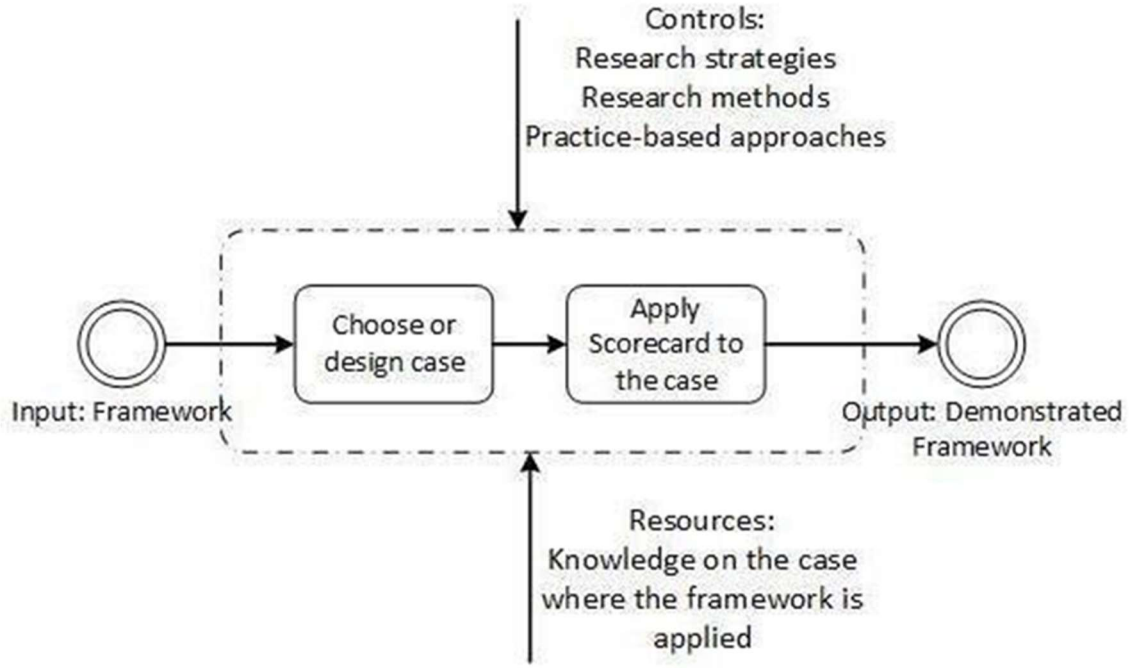

Figure 6. Phase 2

3.4 Phase 3: Validating the Cybersecurity Assessment Framework (CAF)

Semi-structured interviews were conducted, where the results of the usability demonstration and the extent to which the proposed framework fulfils its requirements were evaluated by a group of IT managers and healthcare professionals. The evaluation involved: (1) analysing the context of the evaluation, where the researcher determined the prerequisites for selecting the goal and strategy for the evaluation; (2) selecting the goal and strategy of the evaluation, where the researcher defined the goal of the evaluation and the strategy to be taken to achieve said goal; and (3) designing and conducting the evaluation, where the researcher designed the evaluation and conducted it. Figure 7 depicts Phase 3 of the present study.

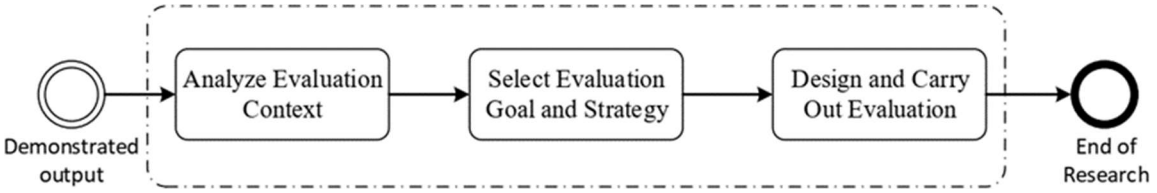

Figure 7. Phase 3

As it was unfeasible to conduct the evaluation in a real-life healthcare institution, a survey as well as open-ended semi-structured interviews of IT managers and healthcare professionals from two Libyan hospitals, namely, Estishari Hospital and Benghazi Children's Hospital, were conducted to collect their opinions on the proposed framework as well as evaluate it against the requirements listed in Phase 1. Table 10 lists the questions that were used to conduct the semi-structured interviews and in the questionnaire.

Table 10. The questions included in the questionnaire and semi-structured interviews

Questionnaire	
No.	Question
1	Is the CAF reliable for assessing the cybersecurity readiness of a healthcare institution?
2	Is the scorecard a valid method for assessing the cybersecurity readiness of a healthcare institution?
3	What is the degree of third-party authentication that the CAF follows when assessing the cybersecurity readiness of a healthcare institution?
4	What is the degree of the security protocols that the CAF follows when assessing the cybersecurity readiness of a healthcare institution?
5	What is the degree of transparency that the CAF follows when assessing the cybersecurity readiness of a healthcare institution?
Semi-structured Interview	
No.	Question
1	Is the CAF a reliable and valid model for assessing the cybersecurity readiness of a healthcare institution to adopt an MCPS?
2	What do you think about the usability of the scorecard method for assessing the cybersecurity readiness of a healthcare institution to adopt an MCPS?
3	How important do you think third-party authentication is when assessing the cybersecurity readiness of a healthcare institution to adopt an MCPS, and does the CAF ensure that?
4	What level of cybersecurity does the CAF provide healthcare institutions?
5	Does the CAF offer a higher level of transparency?

3.5 Research Hypothesis

The study hypothesizes that: "A cybersecurity assessment framework and scorecard based on the specific CSFs of healthcare institutions shall ensure better earnestness and effective results from readiness assessment for MCPS adoption." Testing of this hypothesis was performed through expert feedback, scorecard tests, and a thematic analysis of stakeholder feedback.

4. RESULTS AND DISCUSSION

By simulating a working cloud storage service, two experimental case scenarios were designed, developed, and implemented to: (1) observe the utility of the cloud forensics component of the proposed framework and (2) to demonstrate the applicability of the proposed framework by using its key processes to locate and extract evidence from private and public cloud services. The findings of Scenario 1 indicate that the proposed

CAF enabled Estishari Hospital and Benghazi Children's Hospital to prepare and ready themselves to adopt MCPS, while Scenario 2, which used the two remaining components of the proposed framework, indicates that it was able to successfully identify the perpetrators.

4.1 Questionnaire

A simple questionnaire that reflected the scorecard was developed and distributed to a group of 10 IT managers and healthcare professionals. Table 11 provides a summary of the response.

Table 11. The distribution of the questionnaire and scorecard responses

No.	Question / CSF	High (%)	Medium (%)	Low (%)	Negligible (%)
1	Is the CAF reliable for assessing the cybersecurity readiness of a healthcare institution? / Reliability.	50	40	10	0
2	Is the scorecard a valid method for assessing the cybersecurity readiness of a healthcare institution? / Validity.	50	50	0	0
3	What is the degree of third-party authentication that the CAF follows when assessing the cybersecurity readiness of a healthcare institution? Third-party authentication.	30	70	0	0
No.	Question / CSF	High (%)	Medium (%)	Low (%)	Negligible (%)
4	What is the degree of the security protocols that the CAF follows when assessing the cybersecurity readiness of a healthcare institution? / Security.	20	70	0	10
5	What is the degree of transparency that the CAF follows when assessing the cybersecurity readiness of a healthcare institution? / Transparency.	40	50	10	0

4.1.1 Results of the analysis

As seen, 50% believed that the reliability of the proposed CAF was high, while 40 and 10%, respectively, believed that it was medium and low. Similarly, 50% believed that the validity of the proposed scorecard was high, while the rest believed that it was medium. Most of the respondents (70%) felt that the proposed CAF's degree of third-party authentication was medium, while 30% felt it was high. Similarly, 70% felt that the proposed CAF's degree of security protocols was medium, while 20 and 10% felt it was high and negligible, respectively. Lastly, 50% of the respondents felt that the proposed CAF's degree of transparency was medium, while 40 and 10% felt that it was high and low, respectively.

4.2 Semi-Structured Interviews

Table 12 provides the responses that the five IT managers from Estishari Hospital and Benghazi Children's Hospital gave during the semi-structured interviews.

Table 12. The semi-structured interview responses of the IT managers from Estishari Hospital and Benghazi Children's Hospital

No.	Question	IT Manager 1 (Estishari)	IT Manager 2 (Estishari)	IT Manager 3 (Benghazi)	IT Manager 4 (Benghazi)	IT Manager 5 (Benghazi)
1	Is the CAF a reliable and valid model for assessing the cybersecurity readiness of a healthcare institution to adopt an MCPS?	The CAF has brought a new perspective to the medical world. It has made it easier to provide specialisations to patients, but that may not be the case always, as the framework is still unreliable, as accurate care possibilities may be misunderstood by a lack of communication by the patients.	It has made a huge difference in medication indeed. The CAF is very easy-to-use and, additionally, provides remote care services to our patients. Our IT team has AI developers, who maintain the channels.	It is important to provide accurate treatments to the children. I think the CAF has brought the precision of smart monitoring, which can be overlooked by humans. Our hospital has integrated the CAF further to provide high-speed real-time response, which is very time efficient, but raises concerns about privacy.	The IT department has been working with the CAF. I think it is highly complex to be integrated seamlessly on a regular basis. I would say that the reliability factor is quite low.	The CAF does not guarantee readiness in privacy and patient data confidentiality. Nevertheless, our IT team is dedicated to improving weak areas. Furthermore, as it operates on a distributed system, it cannot be decentralised.
2	What do you think about the usability of the scorecard method for assessing the cybersecurity readiness of a healthcare institution to adopt an MCPS?	The scorecard method is highly beneficial. It has been integrated to check the preparedness of our system in emergency situations.	Patient confidentiality and the maintenance of privacy standards is important for us. So, the scorecard has helped us assess third-party	The scorecard was designed to accurately assess the transparency of the system, reduce errors, and preserve the highest level of data security. Analysis indicates that the	Child care at the hospital is highly maintained with valid medications. The scorecard makes it easier and shows us our readiness to adopt an MCPS.	The healthcare industry still struggles with patient privacy and data theft. An MCPS lessens these concerns. The complexity of the structure can be modified in

No.	Question	IT Manager 1 (Estishari)	IT Manager 2 (Estishari)	IT Manager 3 (Benghazi)	IT Manager 4 (Benghazi)	IT Manager 5 (Benghazi)
2	What do you think about the usability of the scorecard method for assessing the cybersecurity readiness of a healthcare institution to adopt an MCPS?					coming years. We are using the scorecard to determine our readiness to adopt an MCPS and reap the most benefits.
3	How important do you think third-party authentication is when assessing the cybersecurity readiness of a healthcare institution to adopt an MCPS, and does the CAF ensure that?	In my opinion, third-party authentication is an important feature that needs to be implemented in MCPS to ensure the safe storage of patient records. The CAF can provide a higher level of organisational security.	The hospital will truly benefit from implementing the CAF as it supports third-party authentication in private hospitals to protect their reputation and prevent financial fraud.	I have been working as an IT manager at Benghazi Children's Hospital for a few years now and have encountered many issues with cybersecurity that have led to financial losses and reputational damage. I think the CAF can help address these issues effectively.	The implementation of the CAF for third-party authentication at public hospitals, like Benghazi Children's Hospital, can help deliver CPS-based healthcare by increasing security when using third-party services.	There is no doubt that the CAF improves third-party authentication in terms of the cybersecurity readiness of a healthcare institution.
4	What level of cybersecurity does the CAF provide healthcare institutions?	The CAF increases cybersecurity, which can ensure better quality care for the patients.	The CAF effectively protects the critical treatment and personal data of the patients and safeguards the hospital staff's professional data.	The CAF protects the data of public hospitals from unauthorised access and increases cybersecurity.	Implementing the CAF enhanced the security of our electronic data and storage systems, in line with government regulations.	Technological growth has increased the risk of threats and breaches. Therefore, there is a great need for security measures, that the CAF lacks.
5	Does the CAF offer a higher level of transparency?	Yes. I think that the CAF is an easier way to track patient health in a transparent manner.	The CAF facilitates better management of patients' healthcare and provides transparency in treatments.	The CAF has a good storage capacity that can store important data about the treatment process, facilitating transparency.	The CAF improved the transparency of the healthcare procedures, but not to a great extent.	Yes. The CAF increased transparency due to its features, such as tracking the healthcare of each patient.

4.2.1 Results of the thematic analysis

The responses were then analysed and six themes were derived: (1) facilitated MCPS adoption, (2) comprehensive CAF for healthcare institutions, (3) CAF contained key CSFs required to assess the cybersecurity and privacy readiness of healthcare institutions, (4) scorecard contained key CSFs required to assess the cybersecurity and privacy readiness of healthcare institutions, (5) CAF was valid and reliable, and (6) scorecard was usable.

Theme 1: Facilitated medical cyber-physical system (MCPS) adoption

The proposed CAF played a crucial role in processing, storing, and accessing healthcare-related information at the case study institutions. More specifically, it effectively increased interactions between their key stakeholders and enabled them to better serve their patients by acquiring and delivering patient data to their healthcare professionals, which enabled them to make data-driven healthcare decisions.

Theme 2: Comprehensive Cybersecurity Assessment Framework (CAF) for Healthcare institutions

The proposed CAF is a comprehensive guide for the successful implementation of MCPS-related cybersecurity measures. Its features effectively increased the cybersecurity readiness of the case study institutions and enabled them to provide the real-time data of their patients to their healthcare professionals, which enhanced their healthcare performance.

Theme 3: Cybersecurity assessment framework (CAF) Contains key CSFs required to assess the cybersecurity and privacy readiness of healthcare institutions

Third-party authentication is a vital factor when assessing the privacy and cybersecurity readiness of healthcare institutions [85]. It also helps maintain transparency and reliability, which are two CSFs when assessing the cybersecurity and privacy readiness of healthcare institutions, by verifying data authenticity, integrity, and adherence to several regulatory standards. The proposed CAF's reliability concerns the system's ability to perform consistently, without any compromises or failure. The CSFs, such as security, were thoroughly maintained. Therefore, the CAF enabled the case study institutions to assure transparency in their MCPS alongside cybersecurity readiness.

Theme 4: The Scorecard contained key CSFs required to assess the cybersecurity and privacy readiness of healthcare institutions

A scorecard plays a vital role when assessing the readiness of a healthcare institution to adopt an MCPS by mitigating cyber threats as well as upholding the standards of privacy as well as assuring secure and reliable services. It also helps healthcare institutions achieve cybersecurity benchmarks and regulations [86, 87]. The proposed scorecard enabled the case study institutions to holistically evaluate their cybersecurity readiness pre-MCPS adoption. It fostered transparency as well as accountability among their stakeholders, with a clear view of their cybersecurity weaknesses and strengths.

Theme 5: Cybersecurity assessment framework (CAF) was valid and reliable

Most of the IT managers reported that the proposed CAF was reliable and valid, and helped improve the overall performance of the case study institutions. More specifically, it enabled their healthcare professionals to provide better healthcare by improving their diagnoses and facilitating smart monitoring. However, some reported that it was not reliable or valid, mostly due to misunderstandings arising from a lack of communication between patients and the highly complex framework that patients find difficult to navigate.

Theme 6: The Scorecard was usable

Most of the IT managers reported that the scorecard was usable. They also stated that the proposed CAF supported third-party authentication, which would effectively enhance the cybersecurity performance of the case study institutions. Furthermore, although the cybersecurity measures of the proposed CAF were effective, they may not always be very effective. Lastly, although the CAF significantly fosters transparency, it may not fully support the transparency of the treatment procedures.

These findings conform to previous literature [57,58], where it was stated that there exists no operational scorecard systems and frameworks specifically designed for healthcare cybersecurity. Differently from these previous models, our proposed CAF was reported to be both usable and actionable in the hospital environment.

4.3 Limitations

The study had several limitations. First, the evaluation was done in two hospitals only, both located in Libya, and it may limit the generalizability to other regions with different regulations or infrastructural mediums. Second, while the CAF was validated with a domain, experts could not actually test or validate it in live MCPS environments. Third, privacy concerns were not

addressed in the proposed framework and remain an area to be enhanced in the future. Last, the subjectivity of self-reported expert feedback remains a minor limitation.

5. CONCLUSION AND RECOMMENDATIONS

The study has addressed a pertinent issue plaguing healthcare cybersecurity-the absence of a domain-specific framework for the study of institutional readiness for medical cyber-physical systems (MCPS). By identifying five empirically grounded critical success factors (CSFs)—reliability, validity, third-party authentication, security, and transparency—the study developed and validated a Cybersecurity Assessment Framework (CAF) and a quantitative scorecard with specifications necessary for healthcare institutions. Theoretically, the CAF and scorecard were tested in two Libyan hospitals and received positive feedback from IT managers and healthcare professionals.

The results taught that these tools did assist in evaluating readiness and creating awareness of cybersecurity gaps prior to MCPS implementation. These results seem to lend credit to the proposition that a sector-specific, CSF-based framework enhances both preparedness and confidence in cybersecurity decision-making. Yet, limitations continue to exist. The study relied on theoretical validation and stakeholder feedback drawn from a purposive sample composed of only 15 participants, a reflection of which could breed bias.

The privacy facet of MCPS is not sufficiently treated in the proposed CAF and will require incorporation with other privacy-oriented frameworks in subsequent iterations. The generalisability of results is also limited due to the regional scope and the lack of MCPS live deployment in the studied institutions. In terms of contribution, this research places a practical healthcare-specific tool into cybersecurity literature to fill the gaps between policy frameworks and institutional implementation.

Future works will involve a longitudinal review of the CAF in practice environments, integration with cutting-edge threat modelling and encryption standards, and validation of the framework across global healthcare systems. In a nutshell, the CAF and scorecard residents represent one of the biggest leaps toward the secure adoption of MCPS and offer a replicable model for healthcare institutions in assessing and improving their cybersecurity maturity.

REFERENCES

[1] A. Darwish and A. E. Hassanien, "Cyber physical systems design, methodology, and integration: the current status and future outlook," *Journal of Ambient Intelligence and Humanized Computing,* vol. 9, no. 5, pp. 1541-1556, Oct. 2018.

[2] N. Jazdi, "Cyber physical systems in the context of Industry 4.0," in *Proceedings of the 2014 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR)*, Cluj-Napoca, Romania, 2014.

[3] D. DiMase, Z. A. Collier, K. Heffner and I. Linkov, "Systems engineering framework for cyber physical security and resilience," *Environment Systems and Decisions,* vol. 35, no. 2, pp. 291-300, Jun. 2015.

[4] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustainable Cities and Society,* vol. 50, p. 101660, Oct. 2019.

[5] H. Ye, J. Liu, W. Wang, P. Li, T. Li and J. Li, "Secure and efficient outsourcing differential privacy data release scheme in cyber–physical system," *Future Generation Computer Systems,* vol. 108, pp. 1314-1323, Jul. 2020.

[6] Y. Zhao, S. K. Tarus, L. T. Yang, J. Sun, Y. Ge and J. Wang, "Privacy-preserving clustering for big data in cyber-physical-social systems: Survey and perspectives," *Information Sciences,* vol. 515, no. 2, pp. 132-155, Apr. 2020.

[7] P. V. Devi and V. Kalaichelvi, "Security issues in medical cyber physical systems (MCPS) – A survey," *International Journal of Pure and Applied Mathematics,* vol. 117, no. 20, pp. 319-324, 2017.

[8] D. Box and D. Pottas, "Improving information security behaviour in the healthcare context," *Procedia Technology,* vol. 9, pp. 1093-1103, Jan. 2013.

[9] L. Esterle and R. Grosu, "Cyber-physical systems: Challenge of the 21st century," *e+i Elektrotechnik und Informationstechnik,* vol. 133, no. 7, pp. 299-303, Nov. 2016.

[10] R. S. Shaji, V. Sachin Dev and T. Brindha, "A methodological review on attack and defense strategies in cyber warfare," *Wireless Networks,* vol. 25, no. 6, pp. 3323-3334, Aug. 2019.

[11] S. A. Haque, S. M. Aziz and M. Rahman, "Review of cyber-physical system in healthcare," *International Journal of Distributed Sensor Networks,* vol. 10, no. 4, p. 217415, Apr. 2014.

[12] H. Habibzadeh, T. Soyata, B. Kantarci, A. Boukerche and C. Kaptan, "Sensing, communication and security planes: A new challenge for a smart city system design," *Computer Networks,* vol. 144, pp. 163-200, Oct. 2018.

[13] L. Piwek, D. A. Ellis, S. Andrews and A. Joinson, "The rise of consumer health wearables: Promises and barriers," *PLOS Medicine,* vol. 13, no. 2, p. e1001953, Feb. 2016.

[14] O. Kocabas, T. Soyata and M. K. Aktas, "Emerging security mechanisms for medical cyber physical systems," *IEEE/ACM Transactions on Computational Biology and Bioinformatics,* vol. 13, no. 3, pp. 401-416, May 2016.

[15] N. Dey, A. S. Ashour, F. Shi, S. J. Fong and J. M. R. Tavares, "Medical cyber-physical systems: A survey," *Journal of Medical Systems,* vol. 42, no. 4, pp. 1-13, Apr. 2018.

[16] A. K. Das, P. H. Pathak, C. N. Chuah and P. Mohapatra, "Uncovering privacy leakage in BLE network traffic of wearable fitness trackers," in *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications (HotMobile '16)*, St. Augustine, FL, USA, 2016.

[17] J. Zhou, Z. Cao, X. Dong and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Communications Magazine,* vol. 55, no. 1, pp. 26-33, Jan. 2017.

[18] Y. Yang, X. Zheng, W. Guo, X. Liu and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," *Information Sciences,* vol. 479, pp. 567-592, Apr. 2019.

[19] G. G. Dagher, J. Mohler, M. Milojkovic and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable Cities and Society,* vol. 39, pp. 283-297, May 2018.

[20] M. Li, W. Lou and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications,* vol. 17, no. 1, pp. 51-58, Feb. 2010.

[21] F. Hak, D. Oliveira, N. Abreu, P. Leuschner, A. Abelha and M. Santos, "An OpenEHR adoption in a Portuguese healthcare facility," *Procedia Computer Science,* vol. 170, pp. 1047-1052, Jan. 2020.

[22] P. Park, S.-Y. Shin, S. Y. Park, J. Yun, C. Shin, J. Jung, K. S. Choi and H. S. Cha, "Next-generation sequencing–based cancer panel data conversion using international standards to implement a clinical next-generation sequencing research system: Single-institution study," *JMIR Medical Informatics,* vol. 8, no. 4, p. e14710, Apr. 2020.

[23] J. Goldman, "F2761 Medical devices and medical systems - Essential safety requirements for equipment comprising the patient-centric integrated clinical environment (ICE) - Part 1: General requirements and conceptual model," ASTM International, West Conshohocken, PA, USA, 2017.

[24] D. Arney, J. Plourde and J. M. Goldman, "OpenICE medical device interoperability platform overview and requirement analysis," *Biomedizinische Technik,* vol. 63, no. 1, pp. 39-47, Feb. 2018.

[25] H. Almohri, L. Cheng, D. Yao and H. Alemzadeh, "On threat modeling and mitigation of medical cyber-physical systems," in *Proceedings of the 2nd ACM/IEEE International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE 2017)*, Philadelphia, PA, USA, 2017.

[26] A. H. Celdrán, F. J. Garcia Clemente, J. Weimer and I. Lee, "ICE++: Improving security, QoS, and high availability of medical cyber-physical systems through mobile edge computing," in *Proceedings of the 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Ostrava, Czech Republic, 2018.

[27] R. Mitchell and I. R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," *IEEE Transactions on Dependable and Secure Computing,* vol. 12, no. 1, pp. 16-30, Jan. 2015.

[28] W. Meng, W. Li, Y. Wang and M. H. Au, "Detecting insider attacks in medical cyber–physical networks based on behavioral profiling," *Future Generation Computer Systems,* vol. 108, pp. 1258-1266, Jul. 2020.

[29] H. Qiu, M. Qiu, M. Liu and G. Memmi, "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0," *IEEE Journal of Biomedical and Health Informatics,* vol. 24, no. 9, pp. 2499-2505, Feb. 2020.

[30] G. Grispos, W. B. Glisson and K. K. R. Choo, "Medical cyber-physical systems development: A forensics-driven approach," in *Proceedings of the 2nd ACM/IEEE International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE 2017)*, Philadelphia, PA, USA, 2017.

[31] A. Alhayajneh, A. N. Baccarini, G. M. Weiss, T. Hayajneh and A. Farajidavar, "Biometric authentication and verification for medical cyber physical systems," *Electronics,* vol. 7, no. 12, p. 436, Dec. 2018.

[32] X. Zhang, J. Zhao, L. Mu, Y. Tang and C. Xu, "Identity-based proxy-oriented outsourcing with public auditing in cloud-based medical cyber–physical systems," *Pervasive and Mobile Computing,* vol. 56, pp. 18-28, May 2019.

[33] Z. Xu, D. He, H. Wang, P. Vijayakumar and K. K. Raymond Choo, "A novel proxy-oriented public auditing scheme for cloud-based medical cyber physical systems," *Journal of Information Security and Applications,* vol. 51, p. 102453, Apr. 2020.

[34] M. J. Butkovic and R. A. Caralli, Advancing cybersecurity capability measurement using the CERT®-RMM maturity indicator level scale, Pittsburgh, PA, USA: Carnegie-Mellon University, 2013.

[35] J. W. Lainhart, "COBIT™: A methodology for managing and controlling information and information technology risks and vulnerabilities," *Journal of Information Systems,* vol. 14, no. s-1, pp. 21-25, Jan. 2000.

[36] G. Disterer and G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information security management," *Journal of Information Security,* vol. 4, no. 2, pp. 92-100, Apr. 2013.

[37] J. L. Fongen, "Manage risks to achieve an appropriate level of security: To what extent does security requirements imposed on critical sectors align with a high common level of security on network and information systems?," University of Oslo, Oslo, Sweden, 2020.

[38] J. H. Eloff and M. M. Eloff, "Information security architecture," *Computer Fraud & Security,* no. 11, pp. 10-16, 11 2005.

[39] K. Dempsey, G. Witte and D. Rike, "Summary of NIST SP 800-53 revision 4, security and privacy controls for federal information systems and organizations," National Institute of Standards and Technology (NIST), Annapolis Junction, MD, USA, 2014.

[40] A. Aliyu, L. Maglaras, Y. He, I. Yevseyeva, E. Boiten, A. Cook and H. Janicke, "A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom," *Applied Sciences,* vol. 10, no. 10, p. 3660, May 2020.

[41] A. Georgiadou, S. Mouzakitis and D. Askounis, "Working from home during COVID-19 crisis: a cyber security culture assessment survey," *Security Journal,* vol. 35, no. 2, pp. 486-505, Jun. 2022.

[42] A. Georgiadou, S. Mouzakitis, K. Bounas and D. Askounis, "A cyber-security culture framework for assessing organization readiness," *Journal of Computer Information Systems,* vol. 62, no. 3, pp. 452-462, May 2020.

[43] D. Proença and J. Borbinha, "Maturity models for data and information management," in *Proceedings of the 22nd International Conference on Theory and Practice of Digital Libraries (TPDL 2018)*, Porto, Portugal, 2018.

[44] R. Sabillon, J. Serra-Ruiz, V. Cavaller and J. Cano, "A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM)," in *Proceedings of the International Conference on Information Systems and Computer Science (INCISCOS 2017)*, Quito, Ecuador, 2017.

[45] R. M. Adler, "A dynamic capability maturity model for improving cyber security," in *Proceedings of the International Conference on Technologies for Homeland Security (HST 2013)*, Waltham, MA, USA, 2013.

[46] R. Akkiraju, V. Sinha, A. Xu, J. Mahmud, P. Gundecha, Z. Liu, X. Liu and J. Schumacher, "Characterizing machine learning processes: A maturity framework," in *Proceedings of the 18th International Business Process*

Management (BPM 2020) Conference, Seville, Spain, 2020.

[47] S. Almuhammadi and M. Alsaleh, "Information security maturity model for NIST cyber security framework," in *Proceedings of the 6th International Conference on Information Technology Convergence and Services (ITCS 2017)*, Sydney, Australia, 2017.

[48] W. Miron and K. Muita, "Cybersecurity capability maturity models for providers of critical infrastructure," *Technology Innovation Management Review,* vol. 4, no. 10, pp. 33-39, Oct. 2014.

[49] S. Cheang, "Conceptual model for cybersecurity readiness assessement for public institutions in developing country: Cambodia," in *Proceedings of the 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT '09)*, Seoul, Korea, 2009.

[50] M. M. Yunis and K. S. Koong, "A conceptual model for the development of a national cybersecurity index: An integrated framework," in *Proceedings of the 21st Americas Conference on Information Systems (AMCIS 2015)*, Fajardo, Puerto Rico, 2015.

[51] G. M. Lee, "Trust in ICT," International Telecommunication Union (ITU), Geneva, Switzerland, 2017.

[52] K. Farahbod, C. Shayo and J. Varzandeh, "Cybersecurity indices and cybercrime annual loss and economic impacts," *Journal of Business and Behavioral Sciences,* vol. 32, no. 1, pp. 63-71, Mar. 2020.

[53] J. Wang, H. Abid, S. Lee, L. Shu and F. Xia, "A secured health care application architecture for cyber-physical systems," *Control Engineering and Applied Informatics,* vol. 13, no. 3, pp. 101-108, Dec. 2011.

[54] A. Banerjee, S. K. Gupta, G. Fainekos and G. Varsamopoulos, "Towards modeling and analysis of cyber-physical medical systems," in *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL '11)*, Barcelona, Spain, 2011.

[55] F. J. Wu, Y. F. Kao and Y. C. Tseng, "From wireless sensor networks towards cyber physical systems," *Pervasive and Mobile Computing,* vol. 7, no. 4, pp. 397-413, Aug. 2011.

[56] E. Sultanovs, A. Skorobogatjko and A. Romanovs, "Centralized healthcare cyber-physical system's architecture development," in *Proceedings of the 57th International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON 2016)*, Riga, Latvia, 2016.

[57] F. Akowuah, X. Yuan, J. Xu and H. Wang, "A survey of security standards applicable to health information systems," *International Journal of Information Security and Privacy,* vol. 7, no. 4, pp. 22-36, Oct. 2013.

[58] M. Spruit and M. Röling, "ISFAM: The information security focus area maturity model," in *Proceedings of the 22nd European Conference on Information Systems (ECIS 2014)*, Tel Aviv, Israel, 2014.

[59] R. E. Moffit and B. Steffen, "Health care data breaches: A changing landscape," Maryland Health Care Commission (MHCC), Baltimore, MD, USA, 2017.

[60] Office of the Government Chief Information Officer, "Smart city development in Hong Kong," *IET Smart Cities,* vol. 1, no. 1, pp. 23-27, Jun. 2019.

[61] International Telecommunication Union & ABIresearch, "Global cybersecurity index & cyberwellness profiles," International Telecommunication Union (ITU), Geneva, Switzerland, 2015.

[62] M. Hathaway, C. Demchak, J. Kerben, J. Mcardle and F. Spidalieri, "Cyber readiness index 2.0 - A plan for cyber readiness: A baseline and an index," Potomac Institute for Policy Studies, Arlington, Virginia, 2015.

[63] O. O. Akinsanya, M. Papadaki and L. Sun, "Current cybersecurity maturity models: How effective in current cybersecurity maturity models: How effective in healthcare cloud? healthcare cloud?," in *Proceedings of the 5th Collaborative European Research Conference (CERC 2019)*, Darmstadt, Germany, 2019.

[64] N. T. Le and D. B. Hoang, "Can maturity models support cyber security?," in *Proceedings of the 35th International Performance Computing and Communications Conference (IPCCC 2016)*, Las Vegas, NV, USA, 2017.

[65] M. Evans, L. A. Maglaras, Y. He and H. Janicke, "Human behaviour as an aspect of cybersecurity assurance," *Security and Communication Networks,* vol. 9, no. 17, pp. 4667-4679, Nov. 2016.

[66] K.-F. Khiew, M. Chen, B.-C. Shia, C.-H. Pan, K.-F. Khiew, M. Chen, B.-C. Shia and C.-H. Pan, "The implementation of adopted balanced scorecard with new insight strategy framework for the healthcare industry: A case study," *Open Journal of Business and Management,* vol. 8, no. 2, pp. 600-627, Jan. 2020.

[67] M. Nour, H. Sindi, E. Abozinadah, Ş. Öztürk and K. Polat, "A healthcare evaluation system based on automated weighted indicators with cross-indicators based learning approach in terms of energy management and cybersecurity," *International Journal of Medical Informatics,* vol. 144, p. 104300, Dec. 2020.

[68] S. Banihashemi, M. R. Hosseini, H. Golizadeh and S. Sankaran, "Critical success factors (CSFs) for integration of sustainability into construction project management practices in developing countries," *International Journal of Project Management,* vol. 35, no. 6, pp. 1103-1119, Aug. 2017.

[69] M. Niazi, D. Wilson and D. Zowghi, "Critical success factors for software process improvement implementation: An empirical study," *Software Process: Improvement and Practice,* vol. 11, no. 2, pp. 193-211, Mar. 2006.

[70] M. A. Moktadir, A. Kumar, S. M. Ali, S. K. Paul, R. Sultana and J. Rezaei, "Critical success factors for a circular economy: Implications for business strategy and the environment," *Business Strategy and the Environment,* vol. 29, no. 8, pp. 3611-3635, Dec. 2020.

[71] A. Moeuf, S. Lamouri, R. Pellerin, S. Tamayo-Giraldo, E. Tobon-Valencia and R. Eburdy, "Identification of critical success factors, risks and opportunities of Industry 4.0 in SMEs," *International Journal of Production Research,* vol. 58, no. 5, pp. 1384-1400, Mar. 2020.

[72] K. Arbanas and N. Ž. Hrustek, "Key success factors of information systems security," *Journal of Information and Organizational Sciences,* vol. 43, no. 2, pp. 131-144, Dec. 2019.

[73] A. C. Shinohara, E. H. D. R. da Silva, E. P. de Lima, F. Deschamps and S. E. G. da Costa, "Critical success factors for digital manufacturing implementation in the context of industry 4.0," in *Proceedings of the Industrial and Systems Engineering Conference*, Pittsburgh, PA, USA, 2017.

[74] C. Granja, W. Janssen and M. A. Johansen, "Factors determining the success and failure of eHealth interventions: Systematic review of the literature," *Journal of Medical Internet Research,* vol. 20, no. 5, p. e10235, May 2018.

[75] Z. Din, D. I. Jambari, M. M. Yusof and J. Yahaya, "Critical success factors for managing information systems security in smart city enabled by Internet of Things," *International Journal of Advanced Research in Engineering and Technology,* vol. 11, no. 12, pp. 1108-1120, Dec. 2020.

[76] K. Peffers, T. Tuunanen, M. A. Rothenberger and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems,* vol. 24, no. 3, pp. 45-77, Dec. 2007.

[77] A. Hevner and S. Chatterjee, "Design research in information systems," in *Design research in information systems: Theory and practice*, vol. 22, R. Sharda and S. Voß, Eds., Boston, MA, USA, Springer Publishing, 2010, pp. 9-22.

[78] K. Peffers, M. Rothenberger, T. Tuunanen and R. Vaezi, "Design science research evaluation," in *Proceedings of the 7th International Conference on Design Science Research in Information Systems (DESRIST 2012)*, Las Vegas, NV, USA, 2012.

[79] J. Venable, J. Pries-Heje and R. Baskerville, "A comprehensive framework for evaluation in design science research," in *Proceedings of the 7th International Conference on Design Science Research in Information Systems (DESRIST 2012)*, Las Vegas, NV, USA, 2012.

[80] P. Johannesson and E. Perjons, An introduction to design science, 2 ed., P. Johannesson and E. Perjons, Eds., Cham, Switzerland: Springer International Publishing AG, 2021, pp. 1-211.

[81] D. Arnott and G. Pervan, "Design science in decision support systems research: An assessment using the Hevner, March, Park, and Ram Guidelines," *Journal of the Association for Information Systems,* vol. 13, no. 11, p. 1, Nov. 2012.

[82] A. Dresch, D. P. Lacerda and J. A. V. Antunes Jr, "Proposal for the conduct of design science research," in *Design science research: A method for science and technology*

advancement, 1 ed., A. Dresch, D. P. Lacerda and J. A. V. Antunes Jr, Eds., Cham, Switzerland, Springer International Publishing AG, 2014, pp. 117-127.

[83] Microsoft 365, "The importance of two-factor authentication," *Microsoft 365 Life Hacks,* pp. -, 8 July 2022.

[84] R. Verma, "Smart city healthcare cyber physical system: Characteristics, technologies and challenges," *Wireless Personal Communications,* vol. 122, no. 2, pp. 1413-1433, Jan. 2022.

[85] O. F. Keskin, K. M. Caramancion, I. Tatar, O. Raza and U. Tatar, "Cyber third-party risk management: A comparison of non-intrusive risk scoring reports," *Electronics,* vol. 10, no. 10, p. 1168, May 2021.

[86] S. K. Al-Kaabi, M. A. Chehab, N. Selim, S. K. Al-Kaabi, M. A. Chehab and N. Selim, "The balanced scorecard as a performance management tool in the healthcare sector – The case of the Medical Commission Department at the Ministry of Public Health, Qatar," *Cureus,* vol. 11, no. 7, p. e5262, Jul. 2019.

[87] F. Amer, S. Hammoud, H. Khatatbeh, S. Lohner, I. Boncz and D. Endrei, "The deployment of balanced scorecard in health care organizations: Is it beneficial? A systematic review," *BMC Health Services Research,* vol. 22, no. 1, pp. 1-14, Dec. 2022.