ISSN No:-2456-2165

A Balanced Information Security Maturity Model Based on ISO/IEC 27001:2013 and O-ISM3

Professor Dr. Muneer A.S Hazza Almekhlafi
Faculty of Computer Science and Information Technology
Dhamar University
dr.Muneer.hazza@tu.edu.ye

Maged Sultan A.A Almekhlafi
Faculty of Computer Science and Information Technology
Yemen Academy for Graduate Studies
majid.sultan@ptc.gov.ye

Abstract:- Today, Information technology is widely used in most fields, and most companies depend on information systems to assist in doing their daily work. In most cases, business continuity requires companies to be connected to the internet, and this exposes information to different risks and increases the probability of exposure of information to security threats and cyber-attacks. These risks can be mitigated by adopting an information security management system (ISMS). Currently, a wide range of information security maturity models have been developed to be used by different types of organizations in order to implement and evaluate the maturity level of information security. This research proposes an information security maturity model named (BISM) with three progressive maturity levels (Basic, Intermediate, Advanced) which contain 54 security controls obtained by mapping and merging the 114 security controls of ISO/IEC 27001:2013 and the 45 security processes of O-ISM3. The security controls of BISM are chosen carefully to cover the most needs of organizations to implement ISMS with high flexibility. This model could be of great value for all types of organizations as it helps them to precisely assess the maturity of information security management system and enables them to establish and implement an ISMS by choosing and applying the most important security controls that are more suitable to their sizes and business needs.

Keywords:- *Information Security, Maturity Model, ISMS, ISO/IEC 27001, O-ISM3, Cybersecurity Introduction.*

I. INTRODUCTION

Most businesses, whether they are small, medium-sized, or large, public or private, profitable or non-profitable, depend heavily on information technology because information technology helps organizations to do their day-to-day tasks. In reality, information technology has become a part of our daily lives whether at work or during time of leisure. It can be seen in most fields of our life, such as communication, learning, health, agriculture, finance etc. Information technology enables organizations to work more efficiently, reduce costs, maximize productivity and enhance the quality of their services. In general, information technology attempts or seeks to automate processes and common administration tasks [1,2]. Due to the increased reliance on information technology to do most of the works in our everyday life and daily work and due to the information security risks that pose threats to the continuity and availability of information systems, especially the risks stemming from cyber-attacks, organizations have to be responsible for managing information security risks. This task can be can be applied by adopting a comprehensive information security management system (ISMS) to manage all information security tasks and related activities within organizations themselves and to ensure that all security objectives are aligned with all organizations' goals. In general, ISMS develop, carry out, run, maintain, and enhance information security policies and procedures. The demands and objectives of the company, the processes used, the size and structure of the organization, the security requirements, and other factors should all be taken into consideration while establishing and implementing an ISMS [3].

In the realm of information systems, the idea of maturity models is frequently applied as a method for organizational evaluation. ISMS with maturity models can offer more benefits by helping organizations to control, manage and enhance the implementation process of information security procedures and processes. They can also be used to evaluate the capabilities of ISMS implemented by the organizations. In addition to that, it can be used to measure how the organizations are capable of protecting their information [4]. Currently, many frameworks that used to assess, manage and implement information security management system (ISMS) exist. ISO/IEC 27001:2013, COBIT 5, ISO 31000:2009, O-ISM3, NIST, CIS and SOC 2 are examples for popular frameworks that can help organizations to adopt ISMS according to their information security objectives [5].

II. LITERATURE REVIEW

Many searchers used most of the popular ISMS standards to design information security maturity models to be used by different industries. According to Mettler et al. [4] more than 100 models are developed in the information systems sector, for example Fariba Ghaffari and Abouzar Arabsorkhi (2018) proposed an "Adaptive Cyber-security Capability Maturity Model" by using a systematic literature review by collecting the security processes and controls from various security maturity models such as (COBIT5, ISM3, PRISAM, ISF, C2M2, ISO 27001) [5]. Sabillon et al. (2017) proposed a Cyber Security Audit Model (CSAM) in order to improve cybersecurity assurance, the CSAM was designed to be used for conducting cybersecurity audits in organizations and Nation States [6]. Almuhammadi and M. Alsaleh (2017) proposed an information security maturity model (ISMM) which consists of 23 assessed areas by identifying the gaps of the NIST Cyber Security Framework for Critical Infrastructure (NIST CSF) and comparing it to the COBIT, ISO/IEC 27001 and ISF frameworks [7]. Diogo Proenca and Jose Borbinha (2018) proposed a maturity model with five maturity levels for planning, implementation, monitoring and improvement of ISMS based on ISO/IEC 27001 [8].

III. PROPOSED MODEL

To design the proposed model, security controls of ISO 27001 and security processes of O-ISM3 are mapped and merged first to obtain security controls of the proposed model, Then, scoring method is used to set scores for security controls and maturity levels.

A. Mapping and Merging ISO:2007/2013 and O-ISM3

To carry out mapping and merging the security controls of the two standards (ISO 27001:2013 and O-ISM3), two steps were processed (direct and undirect mapping).

➢ *Direct Mapping*

The core difference between O-ISM3 and ISO 27001 is that the ISO 27001 deeply defines the security controls that are needed to implement ISMS, whereas O-ISM3 addresses ISM and maturity using an approach based on processes. It was found that it is not feasible to align every security control in ISO/IEC 27001with each security process of O-ISM3 because every security control can be implemented by one or more processes in O-ISM3 and vice versa. Consequently, the comparison was necessarily implemented by comparing the whole security controls in each security objectives of ISO/IEC 27001 with all O-ISM3 processes that can be used to implement those controls. To fulfill this alignment, a table (containing the security controls of the 18 security objectives of ISO/IEC 27001) is designed to align the controls of ISO/IEC 27001:2013 with the equivalent process of O-ISM3. Then, the proposed controls are selected based on merging security controls of ISO 27001 and O-ISM3, with keeping their core functions. Eventually, 52 distinct controls are obtained from this step. Table 1 shows mapping and merging of the two standards used in the research. It should be noticed that only the security objectives of ISO 27001 are mentioned without the security controls themselves in order to decrease the size of table, but as mentioned above the entire controls of each security objective were used during the mapping step.

TABLE1: MAPPING and MERGING ISO 27001and O-ISM2.

A.5 Information security policies		
ISO Security Objectives	**O-ISM3 Processes**	**Proposed Controls**
A.5.1 Management direction for information security	GP-3 ISM Design and Evolution TSP-3 Define Security Targets SSP-2 Coordination SSP-6 Allocate Resources for Information Security GP-2 ISM and Business Audi	• ISM Design • Review and evolution of ISM • Coordination • Allocate Resources for Information Security
A.6 Organization of Information Security		
ISO Security Objectives	**O-ISM3 Processes**	**Proposed Controls**
A.6.1 Internal Organization	SSP-2 Coordination TSP-13 Insurance Management SSP-4 Define Division of Duties Rules	• Define Division of Duties Rules • Coordination • Insurance
A.6.2 Mobile Devices and Teleworking	OSP-16 Segmentation and Filtering Management	• Networks Segregation and Segmentation
A.7 Human Resource Security		
ISO Security Objectives	**O-ISM3 Process**	**Proposed Controls**
A.7.1 Prior to Employment	TSP-7 Background Checks TSP-8 Personnel Security	• Background Checks • Personnel Security
A.7.2 During Employment	TSP-8 Personnel Security TSP-9 Security Personnel Training. TSP-11 Security Awareness	• Management responsibilities • Personnel Security • Security Personnel Training • Security Awareness • Disciplinary Process
A.7.3 Termination and Change of Employment	OSP-12 User Registration	• User Registration
A.8 Asset Management		
ISO Security Objectives	**O-ISM3 Process**	**Proposed Controls**
A.8.1 Responsibility for Assets	OSP-3 Inventory Management TSP-2 Managed Allocated Resources	• Inventory Management • Assets Ownership • Managed Allocated Resources
A.8.2 Information Classification	OSP-3 Inventory Management TSP-2 Managed Allocated Resources OSP-21 Information Quality and Compliance Assessment OSP-4: Information Systems Environment Change Control	• Classification of Information • Managed Allocated Resources • Information Quality • Compliance with Legal and Standards • Information Systems Environment Change
A.8.3 Media Handling	OSP-3 Inventory Management OSP-6 IT Managed Domain Clearing	• Removable Media • IT Managed Domain Clearing

	OSP-4 Information Systems Environment Change Control	• Information Systems Environment Change
A.9 Access Control		
ISO Security Objectives	**O-ISM3 Process**	**Proposed Controls**
A.9.1 Business Requirements of Access Control	OSP-11 Access Control	• Access Control
A.9.2 User Access Management	OSP-11 Access Control OSP-12 User Registration OSP-19 Internal Technical Audit	• Access Control • User Registration • Review and Adjustment of Access Rights • Internal Technical Audit
A.9.3 User Responsibilities	OSP-12 User Registration	• User Registration
A.9.4 System and Application Access Control	OSP-11 Access Control OSP-12 User Registration	• Access Control • User Registration • Passwords Management
A.10 Cryptography		
ISO Security Objectives	**O-ISM3 Process**	**Proposed Controls**
A.10.1 Cryptographic Controls	OSP-12 User Registration	• User Registration • Cryptographic
A.11 Physical and Environmental Security		
ISO Security Objectives	**O-ISM3 Process**	**Proposed Controls**
A.11.1 Secure Areas	OSP-11 Access Control OSP-14 Physical Environment Protection Management	• Working in Secure Areas • Access Control • Physical Environment Protection
A.11.1.2 Equipment	OSP-4 Information Systems Environment Change Control OSP-6 IT Managed Domain Clearing OSP-7 IT Managed Domain Hardening OSP-14 Physical Environment Protection Management	• Equipment Siting and Protection • IT Managed Domain Clearing • Supporting Utilities • Physical Environment Protection • Information Systems Environment Change
A.12 Operations Security		
ISO Security Objectives	**O-ISM3 Process**	**Proposed Controls**
A.12.1 Operational Procedures and Responsibilities	GP-1 Knowledge Management OSP-4 Information Systems Environment Change Control OSP-9 Security Measures Change Control OSP-27 Archiving Management	• Knowledge Management • Information Systems Environment Change • Security Measures Change • Capacity and Archiving • Separation of development, testing and operational environments
A.12.2 Protection from Malware	OSP-17 Malware Protection Management	• Malware Protection
A.12.3 Backup	OSP-10 Backup Management	• Backup
A.12.4 Logging and Monitoring	OSP-22 Alerts Monitoring OSP-23 Internal Events Detection and Analysis	• Information Security Events • Internal Events Detection and Analysis
A.12.5 Control of Operational Software	OSP-4 Information Systems Environment Change Control	• Information Systems Environment Change
A.12.6 Technical Vulnerability Management	OSP-22 Alerts Monitoring OSP-23 Internal Events Detection and Analysis OSP-5 IT Managed Domain Patching	• Internal Events Detection and Analysis • Software Installation • IT Managed Domain Patching
A.12.7 Information Systems Audit Considerations	OSP-19 Internal Technical Audit	• Internal Technical Audit
A.13 Communications security		
ISO Security Objectives	**O-ISM3 Process**	**Proposed Controls**
A.13.1 Network Security Management	OSP-16 Segmentation and Filtering Management	• Networks Segregation and Segmentation
A.13.2 Information Transfer	OSP-16 Segmentation and Filtering Management	• Information Transfer • Networks Segregation and Segmentation
A.14 System Acquisition, Development and Maintenance		
ISO Security Objectives	**O-ISM3 Process**	**Proposed Controls**

ISSN No:-2456-2165

A.14.1 Security Requirements of Information Systems	OSP-7 IT Managed Domain Hardening OSP-8 Software Development Lifecycle Control OSP-11 Access Control	• Internal Technical Audit • Access Control
A.14.2 Security in Development and Support Processes	OSP-4 Information Systems Environment Change Control OSP-6 Security Architecture OSP-8 Software Development Lifecycle Control	• Information Systems Environment Change • Test and Development Environment • Internal Technical Audit
A.14.3 Test Data	OSP-11 Access Control	• Access Control
A.l5 Supplier Relationships		
ISO Security Objectives	**O-ISM3 Process**	**Proposed Controls**
A.l5.1 Information Security in Supplier Relationship	OSP-2 Security Procurement	• Supplier Relationship
A.l5.2 Supplier Service Delivery Management	OSP-2 Security Procurement	• Supplier Relationship
A.16 Information Security Incident Management		
ISO Security Objectives	**O-ISM3 Process**	**Proposed Controls**
A.16.1 Management of information Security Incidents and Improvements	SSP-1 Report to Stakeholders TSP-1 Report to Strategic Management OSP-1 Report to Tactical OSP-20 Incident Emulation OSP-23 Internal Events Detection and Analysis OSP-24 Handling of Incidents and Near-incidents OSP-25 Forensics	• Incidents Handling • Internal Events Detection and Analysis • Incidents Emulation • Learning From Information Security Incidents • Information Security Reports • Forensics
A.17 Information Security Aspects of Business Continuity Management		
ISO Security Objectives	**O-ISM3 Process**	**Proposed Controls**
A.17.1 Information Security Continuity	OSP-15 Operations Continuity Management OSP-20 Incident Emulation	• Operations Continuity • Incidents Emulation
A.17.2 Redundancy	OSP-15 Operations Continuity Management OSP-26 Enhanced Reliability and Availability Management	• Operations Continuity
A.18 Compliance		
ISO Security Objectives	**O-ISM3 Process**	**Proposed Controls**
A.18.1 Compliance with Legal and Contractual Requirements	OSP-21 Information Quality and Compliance Assessment GP-3 ISM Design and Evolution OSP-27 Archiving Management	• Compliance with Legal and Standards • Protection of Records • Capacity and Archiving • ISM Design
A.18.2 Information Security Reviews	GP-2 ISMS and Business Audit OSP-19 Internal Technical Audit OSP-21 Information Quality and Compliance Assessment	• Review and Evolution of ISM • Compliance With Legal and Standards

B. Undirect Mapping

In undirect mapping, the security process of O-ISM3 which were not mapped due to the absence of matching controls from ISO 27001 were discussed. There were four processes not mapped to ISO (TSP-4, TSP-6, TSP-14 and OSP-28), these processes were studied separately and two processes (TSP-14 and OSP-28) were selected and added to the proposed model. The 54 security and privacy controls of BISM are shown in Table 2. They are distributed to three levels of maturity (Basic, Intermediate, Advanced) and three levels according to Management, Technical , Operational (MTO) classification (based on Federal Enterprise Architecture Framework (FEAF) classification). These security controls are also coded by assigning each control a unique code according to the level in which it is located.

TABLE 2: SECURITY CONTROLS of BISM WITH MATURIY AND MTO LEVELS.

Level	**Basic**		**Intermediate**		**Advanced**	
Management	MB-1	ISM Design	MI-1	Define Division of Duties Rules	MA-1	Internal Technical Audit
	MB-2	Review and Evolution of ISM	MI-2	Management Responsibilities	MA-2	External Events Detection and Analysis
	MB-3	Compliance with Legal and Standards	MI-3	Allocate Resources for Information Security	MA-3	Information Operations
	MB-4	Knowledge Management	MI-4	Managed Allocated Resources	MA-4	Insurance
	MB-5	Coordination	MI-5	Supplier Relationships	MA-5	Disciplinary Process
	MB-6	Ownership of Assets	MI-6	Inventory Management	MA-6	Forensics
			MI-7	Software Installation		
Level	**Basic**		**Intermediate**		**Advanced**	
Technical	TB-1	User Registration	TI-1	Operations Continuity	TA-1	Cryptographic
	TB-2	Access Control	TI-2	Classification of Information	TA-2	Internal Events Detection and Analysis
	TB-3	Passwords Management	TI-3	Information Quality		
	TB-4	Information Security Events	TI-4	Information transfer		
	TB-5	Networks Segregation and Segmentation	TI-5	Test and Development Environment		
	TB-6	Malware Protection				
	TB-7	Protection of Records				
	TB-8	Capacity and Archiving				
	TB-9	Separation of Development, Testing and Operational Environments				
Level	**Basic**		**Intermediate**		**Advanced**	
Operational	OB-1	Information Security Reports	OI-1	Security Personnel Training	OA-1	Security Awareness
	OB-2	Review and Adjustment of User Access Rights	OI-2	IT Managed Domain Clearing	OA-2	Personnel of Information Security
	OB-3	Backup	OI-3	IT Managed Domain Patching	OA-3	Employees Background Checks
	OB-4	Equipment Siting and Protection	OI-4	Physical Environment Protection	OA-4	Incidents Emulation
	OB-5	Working in Secure Areas	OI-5	Incidents Handling	OA-5	Learning from Information Security Incidents
	OB-6	Supporting Utilities	OI-6	Information Systems Environment Change		
			OI-7	Security Measures Change		
			OI-8	Removable Media		

IV. BISM SCORING METHOD

BISM model is a hybrid maturity model because it has stage (progressive) levels of maturity which contains three levels of stages (Basic, Intermediate, Advanced), and inside each stage level there are the attributes (security and privacy controls). The assessment and implementation of these controls shall use a capability maturity model. Any available capability maturity model such as CMMI or O-ISM3 can be used to assess the maturity of the security controls themselves. For the scoring of stage levels of BISM model, a scoring method is set by assigning a different weight to each level and an equal score is assigned to each control in the same level. Total weight of all levels of the model is set to be 100. After examining the number of controls in each level and their effect on the whole maturity of the model, a scoring method is chosen as shown in table 3.

TABLE 3: WEIGHTS and SOCORS of BISM MODEL.

Level	**Score / Control**	**No. of Controls**	**Scores of Levels**
Basic	1	21	21
Intermediate	2	20	40
Advanced	3	13	39
Total		54	100

Fig. 1 shows the difference between using the scoring method of BISM and the traditional one that assigs an equal score for each control. This score is 1.85 obtained by dividing 100 to the total number of controls (54).

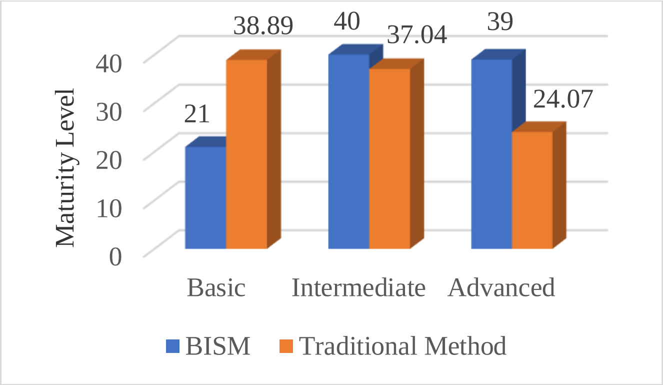

Fig. 1: LEVELS MATURITY COMARISION.

V. TESTING MATURITY LEVELS OF BISM

A survey questionnaire is used to test the allocation of the security controls to the maturity levels of BISM. It is assumed that the security controls of the Basic level shall obtain higher compliance scores, then the intermediate level controls and finally the Advanced level controls. Fig. 2 shows the obtained compliance values of all security controls in each maturity level (Basic, Intermediate, Advanced). These values were calculated as the average of the security controls in each level. Fig. 2 illustrates that the maturity score for each level is (65.63, 60.36, 52.84) respectively, meaning that the Basic Level has higher compliance values than the Intermediate Level whereas the Advanced Level has the lowest values.

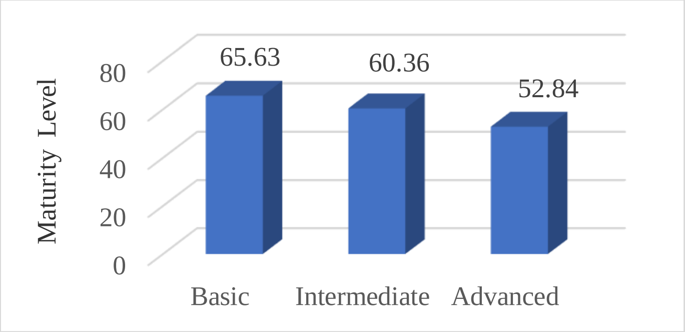

Fig. 2: COMPLIANCE VALUES of LEVELS.

In general, it can be confirmed that the overall maturity of the three levels is satisfactory and most security controls of BISM model are appropriately distributed into the three levels of maturity. Detailed results showed that all security controls of BISM model obtained the expected compliance values except 9 controls which are shown in Table 4. All of these controls obtained lower compliance values than expected except (TI-1: Operations Continuity) which obtain higher compliance value.

TABLE 4: UNSATISFIED SECURITY CONTROLS.

Management	MB-1: ISM Design
	MB-2: Review and Evolution of ISM
	MB-3: Coordination.
	MB-4: Knowledge Management.
	MB-5: Compliance with Legal and Standards
Technical	TI-1: Operations Continuity
Operational	OB-1 Information Security Reports
	OI-1 Security Personnel Training
	OI-2 IT Managed Domain Clearing

It can be observed that most of these security controls are management controls which are used to plan, control and monitor ISMS, this means most organizations implement ISMS in unorganized approach. According to BISM these security controls are of paramount importance and should be applied first because they are used for planning and monitoring ISMS.

VI. CONCLUSION

This research focused on developing an information security maturity model based on two of leading standards in information security (ISO/IEC 27001:2013 and O-ISM3). The proposed model (BISM) in this research contains 54 security and privacy controls obtained by merging the 114 controls of ISO/IEC 27001 and 45 of O-ISM. The BISM model was flexibly designed with three levels of maturity (Basic, Intermediate, Advanced) each of which has its own security controls: 21, 20 and 13 respectively. It is concluded that when implementing the BISM model, it enables organization to prioritize and enhance their investments when implementing ISMS by applying security controls sequentially starting with the security controls of the Basic level then the intermediate level and finally the Advanced level. In addition, the three levels of maturity of BISM help organizations to choose the appropriate level of maturity according to their size. The results of the testing for the BISM model conducted by using a survey questionnaire involved 72 IT experts in 30 organizations from different sectors in Yemen showed a high compliance value (83.33%). This result could emphasize that the security controls of BISM model were distributed fairly appropriately to the proposed maturity levels.

REFERENCES

[1]. International Organization for Standardization/ International Electrotechnical Commission, ISO 27001:2013: Information technology – Security techniques – Information security management systems – Requirements, 2013.

[2]. The Open Group, Open Information Security Management Maturity Model (O-ISM3), 2017. [Online]. Available: https://www.opengroup.org/forum/security/infosecmanagement

[3]. M. J. Butkovic and R. A. Caralli, Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale. Technical Report CMU/SEI-2013-TN-028, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA,2013.

[4]. T. Mettler, P. Rohner, and R. Winter, "Towards a classification of maturity models in information systems," Management of the Interconnected World, Physica-Verlag, Heidelberg, pp. 333-340, 2010.

[5]. F. Ghaffari, A. Arabsorkhi, "A New Adaptive Cyber-Security Capability Maturity Model," 9th International Symposium on Telecommunications, IEEE, 2018.

[6]. R. Sabillon, J. Serra-Ruiz, V. Cavaller, and J. Cano, "A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM)," International Conference on Information Systems and Computer Science (INCISCOS), IEEE, pp. 253–259, 2017.

[7]. S. Almuhammadi and M. Alsaleh, “Information security maturity model for NIST cyber security framework,” Computer Science & Information Technology (CS & IT), vol. 7, pp. 51–62, 2017.

[8]. D. Proença and J. Borbinha, “Information Security Management Systems - A Maturity Model Based on ISO/IEC 27001,” International Conference on Business Information Systems, Springer, vol. 320, pp. 102–114, 2018.

[9]. International Standard Organization and International Standard Technical Specification ISO/IEC, Information technology Process assessment - Process capability assessment model for Information Security Management, 2016.

[10]. International Standard Organization, Information security management systems - overview and vocabulary - ISO Standard 27000. 3rd edition, 2014.

[11]. Caralli and Rich, Discerning the Intent of Maturity Models from Characterizations of Security Posture. Software Engineering Institute, Carnegie Mellon University, 2012.

[12]. Nolan and L. Richard, “Managing the Computer Resource: a Stage Hypothesis,” Communications of the ACM, vol. 16, no. 7, pp 399–405, 1973.

[13]. C. Dawson, Introduction to Research Methods 5th Edition: A Practical Guide for Anyone Undertaking a Research Project Paperback, 5th edition, Robinson, 2019.

[14]. American Federal CIO Office, Federal Enterprise Architecture Framework Version 2. 2013. [Online]. Available: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf.

[15]. National Institute of Standards and Technology (NIST), NIST Special Publications revision 5, 2022. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[16]. National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity version 1.1, 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.

[17]. 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” School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK, 2020.