International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Cybersecurity Maturity Assessment of Information Systems for Yemen Telecoms

Abdulkarem Yahya Abohatem [1,*], Fadl Mutaher Ba-Alwi [2]

Submitted: 03/10/2023 **Revised**: 25/11/2023 **Accepted**: 08/12/2023

Abstract: With the use of several standards, this study seeks to ascertain Yemen Telecoms' level of maturity and assess the efficacy of information systems protection. Specialist information and recurring technical reports were used to gather the data, which was then compared to the international standard required to determine the maturity level. Strong cybersecurity procedures must be in place since cybersecurity threats are becoming more frequent and complicated. Although Yemen Telecoms has put in place a number of cybersecurity measures, our analysis shows that its information system protection rules and procedures still have holes. Choosing the best cybersecurity framework will also be aided by the study. In order to effectively defend Yemen Telecoms against cyber threats, we offer suggestions for bolstering the cybersecurity information systems.

Keywords: *Yemen Telecoms, Information Systems, cybersecurity maturity, Maturity assessments, and Security measures.*

1. Introduction

Cybersecurity maturity models are frameworks that provide organizations with a structured approach to assess and improve their cybersecurity capabilities. These models offer a roadmap for organizations to gauge their current cybersecurity posture, identify areas for improvement, and establish a path toward enhanced cybersecurity maturity. In today's digital landscape, where threats and attacks are becoming increasingly sophisticated, organizations must comprehensively understand their cybersecurity strengths and weaknesses. Cybersecurity maturity models enable organizations to evaluate their readiness to effectively prevent, detect, and respond to cyber threats.

Maturity models typically consist of multiple levels or stages that depict different levels of cybersecurity maturity. These levels often range from an initial or ad hoc stage to a fully optimized and proactive stage. The number of levels may vary depending on the specific model being used, but they generally represent a progression from a foundational state to a more advanced and mature cybersecurity posture. The levels within a cybersecurity maturity model are typically defined based on various factors, such as the organization's cybersecurity policies, procedures, technical controls, risk management practices, incident response capabilities, and overall cybersecurity culture. Each level represents a set of characteristics or capabilities that organizations should strive to achieve as they progress toward higher maturity.

[1] *Sana'a University, Yemen*
ORCID ID: 000-0002-8993-4613
** Corresponding Author Email: Abdulkareem.abohatem@ptc.gov.ye*
[2] *Sana'a University, Yemen*
Dr.fadlbaalwi@gmail.com,
[1,2] *Information System Department, Faculty of Computer and Information Technology*

2. Importance Study of Assessing Cybersecurity Maturity

Emphasize the importance of measuring the adequacy of protection as an indicator of an organization's cybersecurity awareness in various business processes, particularly in the field of information and communication technologies (ICT).

They argue that appropriate security standards are necessary to determine the required level of cybersecurity maturity for information protection. [20] The primary objective of this

paper is to emphasize the importance of implementing IT best practices, such as COBIT, ITIL, and ISO/IEC 27002, within organizations operating in IT environments. The authors argue that these best practices should be aligned with business requirements, integrated with internal procedures, and mapped onto the COBIT framework. This approach allows organizations to establish a comprehensive and harmonized IT governance framework, improving operational efficiency and mitigating IT-related risks Based on the above, it is evident that the importance of evaluation can be summarized in the following points: • Telecom companies hold vast amounts of sensitive customer data and manage critical infrastructure. As such, they are high-value targets for cyber-attacks. Evaluating maturity helps strengthen defenses. • Yemen Telecoms operates in a region that experiences political instability and conflict. This environment attracts state-sponsored hacking groups. Maturity assessments mitigate risks from sophisticated actors. • As telecom networks become more software-defined and software apps take centralized control, traditional perimeter-based

security is insufficient. Maturity models evaluate adoption of modern security DevOps practices. • Regulators in many countries mandate adherence to baseline security standards.

Maturity assessments allow Yemen Telecoms to benchmark compliance and manage regulatory/audit risks. • Customers expect assurances about how their personal data and privacy are protected. Demonstrating maturity through assessments boosts brand trust and loyalty. • Security breaches can result in revenue loss from subscriber churn, fines and litigation.

Maturity evaluations minimize financial fallout by strengthening

controls proactively. • With growing digital transformation, security best practices must continuously improve. Maturity models provide a framework to institutionalize ongoing enhancement. • Understanding maturity gaps facilitates prioritized risk remediation. This optimal allocation of security resources enhances the overall protection of Yemen Telecoms' digital assets and infrastructure.

3. Literature Reviews

This literature review aims to analyze existing cybersecurity maturity models and frameworks to identify trends, contributions,

limitations, and opportunities for future work. An understanding of previous approaches can inform the development of more comprehensive and customized solutions tailored to evolving needs. [1] the emergence of disruptive technologies like Social, Mobile, Analytics, and Cloud (SMAC) and the Internet of Things (IoT) has revolutionized the information technology sector. However, it has also led to an increase in cybersecurity threats to digital infrastructure. Bashofi and Salman (2022) highlight that as organizations heavily rely on information technology, the risk of security breaches and cybercrime also escalates. To address this, organizations must adopt appropriate security standards and understand them cybersecurity maturity. [2] note that cybersecurity is growing exponentially in both the public and private sectors. However, this growth brings new and dynamic cyber threats, potentially hindering the performance of industries. To mitigate this, organizations need to update their cybersecurity measures and gauge their cybersecurity preparedness using maturity models. emphasize the significance of cybersecurity in organizations and the need for comprehensive training to manage different forms of cyberattacks. Evaluating an organization's security maturity level plays a crucial role in providing cybersecurity. [3] This paper introduces an Information Security Management (ISM) model that serves as a framework for assessing an organization's security level. The authors establish a correlation between maturity levels and security levels within the organization. Moreover, the proposed model incorporates process capability controls that have an impact on both levels. The primary objective of the model is to assist organizations in addressing cybersecurity gaps. These gaps encompass various aspects such as talent, technology, organizational units, financial resources, management, and operations. By utilizing the proposed model, organizations can effectively identify and bridge these gaps. This, in turn, enables cybersecurity auditors to develop a comprehensive plan for assessing the organization's security level. The plan facilitates the management and enhancement of automated countermeasures within the organization and helps in the application of suitable standards and frameworks that align with the organization's daily operations. Cybersecurity auditors utilize cybersecurity techniques and tools to evaluate the organization's security posture. They can employ the proposed security model in conjunction with established standards, tools, and techniques. The model enables the assignment of the organization to an appropriate security maturity level based on the automated controls. The resources and requirements process serves as an indicator of the organization's security level within the model. Based on the organization's security maturity level, cybersecurity auditors can generate reports for the organization and provide recommendations to elevate its security levels. By adapting the proposed model from the ISM3 model and aligning it with maturity levels, the model effectively addresses cybersecurity gaps and supports organizations in enhancing their overall security posture. [4] point out that existing cybersecurity vulnerability assessment tools are built based on guidelines from organizations such as the U.S. Department of Energy and the National Institute of Standards and Technology (NIST). While frameworks like the Cybersecurity Capability Maturity Model (C2M2) and the NIST Cybersecurity Framework (CSF) help determine cybersecurity maturity, they don't prioritize mitigating vulnerabilities [5] suggests that structured requirements and metrics for different levels of maturity and capability are essential to assess the level of cybersecurity readiness.[7] This paper introduces a capability maturity framework called CYBERGOV, designed to assess and enhance cybersecurity governance in organizations. The framework offers a structured approach for measuring the maturity of cybersecurity governance practices within an organization. It provides a comprehensive assessment, identifies strengths and areas for improvement, and has been implemented and validated in a medium-sized organization.

The findings suggest that the CYBERGOV framework has the potential to support organizations of various sizes and sectors in improving their cybersecurity governance. [9] The study focuses on evaluating the accuracy of security managers in assessing the maturity of security controls. To assess the quality of maturity assessments, a case study was conducted, involving security experts who evaluated a subset of ISO/IEC 27002 security controls against COBIT

maturity levels within a hypothetical scenario. [10] This article introduces a network-based model specifically designed for cybersecurity assessment in UK higher education institutions. The model provides a holistic framework for evaluating the cybersecurity maturity of these institutions, encompassing relevant security and privacy regulations and best practices. It serves as both a self-assessment tool and a cybersecurity audit tool, with 15 security categories and six maturity levels. The model is implemented on an online platform, offering a user-friendly interface for self-assessments, gap analysis, compliance reports, and visualization of security conditions. [12] The Cybersecurity Focus Area Maturity (CYSFAM) Model is suggested by this study as a means of evaluating cybersecurity competencies. A major financial institution examined CYSFAM for this design science study.

There are numerous cybersecurity standards, but 11 broad focus areas were chosen. A tool for evaluation was created. The comprehensive single case study shows how and to what degree cybersecurity-related flaws might be found. Although the new scoring metric has been shown to be sufficient, it still has room for improvement. [14] The review brings attention to a crucial insight regarding the limitations of existing cyber security maturity models in effectively evaluating security in healthcare organizations that utilize cloud computing. [15] The primary objective of this article is to perform a thorough examination of existing cybersecurity capability maturity models through a systematic review of published articles from 2011 to 2019. The review incorporates a comparative study based on Halverson and Conradi's taxonomy. [17] This excerpt highlights the trend of combining multiple standards, specifically ISO 27001 (information security management) and ISO 22301 (business continuity), to streamline the risk assessment process. The integration of these standards allows organizations to take a holistic approach to managing risks related to information security and business continuity, resulting in improved efficiency, a unified framework for risk assessment, and enhanced overall resilience. [18] In this excerpt, the objective is to evaluate the cybersecurity maturity within the Workforce Management domain of Bank Indonesia. The assessment is conducted using the C2M2 Framework, revealing that the cybersecurity maturity level in this domain has not reached MIL3. The findings suggest that there is room for improvement in processes, policies, and training programs to enhance the organization's workforce's knowledge and awareness of cybersecurity best practices. [21] This research paper emphasizes the use of ISO/IEC 27005:2018 as a guidance document for conducting risk assessments. It also mentions the implementation of ISO/IEC 27002:2013 as a code of practice for information security controls. The Cyber Security Maturity Model (CSMM) version 1.10 is utilized to evaluate the organization's cybersecurity maturity. The results show an improvement in cybersecurity maturity after implementing additional security controls. [22] This research analyzes three prominent cybersecurity standards (NIST, CIS Controls v8, and ISO27002) to develop a cybersecurity maturity framework for ICT management. The integration of key concepts from these standards into 21 cybersecurity categories forms a comprehensive set of guidelines for managing and improving ICT security. The proposed framework aims to enhance cybersecurity maturity and strengthen ICT management practices. [23] The study compares the adequacy and selection criteria of NIST and ISO 27001 cybersecurity frameworks. It highlights the significance of risk maturity level, cost, and certification in implementing a cybersecurity framework. The NIST Cybersecurity Framework (CSF) emphasizes organizational structure and risk management, while ISO 27001 focuses on establishing and maintaining effective Information Security Management Systems (ISMS).

4. Methodology

The report offers a framework for assessing how mature an organization's information security and technology are. Utilizing cybersecurity standards from well-known frameworks like PCI-DSS, NIST, CIS, and COBIT, this evaluation is carried out. The researchers suggest that a useful indicator of the maturity of technology and information security is PCI-DSS, a widely accepted standard for protecting credit card data. Organizations can evaluate their degree of compliance and preparedness for protecting sensitive data by aligning with PCI-DSS requirements. [11] A Cybersecurity Maturity Assessment Framework (SCMAF) is suggested in this research for Saudi Arabian Higher Education Institutions (HEIs). A thorough security maturity assessment framework that complies with national and international security criteria is called SCMAF. It provides an organization with a way to evaluate themselves to establish their security levels, identify weaknesses, and develop mitigation plans. The framework uses different levels of maturity to measure the security performance of each organization, and it can be implemented as a lightweight assessment tool provided online or offline. The assessment results are communicated to the organization using visual score charts and an evaluation report. [13] We have developed a comprehensive framework and software program called CyFEr (Cybersecurity Vulnerability Mitigation Framework through Empirical Paradigm) in answer to the challenge. This article describes the advanced prioritized gap analysis (EPGA) technique developed by CyFEr and how it is implemented in the CSF (Cybersecurity Framework). We verify this framework's efficacy by contrasting it with other models and testing it using cyber injects taken from a real cyberattack targeting the industrial control systems (ICS) of critical infrastructures. [19] In businesses that have adopted

an Information Security Management System (ISMS) based on ISO 27001:2013, this article offers a workable approach for doing information security maturity assessments. The technique integrates recommendations from ISO 27002:2013 and uses a COBIT 5-comparable approach. The assessment's conclusions include measurements and suggestions for strengthening the ISMS and raising the standard of information security risk management procedures in general. This study employed a mixed-methods approach to its research, combining interviews and surveys. semi-structured interviews with cybersecurity specialists to obtain qualitative data and a survey to acquire quantitative data from a sample of information systems. While the interviews shed light on how well the security measures are working to mitigate weaknesses, the survey evaluates the ones that are already in place. IOS standers techniques are used for the data analysis. a study of the literature examining the techniques applied in information systems audits for cybersecurity. To find pertinent papers, the study conducts a thorough search across databases like IEEE Explore, ACM Digital Library, and Scopus. The techniques employed in cybersecurity information systems audits are then determined by performing a theme analysis on the selected articles.

4.1. Using a Cybersecurity Maturity Model

1) Assess their current cybersecurity posture: Maturity models provide a structured framework for organizations to assess their cybersecurity strengths and weaknesses across different domains.

2) Identify areas for improvement: By evaluating them maturity level within each domain, organizations can pinpoint specific areas that require attention and improvement.

4.2. Importance of Cybersecurity Maturity Models

• Benchmarking: By comparing an organization's present cybersecurity procedures and capabilities to industry best practices, they offer a baseline for evaluating the maturity level of those practices and capabilities.

• Prioritization: Maturity models identify gaps at different maturity levels, which aids in the prioritization of security investments and upgrades. This guarantees that resources are allocated to areas with greater impact initially.

This study's contribution to our understanding of cybersecurity in information systems makes it significant. Effective cybersecurity measures are now more important than ever as firms rely more and more on information technology. This analysis sheds light on the weaknesses in these systems and how well the security mechanisms in place now address those weaknesses.

The results of this study can help firms create better cybersecurity policies and procedures, which will ultimately improve the security of information systems. and be aware of the degree of maturity to assist in creating the cybersecurity framework for any IS company.

5. Mapping Control Maturity of Cybersecurity Standards Objectives

Maturity of cybersecurity standards and frameworks that make use of this type of include: 1-NIST Cybersecurity Framework (CSF) - The Framework Core categorizes cybersecurity activities around the functions of Identify, Protect, Detect, Respond, Recover which maps to the objectives. 2-ISO/IEC 27001 - The control objectives and controls specified in Annex A of the standard are organized by confidentiality, integrity and availability. 3-COBIT (Control Objectives for Information and Related Technologies) - The control objectives reference categories that relate to preventative, detective and corrective controls. 4-NIST SP 800-53 Revision 5 - Security and Privacy Controls for Federal Information Systems and Organizations. Controls are mapped to families which align to security goals. 5-CSA CCM (Critical Security Controls) - The 20 CIS controls refer to categories like deterrent, preventative, detective and responsive. 6-PCI DSS (Payment Card Industry Data Security Standard) - Requirements can be viewed through the lens

of people, processes and technologies protecting cardholder data. So in summary, the major international and U.S. federal cybersecurity standards and frameworks commonly utilize this objective/control type relationship to help organizations implement comprehensive cyber defenses and assess risk and compliance status. It provides a structure for control selection, assessment and continuous monitoring practices. Here is an updated table 1 that includes different controls from

various standards (COBIT, ISO 27001, PCI DSS, NIST, CSA),

along with their primary objectives and the types of controls

associated with each objective:

The table 1 provided includes a selection of controls from each standard and their corresponding control identifiers. The primary objectives and control types mentioned are generalizations and may vary depending on the specific requirements and implementation within each standard. It is important to refer to the specific standards for detailed control descriptions and mappings.

6. Result of Evaluated the Cybersecurity Maturity Level

This framework offers a thorough method for handling risk related to information security. It contains a set of best practices and controls for handling information security,

including as protocols for incident handling, access control, and risk assessment. The framework is widely accepted around the world and frequently serves as a standard for information security management. For the purpose of identifying essential processes and prioritizing their recovery, conduct periodic business impact assessments. To reduce downtime, put backup and recovery procedures in place for important systems and data. To verify the efficacy of the business continuity strategy, test and exercise it frequently. Provide explicit routes for communication and escalation protocols in the case of a business continuity event. Employees should receive programs and training explaining their roles and duties in the case of a business continuity event.

Work together with important stakeholders and outside partners to make sure synchronized efforts for recovery and reaction. Maintain a constant eye on business continuity procedures, assess their efficacy, and adjust them as necessary.

7. Maturity of Cybersecurity Standards and Frameworks

Maturity of cybersecurity standards and frameworks that make use of this type of include: 1-NIST Cybersecurity Framework (CSF) - The Framework Core categorizes cybersecurity activities around the functions of Identifying, Protecting, Detecting, Responding, Recover which maps to the objectives. 2- ISO/IEC 27001 - The control objectives and controls specified in Annex A of the standard are organized by confidentiality, integrity, and availability. 3-COBIT (Control Objectives for Information and Related Technologies) - The control objectives reference categories that relate to preventative, detective, and corrective controls. 4-NIST SP 800-53 Revision 5 – Security and Privacy Controls for Federal Information Systems and Organizations. Controls are mapped to families that align with security goals. 5-CSA CCM (Critical Security Controls) – The 20 CIS controls refer to categories like deterrent, preventative, detective, and responsive. 6-PCI DSS (Payment Card Industry Data Security Standard) - Requirements can be viewed through the lens of people, processes, and technologies protecting cardholder data. So in summary, the major international and U.S. federal cybersecurity standards and frameworks commonly utilize this objective/control type relationship to help organizations implement comprehensive cyber defenses and assess risk and compliance status. It provides a structure for control selection, assessment, and continuous monitoring practices.

Here is an updated table 1 that includes different controls from

various standards (COBIT, ISO 27001, PCI DSS, NIST, CSA), along with their primary objectives and the types of controls associated with each objective:

Table 1. Types standards of controls

Control	COBIT	ISO 27001	PCI DSS	NIST	CSA	Type	Primary Objective
Information security policies	APO01.01	A.5.1	12.1	PR.IP-1	CC6.1	Prevent	Confidentiality
Organization of information security	APO01.02	A.6.1	12.2	PR.IP-2	CC6.2	Prevent	Confidentiality
Human Resources Security	APO07.01	A.7.1	12.3	PR.AC-1	CC6.3	Prevent	Confidentiality
Asset Management	APO07.02	A.8.1	12.4	PR.AC-2	CC6.4	Prevent	Confidentiality
Access Control	DSS05.01	A.9.2	7.1	PR.AC-3	CC6.5	Prevent	Confidentiality
Cryptography	DSS04.02	A.10.1	3.6	PR.AC-4	CC6.6	Prevent	Confidentiality
Physical and Environmental Security	DSS02.01	A.11.1	9.1	PR.PT-1	CC6.7	Prevent	Confidentiality
Operations Security	DSS06.01	A.12.1	9.2	PR.PT-2	CC6.8	Prevent	Confidentiality
Communications Security	DSS06.02	A.13.1	10.8	PR.PT-3	CC6.9	Prevent	Confidentiality
System acquisition, development, and maintenance	BAI05.04	A.14.1	6.3	PR.DEF-1	CC6.10	Prevent	Confidentiality
Supplier relationships	DSS05.04	A.15.1	12.8	PR.SUP-1	CC6.11	Prevent	Confidentiality
Information security incident management	DSS06.03	A.16.1	10.8	PR.IP-3	CC6.12	Detect	Integrity
Information security aspects of business continuity management	DSS07.01	A.17.1	9.9	PR.MA-1	CC6.13	React	Availability
Compliance	APO12.01	A.18.1	12.11	PR.MA-2	CC6.14	Prevent	Confidentiality

8. Data collection

The Target Score for each control can be determined by referencing the ISO 27001 standard or other relevant standards and best practices. The Policy Score and Practice Score for each control can be determined by assessing the organization's current practices and processes. It is important to note that there is no one-size-fits-all approach to collecting data for the table 2. The best approach will vary depending on the size and complexity of the organization, as well as the resources that are available. collecting data for the table 2:

7.1 Start with the most important controls. The organization should focus on collecting data for the controls that are most important to the organization and its stakeholders.

7.2 Use a variety of methods. The organization should use a variety of data collection methods to get a complete picture of its

current maturity level.

7.3 Involve key personnel. The organization should involve key personnel from all levels of the organization in the data collection process.

7.4 Be objective. The organization should be objective when assessing its current maturity level.

7.5 Update the table 2 regularly. The organization should update the table 2 regularly to reflect changes in its maturity level.

Table 2. Result Of Maturity Between Different Standards

	Control	Target Score	Policy Score	Practice Score
1	Information security policies	3	3	4
2	Organization of information security	3	1.7	3.5
3	Human Resources Security	3	2.5	4
4	Asset Management	3	2.7	3
5	Access Control	3	2.1	3
6	Cryptography	3	2.5	2.5
7	Physical and Environmental Security	3	3	3
8	Operations security	3	3	3.5
9	Communications security	3	2.5	4
10	System acquisition, development and maintenance	3	2.5	3
11	Supplier relationships	3	3	2
12	Information security incident management	3	2.8	2.5
13	Information security aspects of business continuity management	3	2	2
14	Compliance	3	3	3
The average level				3.22

9. Results of Maturity Between Different Standards

The standards or other pertinent standards and best practices can be used to determine the Target Score for each control. Examining the organization's present procedures and practices will yield the Policy Score and Practice Score for each control. It is crucial to remember that there isn't a single, universal method for gathering information for Table 2. The optimal strategy will change based on the organization's size, complexity, and available resources. See Fig 1.

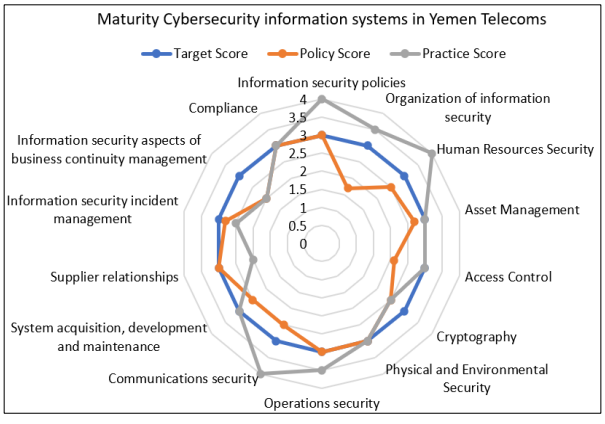

Fig 1. Maturity of YT

10. The Gaps of Cybersecurity Maturity

The provided table 2 of section control scores can be used to identify security maturity gaps within an organization. Security maturity gaps refer to the disparities between the desired target scores and the actual policy and practice scores. These gaps highlight areas where the organization may need to focus on improving its security posture and enhancing its adherence to the standards. Organization of information security: There is a significant gap between the policy score (1.7) and the practice score (3.5). This indicates that although the organization has defined policies for organizing information security, there is a need for better implementation and execution of these policies. The organization should focus on bridging this gap by aligning its practices with the established policies. Access Control: The policy score (2.1) is lower than the target score (3), indicating that the organization's access control policies may not fully meet the desired level. To improve security maturity in this area, the organization should review and strengthen its access control policies, ensuring they align with industry best practices and regulatory requirements. Cryptography: Both the policy score (2.5) and the practice score (2.5) fall below the target score (3). This suggests that the organization's cryptography policies and practices may need improvement. Enhancing cryptographic controls, such as encryption algorithms, key management, and secure protocols, can help address this security maturity gap. System acquisition, development, and maintenance: The practice score (3) is lower than the target score (3), indicating that the organization may need to enhance its practices related to system acquisition, development, and maintenance. This could involve implementing secure coding practices, conducting thorough security assessments during system development, and ensuring robust change management processes. Supplier relationships: The practice score (2) falls below the target score (3), indicating that the organization needs to improve its practices concerning managing supplier relationships. Strengthening supplier due diligence, vendor risk assessment, and contractual agreements can help address this security maturity gap. Information security incident management: Both the policy score (2.8) and the practice score (2.5) are below the target score (3). This suggests that the organization may need to enhance its incident management policies and practices. Improving incident response planning, establishing clear escalation procedures, and conducting regular incident drills can help bridge this security maturity gap. These identified security maturity gaps present opportunities for the organization to focus its efforts and resources on improving specific areas of information security. By addressing

these gaps, the organization can enhance its security posture, mitigate risks, and align more closely with the requirements of the standards. It is important for the organization to prioritize these areas and develop action plans to bridge the identified gaps effectively.

11. The Finding

Based on the provided table 2 section control scores, the following findings can be observed: Information security

policies: The organization has well-defined policies and effective practices in place for information security policies. Organization of information security: There is a gap between the policy score and the practice score, indicating a need for better implementation of policies related to organizing information security. Human Resources Security: The organization has well-defined policies and effective practices in place for human resources security. Asset Management: While policies for asset management are defined, there may be room for improvement in effectively implementing these practices. Access Control: There is a slight gap between the policy score and the practice score, suggesting the need for better implementation of access control practices. Cryptography: The organization has defined policies and practices for cryptography, but there may be room for improvement in both areas. Physical and

Environmental Security: The organization has well-defined policies and practices for physical and environmental security. Operations security: The organization has well-defined policies and practices for operations security. Communications security: The organization has well-defined policies and effective practices for communications security. System acquisition, development, and maintenance: While policies for system acquisition, development, and maintenance are defined, there may be room for improvement in effectively implementing these practices. Supplier relationships: The organization has well-defined policies for managing supplier relationships, but there may be room for improvement in effectively implementing these practices. Information security incident management: There may be room for improvement in effectively implementing policies and practices related to information security incident management. Information security aspects of business continuity management: There may be room for improvement in effectively implementing policies and practices related to information security aspects of business continuity management. Compliance: The organization has well-defined policies and practices for compliance This average value

serves as an indicator of the overall cybersecurity maturity of the organization. A score of 3.22 suggests a moderate level of maturity, implying that the organization has made progress in implementing cybersecurity practices and policies across various domains. However, the findings also reveal areas where the organization can further improve its cybersecurity posture. For controls where the practice scores are lower than the policy scores,

improvement to bridge the divide between policy and practice.

12. Analysis the Results and Recommendations

Maturity is a crucial aspect for organizations, especially in the telecommunications industry, where technology plays a central role in operations and service delivery. This report aims to analyze the maturity of IT within Yemen Telecoms, a leading telecommunications company in Yemen, and provide recommendations for improvement. Yemen Telecoms operates in a highly competitive market, where efficient and effective IT infrastructure is essential for delivering reliable services, enhancing customer experience, and staying ahead of the competition. Assessing the maturity of IT systems and processes is vital to identify strengths, weaknesses, and areas for enhancement within the organization's IT ecosystem. This analysis will involve evaluating various dimensions of IT maturity, including infrastructure, applications, data management, IT governance, security, and digital transformation initiatives. By examining these areas, we can gain insights into the current state of IT maturity within Yemen Telecoms and identify areas that require attention and improvement.

Table 3. Analysis the results and recommendations

Analysis of Results	**Recommendations**
The organization has well-defined and effectively implemented information security policies and practices.	1. Regularly review and update information security policies. 2. Conduct awareness programs on policies and their importance. 3. Ensure policies are easily accessible to all employees.
There is a gap between the organization's policies and their implementation, indicating a need for improvement in practice.	1. Establish clear responsibilities and accountabilities for implementing policies. 2. Provide training and resources to employees for effective implementation. 3. Conduct regular audits to assess compliance.
The organization has strong human resources security policies and practices in place.	1. Develop a comprehensive employee onboarding and off boarding process. 2. Conduct regular security awareness training for employees. 3. Implement background checks and access control for employees.
The organization's asset management practices need impro to align with established policies.	1. Implement a centralized asset inventory system. 2. Define roles and responsibilities for asset management. 3. Regularly update and monitor asset configurations and vulnerabilities.
There is a significant gap between the organization's acces policies and their implementation.	1. Conduct access control reviews and audits regularly. 2. Implement multi-factor authentication for critical systems. 3. Enforce the principle of least privilege for user access.
Both policies and practices related to cryptography need improvement to meet the desired target.	1. Implement industry-standard encryption algorithms and protocols. 2. Establish secure key management practices. 3. Conduct regular cryptographic controls audits and assessments.
The organization has robust physical and environmental security measures in place.	1. Implement access control mechanisms for physical premises. 2. Conduct regular physical security assessments. 3. Implement surveillance and monitoring systems.
The organization demonstrates strong operations security policies and practices.	1. Implement change management procedures for systems and applications. 2. Regularly update and patch systems to address vulnerabilities. 3. Conduct regular security awareness programs for employees.
The organization excels in communications security, surpassing the target score.	1. Ensure secure transmission protocols are used for data transfer. 2. Implement strong email and web filtering mechanisms. 3. Regularly update and patch communication systems.
There is a gap between the organization's policies and practices regarding system acquisition, development, and maintenance.	1. Implement secure coding practices and conduct regular code reviews. 2. Establish change management procedures for system updates and patches. 3. Perform regular security testing and vulnerability assessments.
The organization needs to improve its supplier relationship practices to align with established policies.	1. Establish a vendor risk management program. 2. Conduct thorough security assessments of third-party suppliers. 3. Clearly define information security requirements in supplier contracts.
The organization has policies and practices in place for incident management, but improvements are needed.	1. Develop and test an incident response plan. 2. Establish clear roles and responsibilities for incident response. 3. Conduct regular incident response drills and simulations.
The organization's policies and practices related to business continuity management are effective, with slight room for improvement.	Regularly review and update the business continuity plan to ensure its effectiveness in addressing potential disruptions.

13. Conclusions

This study assessed the efficacy of cybersecurity measures by using existing criteria to determine the maturity level of those measures in Yemen Telecoms' information systems. According to the report, Yemen Telecoms has put in place some cybersecurity safeguards, but its information system protection rules and processes still have gaps. Given the growing frequency and complexity of cybersecurity threats, the study emphasizes how important it is to have strong cybersecurity safeguards in place. Several recommendations have been made to improve the maturity of cybersecurity measures in Yemen Telecoms' information systems based on the assessment. These suggestions include deciding on a suitable cybersecurity structure, carrying out frequent security evaluations, and putting in place thorough staff training initiatives. Yemen Telecoms can strengthen the defense of its information networks against cyberattacks by putting these precautions into practice.

References

[1] D. P. Dube and R. J. I. J. o. B. I. S. Mohanty," Towards the development of a cyber security capability maturity model," vol. 34, no. 1, pp. 104-127, 2020.

[2] A. Garba, M. M. Siraj, and S. H. J. A. S. T. E. S. J. Othman," An explanatory review on cybersecurity capability maturity models," vol. 5, no. 4, pp. 762-769, 2020.

[3] O. M. Al-Matari, I. M. Helal, S. A. Mazen, and S. J. I. S. J. A. G. P. Elhennawy," Integrated framework for cybersecurity auditing," vol. 30, no. 4, pp. 189-204, 2021.

[4] S. N. G. Gourisetti, M. Mylrea, and H. J. F. G. C. S. Patangia," Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis," vol. 105, pp. 410-431, 2020.

[5] Barclay," Sustainable security advantage in a changing environment: The Cybersecurity Capability Maturity Model (CM 2)," in Proceedings of the 2014 ITU kaleidoscope academic conference: Living in a converged world-Impossible without standards? 2014, pp. 275-282: IEEE.

[6] Sulistyowati, F. Handayani, and Y. J. J. I. J. o. I. V. Suryanto," Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss," vol. 4, no. 4, pp. 225-230, 2020.

[7] Y. Maleh, A. Sahid, and M. J. E. Belaissaoui," A maturity framework for cybersecurity governance in organizations," vol. 63, no. 6, pp. 1-22, 2021.

[8] Schmitz, M. Schmid, D. Harborth, S. J. C. Pape, and Security," Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities," vol. 108, p. 102306, 2021.

[9] M. Bitzer et al.," Managing the Inevitable–A Maturity Model to Establish Incident Response Management Capabilities," vol. 125, p. 103050, 2023.

[10] Aliyu et al.," A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom," vol. 10, no. 10, p. 3660, 2020.

[11] Almomani, M. Ahmed, and L. J. P. C. S. Maglaras," Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia," vol. 7, p. e703, 2021.

[12] Yigit Ozkan, S. van Lingen, M. J. J. o. C. Spruit, and Privacy," The cybersecurity focus area maturity (CYSFAM) model," vol. 1, no. 1, pp. 119-139, 2021.

[13] N. G. Gourisetti, M. Mylrea, and H. Patangia," Application of rank-weight methods to blockchain cybersecurity vulnerability assessment framework," in 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019, pp. 0206-0213: IEEE.

[14] G. Drivas, A. Chatzopoulou, L. Maglaras, C. Lambrinoudakis, A. Cook, and H. Janicke," A nis directive compliant- cybersecurity maturity assessment framework," in 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), 2020, pp. 1641-1646: IEEE.

[15] M. Rea-Guaman, T. San Feliu, J. A. Calvo-Manzano, and I. D. Sanchez-Garcia," Comparative study of cybersecurity capability maturity models," in Software Process Improvement and Capability Determination: 17th International Conference, SPICE 2017, Palma de Mallorca, Spain, October 4–5, 2017, Proceedings, 2017, pp. 100-113: Springer.

[16] Razikin and A. J. C. J. Widodo," General Cybersecurity Maturity Assessment Model: Best Practice to Achieve Payment Card Industry-Data Security Standard (PCI-DSS) Compliance," vol. 15, no. 2, pp. 91-104, 2021.

[17] N. Ramadhan and U. Rose," Adapting ISO/IEC 27001 Information Security Management Standard to SMEs," ed, 2022.

[18] P. G. Putra, F. Humani, F. W. Zakiy, M. R. Shihab, and B. Ranti," Maturity Assessment of Cyber Security in The Workforce Management Domain: A Case Study in Bank Indonesia," in 2020 International Conference on Information Technology Systems and Innovation

(ICITSI), 2020, pp. 89-94: IEEE.

[19] V. Monev," Organisational information security maturity assessment based on ISO 27001 and ISO 27002," in 2020 International Conference on Information Technologies (InfoTech), 2020, pp. 1-5: IEEE.

[20] P. N˘astase, F. N˘astase, C. J. E. c. Ionescu, e. c. studies, and research," Challenges generated by the implementation of the IT standards CobiT 4.1, ITIL v3 and ISO/IEC 27002 in enterprises," vol. 43, no. 3, pp. 1-16, 2009.

[21] J. Wibowo and K. J. J. S. I. Ramli," Impact of Implementation of Information Security Risk Management and Security Controls on Cyber Security Maturity (A Case Study at Data Management Applications of XYZ Institute)," vol. 18, no. 2, pp. 1-17, 2022.

[22] Bashofi and M. Salman," Cybersecurity Maturity

[23] Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002," in 2022 IEEE International Conference- on Cybernetics and Computational Intelligence (CyberneticsCom), 2022, pp. 58-62: IEEE.

[24] M. J. A. c. J. Alshar'e," CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001," pp. 245-255, 2023.