2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)

A NIS Directive compliant Cybersecurity Maturity Assessment Framework

George Drivas
Department of Digital Systems
University of Piraeus
Piraeus, Greece &
National Cyber Security Authority of Greece

Argyro Chatzopoulou
APIROPLUS Solutions
Limassol, Cyprus

Leandros Maglaras
Faculty of Computing, Engineering and Media
De Montfort University &
National Cyber Security Authority of Greece

Costas Lambrinoudakis
Department of Digital Systems
University of Piraeus
Piraeus, Greece

Allan Cook
and Helge Janicke
Faculty of Computing, Engineering and Media
De Montfort University

***Abstract*—The EU NIS Directive introduces obligations related to the security of the network and information systems for Operators of Essential Services and for Digital Service Providers. Moreover, National Competent Authorities for cybersecurity are required to assess compliance with these obligations. This paper describes a novel Cybersecurity Maturity Assessment Framework (CMAF) that is tailored to the NIS Directive requirements. CMAF can be used either as a self-assessment tool from Operators of Essential Services and Digital Service Providers or as an audit tool from the National Competent Authorities for cybersecurity.**

1. Introduction

Cyber attacks could contribute towards the collapse of a state if they initiate or prolong the failure of Critical National Infrastructures (CNI). Nations are becoming reliant on the cyber domain to provide services that keep a nation running: power grids, water supplies, communications, transportation, and finance are all increasingly becoming cyber dependant.

The NIS Directive (Directive (EU) 2016/1148) (European Union, 2016) has certain obligations that each member state should follow, with a major goal of enhancing cybersecurity posture across the EU. Having to cope with the obligations of the NIS Directive and to meet strict deadlines, Greece has taken some steps forward [1]. The directive and a relevant national Law (Greek National Law 4577/2018)(Greek Government, 2018) introduce obligations for the security of the network and information systems of Operators Of Essential Services (OES) and the security of the network and information systems of Digital Service Providers (DSP) and require from the National Competent Authorities (NCA) to assess the compliance of OES and DSP with these obligations.

More specifically, the Greek National Law 4577/2018 (Greek Government, 2018) states that "the National Cyber Security Authority (NCSA), acting as the NCA for cybersecurity, in collaboration with the relevant CSIRTs and other organizations and entities, as appropriate, assesses the technical and organizational measures implemented by OES, in order to manage risks related to the security of network and information systems used in their activities, regarding their suitability and their proportionality". Additionally, NCSA "assesses the suitability of the measures implemented by DSP for the avoidance and the minimization of the impact of incidents affecting the security of network and information systems used for the provision of the basic services, aiming to assure their business continuity".

Moreover, the objectives of the NCA across the EU reach further than just the collection of evidence sent by the assessed entities and include the vision to reach a common level of cybersecurity posture. In order to effectively meet this vision, an initial step for NCSA was to conduct an assessment of the current cybersecurity posture of public sectors' main ICT services, using a structured questionnaire. This assessment revealed inconsistencies and major misalignment among different entities [2]. As a result, some additional targets are proposed below:

- Standardization of the collected feedback
- Assignment of a specific level of security, based in the implemented controls per category
- Analysis of the outputs and extraction of relevant statistical information regarding the level achieved per industry, category, and service
- Implementation of comparisons between subsequent assessments, in order to monitor progress
- Extraction of possible correlations or contrasts between the information security posture among stakeholders
- Conduction of further analysis and definition of best practices

The minimum security requirements that OES and DSP have to comply with, have been defined in Decision 1027 published in 3739, B, 08.10.2019 Official Gazette of the Greek Government (Greek Government, 2019). This set of

978-1-7281-7303-0/20/$31.00 ©2020 IEEE
DOI 10.1109/COMPSAC48688.2020.00-20

requirements, covering areas like Risk Management, Access Control, Physical and Environmental Controls etc, is based on a higher-level approach and does not provide any guidance regarding the implementation of these requirements. For example, for the area of physical and environmental security, the requirement is that the installations of data centers and information processing facilities shall be protected against physical or environmental risk through suitable and relevant policies and measures based on a risk management strategy (Greek Government, 2019). This requirement, although mandated by the fact that the relevant entities may have a great diversity in terms of business operation, size, security posture, and technical and organizational capability, is difficult to be monitored effectively by the NCA in order to achieve the objectives mentioned above.

What was needed in order to facilitate the fulfillment of the NCSA's security requirements, especially the measurable ones, was a tool to standardize the possible maturity levels of the organizations. For this purpose a specific assessment framework, the Cybersecurity Maturity Assessment Framework (CMAF), was designed and tested for implementation. The CMAF could help identify the strengths and weaknesses of an organization's processes and examine how compatible these processes are to related identified best practices or guidelines.

The assessment framework consists of the security requirements against which the organization's processes are appraised and the scale, based on which the rating of compliance of the organization's processes is evaluated. Based on the proposed targets mentioned above the assessment framework should incorporate the following characteristics:

- Cover the full extent of the security requirements complying to the NIS Directive obligations
- Be able to be used as a self-assessment tool
- Be able to be used as a basis for an external audit
- Provide clear results regarding the security posture of the organizations
- Be able to be used as a benchmarking tool per industry, type of organization and area of operation
- Be able to be used as a guide for security requirements implementation by the organizations
- Be measurable
- Be easily extractable

2. Related Work

Rea-Guaman et al [3] describe a cybersecurity capability maturity model as a means by which an organisation can assess its current level of maturity of its practices. They provide a comparative study of cybersecurity capability maturity models that builds on a previous review [4]. The research presents an assessment of the differences, advantages and disadvantages of a systematic review of published studies from 2012 to 2017. The method was based on a modified taxonomy of software improvement environments across five categories proposed by Halvorson and Conradi [5]:

1) General: The broad attributes of the improvement environment.
2) Process: Describing how the environment is used.
3) Organisation: The features that articulate the relationship between the organisation and the environment in which it is used.
4) Quality: The indicators used to determine quality in the environment.
5) Result: A statement of the required outcomes, associated costs, and the methods used for evaluation.

Rea-Guaman et al [4] reduce the categories to three, arguing that quality and result do not support the comparison of cybersecurity capability maturity models.

The research considers the Systems Security Engineering Capability Maturity Model (SSE-CMM), Cybersecurity Capability Maturity Model (C2M2) [6], Community Cyber Security Maturity Model (CCSMM) [7], National Initiative for Cybersecurity Education – Capability Maturity Model (NICE) [8].

The analysis concludes that all four models require a degree of customization and that SSE-CMM is the most established of those reviewed. The paper assessed C2M2 as the only model focused on cybersecurity. It went on to state that C2M2 and CCSMM are designed to be implemented in conjunction with the NIST framework and that recent updates to the models had not been identified. It further concluded that only SSE-CMM and C2M2 provided detailed considerations of risk. The research did not present a model to address the issues identified within those reviewed.

Sabillon [9] reviews the best practices and methodologies in cybersecurity assurance and audit and presents the Cyber Security Audit Model (CSAM) for use by organizations and nation-states to validate audit, preventative, forensic and detective controls. CSAM comprises 18 domains, with one limited to nation-states and the remaining 17 applicable to organisations in general. All domains have at least one sub-domain, controls, checklists, sub-controls, and scorecard. The authors compare CSAM to the NIST Cyber Security Framework (CSF) version 1.1 and the Audit First Methodology [10], highlighting the differences. The work describes the CSAM model and states it was tested, implemented and validated in a Canadian higher education institution, although no results are presented, and its efficacy is not evidenced.

The research does not indicate whether CSAM requires specific expertise for its use, or whether self-assessment is feasible. Neither does it present whether the model provides any actionable outcomes following its use.

Akinsanya [11] performed a literature review of cyber security models for healthcare organizations adopting cloud computing. The analysis considers the following:

- Information Security Focus Area Maturity Model (ISFAM) [12]
- Cloud Security Capability Maturity Model (CSCMM)
- UK National Health Service (NHS) National Infrastructure Maturity Model (NIMM) [13]

- Health Information Network (HIN) Capability Maturity Model

The researchers concluded that maturity models provide a compliance model that could not support the complexity of the emerging cyber environment, particularly for healthcare organizations adopting cloud technologies. The conclusions highlight three specific areas of concern and requirements for further work:

- Cyber security maturity models should focus on more than standards compliance.
- Any new measures of maturity introduced should be provided with adequate metrics to make them meaningful.
- The model should be extensible to accommodate the dynamic nature of the cyber security threat landscape.

The research focuses specifically on healthcare and the adoption of cloud computing and does not consider adoption beyond this industry or technology.

Miron and Muita [14] examine cybersecurity maturity models to identify the standards and controls available to providers of Critical National Infrastructures (CNI). The research considers the cyber threats to CNI and the impact of a loss of such services. The authors document nine cybersecurity capability maturity models assessed as applicable to CNI. These are presented based on their applicability to either specific CNI sub-sectors or their general cyber security focus. The review concludes that, of the models considered, none are designed to address the scenario of a CNI operator with a multiplicity of interdependent systems. Instead, the authors propose that the models are described at a high level and focus on CNI or industry sub-sectors and present the need for a model to support municipal governments.

Adler [15] states that capability maturity models are inherently static and diagnostic, in that they identify maturity gaps but are not directly actionable. The research proposes a methodology that follows three stages:

1) Model: Captures the organization's current-state cybersecurity maturity levels, formulates a maturity improvement plan, and identifies influences factors that will shape the organization's cybersecurity posture.
2) Simulate: Produces dynamic simulations of scenarios to determine how particular cybersecurity situations could evolve within the organization, potential interventions, and likely outcomes and impacts.
3) Analyze: Assesses the projected mitigation costs and risk reduction benefits, comparing outcomes across alternate plans and scenarios.

The stages are illustrated through an analysis based upon extension to the Electric Sub-sector Cybersecurity Capability Maturity Model (ES-C2M2) [16]. ES-C2M2 is a lightweight adaptation of the Resilience Maturity Model [17]. This extension describes that the requirement for any process improvement elements within the maturity model should provide explicit guidance for improving performance levels towards a desired end-state.

Le and Hoang in [18] investigate existing cybersecurity maturity models to examine their strengths and weaknesses. They provide a comparison of 12 models mapped against five levels of maturity proposed by Humphrey (1989), concluding that models require relevant quantitative metrics for measurable and actionable assessment. No examples of such metrics are provided.

Almuhammadi and Alsaleh in [19] review the NIST Cyber Security Framework (CSF) for critical infrastructures in order to assess how it can be applied to cybersecurity maturity models and to determine if any gaps exist. The authors propose that one of the key benefits of a cybersecurity capability maturity model is that it provides a structure to allow stakeholders to reach a consensus and set agreed priorities. The authors state that the NIST CSF does not provide organizations with a mechanism to measure the progress of a NIST implementation, or the maturity levels and information security processes' capabilities. They assess that the framework focuses on high-level information security requirements and is applicable for the development of information security programmes and policies. They contrast this to other frameworks such as COBIT, ISO 27001, and the ISF Standard of Good Practice (SoGP) for Information Security. They argue that these focus on information security technical and functional controls, and that they are applicable for developing checklists and conducting compliance/audit assessments. The research proposes an information security maturity model that is able to measure the implementation progress of a security programme over time and assesses the reliability of the IT services that underpin a business. No examples of such measures are provided, and no experimental data is presented.

3. Design of the framework

In order to design the CMAF, a combination of literature review regarding security requirements and a review of existing frameworks (related to cybersecurity or other well-established areas) was conducted. At the time of this review there was only a limited number of established frameworks in the field, although during the past months, some more have been introduced. The literature review regarding security requirements included 16 basic documents. These documents were published by organizations like ENISA, ISO, CIS, European Union, NIST, ISACA and others. The review regarding existing frameworks included frameworks or models from organizations like CMMI, CIS, ENISA, Department of Homeland Security – USA, Citigroup, U.S.Department of Energy and others.

The main aim while designing the CMAF was to be compliant with the scope of the NIS Directive, while following a risk-based approach. Meanwhile, effort was given to integrate scalability, in order to easily adapt to future requirements, to introduce a metric scale, facilitating benchmarking and improvement planning, and finally to integrate

cybersecurity economics aspects, for achieving cost efficiency. Therefore, the proposed framework consists of 20 baseline security requirements, used as a point of reference, and 6 maturity levels, used as a qualitative metric scale.

3.1. Baseline security requirements

The basis of the CMAF and thus the requirements of the framework, are those that have been published under the section "Common Security Policy and Baseline Security Requirements", in Ministerial Decree 1027 - 3739, B, 08.10.2019 Official Gazette of the Greek Government (Greek Government, 2019). These requirements are grouped under 3 main categories:

A. IDENTIFICATION: Requirements that are necessary for the the analysis of the business/operational ecosystem of the organization, the assets that support its essential services and the risks related to the security of network and information systems. These requirements allow the organization to focus its efforts and manage its assets effectively and efficiently.

B. PROTECTION: Requirements that are necessary to protect all assets (people, procedures and technologies) that support the essential services of the organization. The selected controls for this category should take into account the Risk Management Strategy.

C. REACTION: Requirements that are necessary to detect, respond and manage an information security incident that may jeopardize the provision of the essential services of the organization. The selected controls for this category should focus on the minimization of the impact of an information security incident, by ensuring the continuity and the recovery of the essential services to an acceptable and predefined level.

Based on these categories the structure of the framework is further divided into 20 baseline security requirements:

- A. IDENTIFICATION
  Requirement A1: Business Environment
  Requirement A2: Asset Management
  Requirement A3: Risk Assessment
  Requirement A4: Risk Management Strategy
  Requirement A5: Supply Chain Risk Management
  Requirement A6: Self-Assessment – Improvement
- B. PROTECTION
  Requirement B7: Policies, Processes and Procedures for the protection of essential services.
  - Sub-Requirement B7.1: Information Security Policy, Processes and Procedures
  - Sub-Requirement B7.2: Communication and acceptance

  Requirement B8: Identity Management and Access Control
  - Sub-Requirement B8.1: Asset Management
  - Sub-Requirement B8.2: Access control for privileged accounts
  - Sub-Requirement B8.3: Management of equipment for administrative purposes
  - Sub-Requirement B8.4: Access Control
  - Sub-Requirement B8.5: Authentication mechanisms

  Requirement B9: Physical and Environmental security
  Requirement B10: Systems and Applications security
  - Sub-Requirement B10.1: Systems Security
  - Sub-Requirement B10.2: Application Security
  - Sub-Requirement B10.3: Security in Application Development

  Requirement B11: Data Security
  - Sub-Requirement B11.1: Encryption
  - Sub-Requirement B11.2: Data Classification

  Requirement B12: Backups
  Requirement B13: Security Technologies
  - Sub-Requirement B13.1: Traffic filtering
  - Sub-Requirement B13.2: Segregation of systems
  - Sub-Requirement B13.3: Malware protection

  Requirement B14: Systems Testing
  - Sub-Requirement B14.1: Security Assessments
  - Sub-Requirement B14.2: Compliance Checking

  Requirement B15: Change Management
  Requirement B16: Awareness and Training
- C. REACTION
  Requirement C17: Threat Detection
  Requirement C18: Incident Management
  Requirement C19: Business Continuity
  Requirement C20: Disaster Recovery

For each of these requirements the applicable controls have been recognized, analyzed and assigned to the appropriate maturity level, as described in the maturity scale below.

3.2. The maturity scale

After the review of the existing frameworks, it was decided that the CMAF would be based in a 6-levels maturity scale:

- **Maturity Level 5: Efficient - Optimized**
  The organization has implemented methods for the continuous improvement of the implemented controls and the security posture of the organization. A full risk-based approach is followed and a cost-benefit balance is applied. The necessary controls

Figure 1. Maturity level representation: For each level of the maturity scale, a different seal was selected. Each seal represents a series of concentric cycles. The color of each cycle has been selected from the PH scale – red being the lowest and blue being the highest.

are implemented, measured, and controlled at the described level.

- **Maturity Level 4: Effective - Quantitatively Managed**
  The organization has set specific objectives. The objectives (were possible S.M.A.R.T. compliant) are being monitored, measured, analyzed, and evaluated. The necessary controls are implemented, measured and controlled at the described level.
- **Maturity Level 3: Advanced - Defined**
  There is a standardized method regarding the fulfillment of the requirement. The necessary controls are implemented, measured, and controlled at the described level.
- **Maturity Level 2: Basic - Managed**
  There is a concrete plan regarding the fulfillment of the requirement. The necessary controls are implemented but are partially measured and partially controlled.
- **Maturity Level 1: Initial - Reactive**
  The organization has started implementing the requirement, but the extent of the implementation is partial or reactive.
- **Maturity Level 0: Incomplete - Not existing**
  The requirement under examination is not implemented or it is implemented only partially or ad hoc.

For each level of the maturity scale, a different seal was selected. Each seal represents a series of concentric cycles. The lowest possible score is represented by a one cycle seal and the highest by a six cycle seal. The color of each cycle has been selected from the PH scale – red being the lowest and blue the highest (Figure 1).

4. Framework validation

Since the framework was primarily based on literature review, it was decided that, before its release, it should be validated through an implementation pilot project. The pilot project should include organizations from different sectors, of different sizes and with different security postures. To achieve this, the following diverse pilots were selected for validation purposes:

- A mid-sized OES from the healthcare sector, that is expected to have a low level of maturity
- A mid-sized OES from the Digital Infrastructures sector, that is expected to have a medium level of maturity
- A large-sized OES from the air-transport sector, that is expected to have a high level of maturity

The pilot assessments were carried out by a team of experts consisting of: One expert, already involved in the development of the CMAF with a deep knowledge of the framework itself and with high auditing skills on security controls, and two experts from the NCSA, tasked with the monitoring of the framework implementation process and the review of the related outcomes.

The assessments were carried out via the following methods: Table-top assessments, interviews, and on-site visits. In Figure 2 the graphical representation of the assessment result of a fictitious organization, that is produced from the CMAF implementation, is presented.

The results of the assessments and the proposed improvements during the pilot project were gathered, analyzed, and incorporated in the final version of the model. Following that, an evaluation of the pilot project revealed that the CMAF was initially able to demonstrate: A holistic higher-level overview of cybersecurity, compatibility with industry-specific security controls, adaptability to diverse and complex environments, industry neutrality and ease of application.

5. Discussion

The National Competent Authorities for cybersecurity, especially those who need to comply with the NIS Directive, could use the proposed maturity assessment framework in order to request from the applicable organizations the implementation of self-assessments based on the framework and collect the results. The authorities can review the collected responses, analyze the data, and produce valuable conclusions. Also, comments regarding possible improvements can be collected from the applicable organizations as well as from the dedicated staff dealing with the assessment of the results.

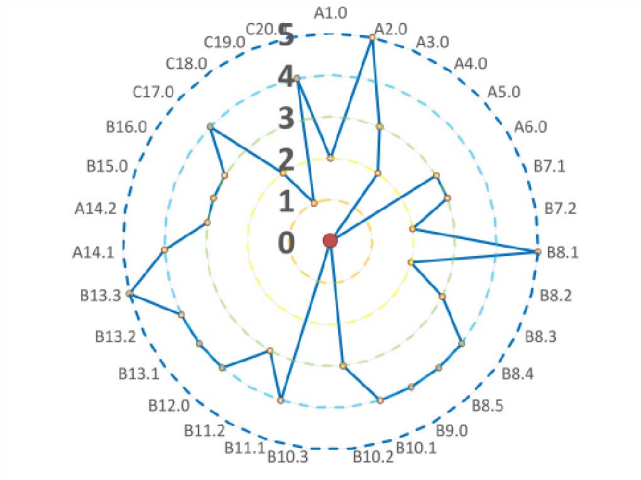

Figure 2. Graphical representation of the cybersecurity maturity assessment result per requirement

An extended version of the CMAF could integrate other industry-specific models or incorporate specific requirements, such as for cloud services and OT/ IoT environments. Based on the findings from the cybersecurity assessments, additional cyber security controls may be introduced related to legal, technical, organizational, capacity building, and cooperation aspects.

6. Conclusions

As Critical National Infrastructures are becoming more vulnerable to cyber attacks, their protection becomes a significant issue for any organization, as well as a nation-state. Cybersecurity for CNI essential services often follows a lifecycle model of identification, protection, detection, and reaction. Moreover, an assessment is an activity that helps identify the strengths and weaknesses of an organization's processes and examine how closely these processes relate to identified best practices and guidelines. In order to help in the evaluation of the cybersecurity posture of CNI, a novel cybersecurity maturity assessment framework, the CMAF, is presented in this paper. The proposed framework consists of 20 security requirements, 6 maturity levels and can be used both as a self-assessment tool and as an external audit tool. Furthermore, it facilitates organizations to perform a gap analysis and receive a graphical representation of their security posture. Information collected from the framework can be used from National Competent Authorities, after proper aggregation and anonymization processes, in order to identify common security gaps and thereafter to prioritize future security programmes and funding initiatives on a national or European level.

Acknowledgments

We thankfully acknowledge the support of the CONCORDIA H2020 (GA no. 830927) EU project and the support of the NCSC, UK funded project (RFA: 20058).

References

[1] L. Maglaras, G. Drivas, K. Noou, and S. Rallis, "Nis directive: The case of greece," *EAI Endorsed Transactions on Security and Safety*, vol. 4, no. 14, 2018.

[2] G. Drivas, L. Maglaras, H. Janicke, and S. Ioannidis, "Cybersecurity assessment of the public sector in greece," in *ECCWS 2019 18th European Conference on Cyber Warfare and Security*. Academic Conferences and publishing limited, 2019, p. 162.

[3] A. M. Rea-Guamán, I. Sánchez-García, T. San Feliu, and J. Calvo-Manzano, "Maturity models in cybersecurity: A systematic review," in *2017 12th Iberian conference on information systems and technologies (CISTI)*. IEEE, 2017, pp. 1–6.

[4] A. M. Rea-Guaman, T. San Feliu, J. A. Calvo-Manzano, and I. D. Sanchez-Garcia, "Comparative study of cybersecurity capability maturity models," in *International Conference on Software Process Improvement and Capability Determination*. Springer, 2017, pp. 100–113.

[5] C. P. Halvorsen and R. Conradi, "A taxonomy to compare spi frameworks," in *European Workshop on Software Process Technology*. Springer, 2001, pp. 217–235.

[6] J. D. Christopher, D. Gonzalez, D. W. White, J. Stevens, J. Grundman, N. Mehravari, and T. Dolan, "Cybersecurity capability maturity model (c2m2)," *Department of Homeland Security*, pp. 1–76, 2014.

[7] G. B. White, "The community cyber security maturity model," in *2011 IEEE international conference on technologies for homeland security (HST)*. IEEE, 2011, pp. 173–178.

[8] P. Curtis, N. Mehravari, and J. Stevens, "Cybersecurity capability maturity model for information technology services (c2m2 for it services), version 1.0," CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States, Tech. Rep., 2015.

[9] 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 *2017 International Conference on Information Systems and Computer Science (INCISCOS)*. IEEE, 2017, pp. 253–259.

[10] S. Donaldson, S. Siegel, C. K. Williams, and A. Aslam, *Enterprise cybersecurity: how to build a successful cyberdefense program against advanced threats*. Apress, 2015.

[11] O. O. Akinsanya, M. Papadaki, and L. Sun, "Current cybersecurity maturity models: How effective in healthcare cloud?" in *CERC*, 2019, pp. 211–222.

[12] M. Van Steenbergen, R. Bos, S. Brinkkemper, I. Van De Weerd, and W. Bekkers, "The design of focus area maturity models," in *International Conference on Design Science Research in Information Systems*. Springer, 2010, pp. 317–332.

[13] A. Savidas, "Your guide to the nhs infrastructure maturity model," *Informatics Directorate, Policy and Planning*, 2009.

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

[15] R. M. Adler, "A dynamic capability maturity model for improving cyber security," in *2013 IEEE International Conference on Technologies for Homeland Security (HST)*. IEEE, 2013, pp. 230–235.

[16] J. Stevens, "Electricity subsector cybersecurity capability maturity model (es-c2m2)(case study)," CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, Tech. Rep., 2014.

[17] R. A. Caralli, J. H. Allen, and D. W. White, *CERT resilience management model: A maturity model for managing operational resilience*. Addison-Wesley Professional, 2010.

[18] N. T. Le and D. B. Hoang, "Can maturity models support cyber security?" in *2016 IEEE 35th international performance computing and communications conference (IPCCC)*. IEEE, 2016, pp. 1–7.

[19] S. Almuhammadi and M. Alsaleh, "Information security maturity model for nist cyber security framework," *Computer Science & Information Technology (CS & IT)*, vol. 7, no. 3, pp. 51–62, 2017.