International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Cybersecurity Risk Assessment for Infrastructure of Information Systems in Yemen Telecoms

Abdulkarem Yahya Abohatem[1*], Fadl Mutaher Ba-Alwi [2], Mona Ahmed Mohammed Al-Haifi [3], Hana Hasan Al-hadheri [4]

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 21/03/2024

Abstract: This research paper focuses on conducting a comprehensive cybersecurity risk assessment for information systems (IS) and infrastructure within Yemen Telecoms (YT). The primary objective is to identify vulnerabilities, threats, and potential business impacts associated with cybersecurity risks. The research aims to prioritize risks, provide recommendations for risk mitigation, and highlight the importance of regular reassessments to adapt to a changing threat landscape.

Keywords: *Information Systems (IS), Yemen Telecoms (YT). Information Technology (IT).*

Introduction

Cybersecurity risk assessment plays a crucial role in providing visibility into vulnerabilities, threats, and potential business impacts. This section introduces the significance of conducting a thorough risk assessment to prioritize resources for remediation efforts. IT risk assessment is a crucial process for any enterprise administration digital assets and infrastructure. A thorough risk assessment provides visibility into vulnerabilities, threats, and potential business impacts. This allows prioritizing risks to focus resources on remediation efforts.[1] The assessment process typically involves identifying key systems, data, applications and networks that need protection as assets. It also determines potential sources of threats both internal and external to the organization. Vulnerabilities or weaknesses in the IT environment that could be exploited by threats are then evaluated. Finally, the likelihood and impact of identified risks are analyzed, considering factors like historical data and severity ratings. Once complete, the assessment provides a foundation for selecting appropriate security controls aligned with the risk profile. It also guides developing mitigation strategies, response plans and compliance programs addressing the organization's top concerns. Regular reassessment ensures risk oversight keeps pace with change.[2]

Problem Statement:

The problem statement highlights the need for a cybersecurity risk assessment in Yemen Telecoms due to the increasing cybersecurity threats faced by the organization. It emphasizes the specific risks associated with YT's location and industry.

1. Objectives of Research:

The research objectives include:

- Identifying key IT assets that require protection within Yemen Telecoms.
- Identifying potential threats to these assets.
- Assessing vulnerabilities in the IT infrastructure that threats could exploit.
- Analyzing the potential impacts of threats exploiting vulnerabilities.
- Evaluating the likelihood and impact of identified risks.
- Prioritizing risks based on their likelihood and impact.

Literature reviews

Area surveys significant writing on cybersecurity risks within the broadcast communications segment and their likenesses to the risks confronted by Yemen Telecoms. It references thinks about on common dangers, such as cyber-attacks, information breaches, human blunder, common fiascos, and obsolete program. Also, it highlights the discoveries of thinks about conducted by the Universal Media transmission Union (ITU). A chance appraisal within the IT environment is basic to the victory of any organization, with chance needing to be overseen in the event that the organization is to realize its objectives.[3] Firms, hence, got to embrace a risks appraisal of the IT environment in arrange to permit administration to

1 Sana'a University, Yemen
ORCID ID: 000-0002-8993-4613
** Corresponding Author Email:* Abdulkareem.abohatem@ptc.gov.ye
2 Sana'a University, Yemen Email: Dr.fadlbaalwi@gmail.com,
Information System Department, Faculty of Computer and Information Technology
3 Mona A M Al-Haifa Email : alhiphymona@gmail.com
Faculty of Banking and Financial Sciences, The Arab Academy for Banking and financial Sciences
4 Hana Hasan Al-hadheri Email : Omimh256@gmail.com
Information System Department, Faculty of Computer and Information

distinguish IT risks and the controls to moderate such dangers. This will empower the firm to apportion assets where they illustrate best esteem by guaranteeing that IT assets are not occupied to understanding issues that seem have been dodged, and guaranteeing more viable and proficient achievement of firm targets. [4] The security risks evaluation takes on numerous names and can shift enormously in terms of strategy, thoroughness, and scope, but the center objective remains the same: survey the data security risks to the organization's data resources. This data is at that point utilized to decide how best to moderate those data security risks and viably protect the organization's mission. There's no deficiency of definitions for security risks evaluation [5]. Numerous of these definitions are excessively complex or may be particularly adapted to an industry fragment such as the government. For illustration, the National Organized of Benchmarks and Innovation gives two elective definitions for the term security risks appraisal. One definition, found within the National Organized of Measures and Innovation (NIST) "Guide for Conducting Risks Assessments" (2012), states that security chance appraisal is "the prepare of distinguishing, evaluating, and prioritizing risks to organizational operations (counting mission, capacities, picture, notoriety), organizational resources, people, other organizations, and the Country, coming about from the operation of an information system." However, another definition found within the Worldwide Measures Organization/ Worldwide Electrotechnical Commission (ISO/IEC) 27000 "Information technology—Security techniques Information security administration systems Overview and lexicon grows the definition to portray the method with regard to risks resilience. It peruses as takes after: Risks Assessment the in general handle of finding, recognizing and portraying risks to comprehend the nature of chance and to decide the level of chance and of comparing the comes about of risks investigation with risks criteria to decide whether the risks and/or its greatness is worthy or mediocre [10]. Other employments of the term risk assessment are equipped toward a particular utilize, such as complying with the PCI DSS. The PCI Security Benchmarks Committee characterizes risks evaluation as a formal handle utilized by organizations to recognize risks and vulnerabilities that may adversely affect the security of cardholder information. The ISO 27001/2 takes an coordinates approach to security administration and recognizes the esteem of security risks appraisals in that prepare. The essential structure of security management involves selecting security prerequisites, surveying the dangers, and selecting controls [11]. The security appraisal is central to this approach, because it surveys the risks that the security prerequisites may not be met and gives the premise for a risk-based choice for selecting security controls. In all the controls, rules, and guidelines, security chance evaluation has been characterized in various ways. A few definitions are more point by point than others in terms of how an appraisal is performed [12]. A few definitions center on the result of the evaluation, whereas others center on the approach. For our purposes, a easier security risks appraisal definition is required to cover any such approach or detail. Since this book will talk about the different strategies of performing a security risks evaluation, the definition utilized here is designed to fit all such strategies. For the purposes of this book, security risks appraisal is characterized as takes after: Security Risks Assessment likelihood assurance of resource misfortunes based on resource valuation, risk examination, and an objective audit of current security controls effectiveness [13].

Methodology

The research methodology comprises six main steps for conducting the cybersecurity risk assessment. These steps include identifying key IT assets, identifying potential threats, assessing vulnerabilities, analyzing potential impacts, evaluating likelihood, and prioritizing risks.

The methodology involves 6 main steps:

1. Identify key IT assets like systems, databases, networks etc. that need protection.
2. Identify potential threats to these assets from external and internal sources like hackers, employee errors etc.
3. Assess vulnerabilities in the IT infrastructure that threats could exploit due to issues like outdated software, weak access controls etc.
4. Analyze potential impacts of threats exploiting vulnerabilities, in terms of financial losses, disruption impacts, data breaches etc.

Evaluate likelihood of each threat occurring and its impact. This is done through qualitative or quantitative analysis using historical data, reports. Prioritize identified risks based on likelihood and impact. This helps allocate resources to address high priority risks first. Regularly reassessing risks allows organizations to adapt to a changing threat landscape. IT risk assessment is important as it provides a comprehensive understanding of risks, enables proactive risk management and alignment with compliance needs. It supports Procedures of Risk Preventions by guiding control selection and implementation as per identified vulnerabilities and risks. Organizations that conduct IT risk assessments demonstrate commitment to managing risks effectively [14].

Importance of IT Risk Assessments:

This passage highlights the drift of combining numerous guidelines, particularly ISO 27001 (data security) and ISO 22301, to streamline the risks evaluation process [15]. The integration of these benchmarks permits organizations to require an all-encompassing approach to overseeing risks related to data security and trade progression, coming about in moved forward effectiveness, a bound together system for chance appraisal, and improved in general flexibility [16]. The paper highlights the utilize of ISO/IEC 27005:2018 as a direction record for conducting risks appraisals. This standard gives a system for organizations to evaluate and oversee data security risks viably. In expansion, the paper notices the utilization of ISO/IEC 27002, which serves as a code of hone for actualizing data security controls. This standard offers rules and best hones for building up and keeping up an data security administration framework (ISMS)[17]. The investigate points to examine and analyze different viewpoints of cybersecurity, counting chance recognizable proof, chance examination, risks assessment, chance treatment, risks acknowledgment, chance control, and cyber security development crevices. To back these targets, the think about utilizes the ISO/IEC 27005:2018 standard as direction for conducting risks appraisals and the ISO/IEC 27002 code of hone for data security control. The development level evaluation is performed utilizing the cyber security development demonstrate form 1.10 created by the National Cyber and Crypto Organization of the Republic of Indonesia [18].

Collecting Data for IT Risk Assessment:

Involves gathering Information from Various Sources to understand the organization's IT Systems, Assets, Processes, and Potential Risks. Here are some common methods and sources for data collection in IT risk assessment [19]:

1. Documentation Review: Review existing documentation such as IT policies, procedures, system documentation, incident reports, business continuity plans, and security controls documentation. This helps in understanding the organization's IT infrastructure, security measures, and previous incidents or vulnerabilities.

2. Interviews and Workshops: Conduct interviews and workshops with key stakeholders, including IT personnel, management, system administrators, and other relevant staff. These discussions can provide insights into system architecture, operational practices, security controls, and potential risks.

3. Asset Inventory: Create an inventory of IT assets, including hardware, software, databases, networks, and critical applications. This inventory should include details such as asset descriptions, locations, owner information, and their importance to business operations.

4. Vulnerability assessment:

Perform defenselessness evaluations utilizing mechanized apparatuses or manual methods to recognize potential shortcomings and vulnerabilities within the IT framework. This incorporates filtering frameworks for known vulnerabilities, misconfigurations, and obsolete program forms.

5. Threats Intelligence: Assemble data from outside sources, such as security advisories, merchant cautions, industry reports, and danger insights nourishes. Remain upgraded on rising dangers, common assault vectors, and vulnerabilities influencing comparative organizations or advances.

6. Incident and Event Logs: Review logs from security devices, intrusion detection systems, firewalls, and other security tools. Analyze past security incidents, breaches, and system events to identify patterns, trends, and potential weaknesses.

Implementing IT risk assessment

The input indicators such as access attempts, user importance and security layers are used to calculate a risk percentage and level based on likelihood, impact and uncertainty factors. The assessment provides a quantitative analysis of network hacking threats.

In the context of IT risk assessment, the formula:

"Risk Assessment = Attempt Period × Number of Access Attempts × User Type Importance × Security Layer Reached × Asset Value"

represents a quantitative approach to assessing risk. It considers factors such as the time period for attempted attacks, the number of access attempts, the importance of user types, the security level layer reached, and the value of the assets at risk. By quantifying these elements, organizations can better understand and prioritize the potential risks they face and allocate resources accordingly [20].

Determine the network layers

In IT network architecture, the concept of layered networking is fundamental for designing and managing a reliable and scalable infrastructure. The network layers typically refer to the OSI model, which has seven layers, but for simplicity, we can focus on a three-layer model that aligns with your description.

Output(risk assessment)		Input				Indicator				
Risk Assessment (%)	Risk Level	Attempt Period (hours)	Number of Access Attempts	User Type Importance1-3	Security Layer Reached	Asset Value	Attack Success Probability	Likelihood	Probable Loss	Uncertainty
70	Medium	24	10	3	2	High	High	High	Low	V-low
41.2	Low	12	5	2	1	High	Medium	Medium	V-low	low
100	V-High	6	2	1	3	High	V-High	V-High	V-high	High
90	V-High	48	20	2	2	High	High	High	low	V-low
86.4	High	72	15	3	1	High	Medium	Medium	V-low	low
10	V-low	1	1	1	1	High	Medium	Medium	V-low	Low

IT Monitoring Systems:

IT monitoring system like Security Data and Occasion Administration (SIEM), Security Occurrence Administration (SIM), and Security Occasion Administration (SEM) are pivotal for compelling cybersecurity operations. SIEM arrangements total and analyze security occasion information from different sources, empowering real-time risk discovery and reaction. SIM frameworks center on occurrence administration and reaction, encouraging the examination and moderation of security occurrences. SEM frameworks give investigation and relationship of security occasions, helping in recognizing designs and potential dangers. Other cases of IT monitoring system incorporate Organize Behavior Investigation (NBA) and Client and Substance Behavior Analytics (UEBA), which screen organize activity and client behavior for peculiarity location. These frameworks collectively upgrade situational mindfulness and empower proactive cybersecurity defenses [21].

Steps to collection data

To obtain information from IT monitoring tools regarding unauthorized access attempts to the network, you can follow these steps:

1. Get the information from the IT monitoring tools such as SIEM or network intrusion detection systems (NIDS) to capture and analyze network traffic and security events.

2. Detect unauthorized access attempts. This can include monitoring failed login attempts, suspicious IP addresses, or unusual patterns of network traffic.

3. When an unauthorized access attempt is detected, the system will trigger an alert or notification. This may involve reviewing logs, examining network traffic, or analyzing system events associated with the incident.

4. Collect and document relevant information related to the unauthorized access attempt, such as the source IP address, timestamp, affected systems or accounts, and any additional contextual details.

5. Based on the severity and nature of the incident, take appropriate actions, such as blocking the IP address, strengthening security controls, or escalating the incident for further investigation and response.

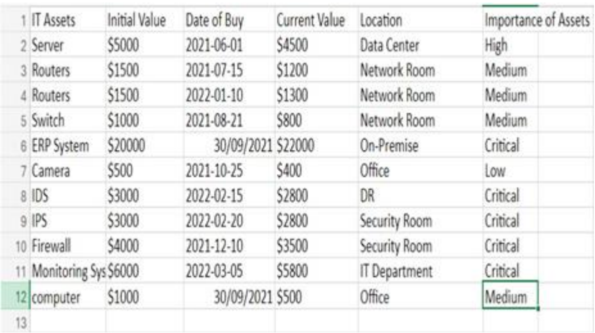
6. Document the incident details, actions taken, and any remediation steps. Report the incident to the appropriate

teams, such as the incident response team or the IT security team, for further analysis and response.

Show the below table from IT monitoring systems

Evaluation the IT assets

This program is designed to evaluate the importance of IT assets, factoring in their location, age, and value. It's particularly useful for organizations that need to prioritize their assets for maintenance, upgrades, or security purposes. By considering whether an asset is in a disaster recovery site (DR) or a primary data center (DC), its current value relative to its initial cost, and the time elapsed since its purchase, the program can categorize assets by importance. This helps in making informed decisions about resource allocation, ensuring that critical assets are maintained or replaced in a timely manner, and ultimately supports the resilience and efficiency of IT operations. The program's logic reflects a nuanced approach to asset management



	IT Assets	Initial Value	Date of Buy	Current Value	Location	Importance of Assets
1	IT Assets	Initial Value	Date of Buy	Current Value	Location	Importance of Assets
2	Server	$5000	2021-06-01	$4500	Data Center	High
3	Routers	$1500	2021-07-15	$1200	Network Room	Medium
4	Routers	$1500	2022-01-10	$1300	Network Room	Medium
5	Switch	$1000	2021-08-21	$800	Network Room	Medium
6	ERP System	$20000	30/09/2021	$22000	On-Premise	Critical
7	Camera	$500	2021-10-25	$400	Office	Low
8	IDS	$3000	2022-02-15	$2800	DR	Critical
9	IPS	$3000	2022-02-20	$2800	Security Room	Critical
10	Firewall	$4000	2021-12-10	$3500	Security Room	Critical
11	Monitoring Sys	$6000	2022-03-05	$5800	IT Department	Critical
12	computer	$1000	30/09/2021	$500	Office	Medium
13						

<table>
<tr><td colspan="15">Technical Risks</td></tr>
<tr><td colspan="4">Risk Codes</td><td colspan="3">2-RSK Tech</td><td colspan="2">Risk</td><td colspan="6">Viruses</td></tr>
<tr><td colspan="4">Risk Description</td><td colspan="11">Unauthorized access to Servers and the main devices of the Organization.</td></tr>
<tr><td colspan="4">Risk Site</td><td colspan="11">Data Center "DC"</td></tr>
<tr><td colspan="5">Responsible Person for contacting him when the Risk is occurred.</td><td colspan="10">1-General Administration for IT (Service Desk)
2- Information Security Administration</td></tr>
<tr><td colspan="5">Risk Probability</td><td colspan="5">Impact of Risk in case of Occurrence.</td><td colspan="5">Risk Level Value</td></tr>
<tr><td><b>1</b></td><td><b>2</b></td><td><b>3</b></td><td><b>4</b></td><td><b>5</b></td><td><b>1</b></td><td><b>2</b></td><td><b>3</b></td><td><b>4</b></td><td><b>5</b></td><td><b>10-20</b></td><td><b>30-45</b></td><td><b>46-74</b></td><td><b>75-85</b></td><td><b>90-100</b></td></tr>
<tr><td colspan="5">Procedures of Risk Prevention</td><td colspan="10">1. Implement advanced threat hunting capabilities to actively search for viruses and related threats.
2. Engage in threat intelligence sharing with trusted partners and industry forums.
3. Implement advanced deception technologies to lure and detect virus attacks
4. Continuously monitor and analyze network and endpoint logs for signs of virus activity.
5. Conduct regular red team exercises to simulate virus outbreaks and test response capabilities.</td></tr>
</table>

Process to determine the mitigated risk:

implementing process on unauthorized access attempts from the internal network of end users in the information systems network for YT

1. Identify Assets: Identify the key assets within the IT organization that need to be protected. This can include hardware, software, data, networks, and systems.

2. Identify Threat Sources: Identify potential sources of threats that could pose risks to the identified assets. This can include external entities such as hackers or malicious actors, as well as internal threats such as employee negligence or system failures.

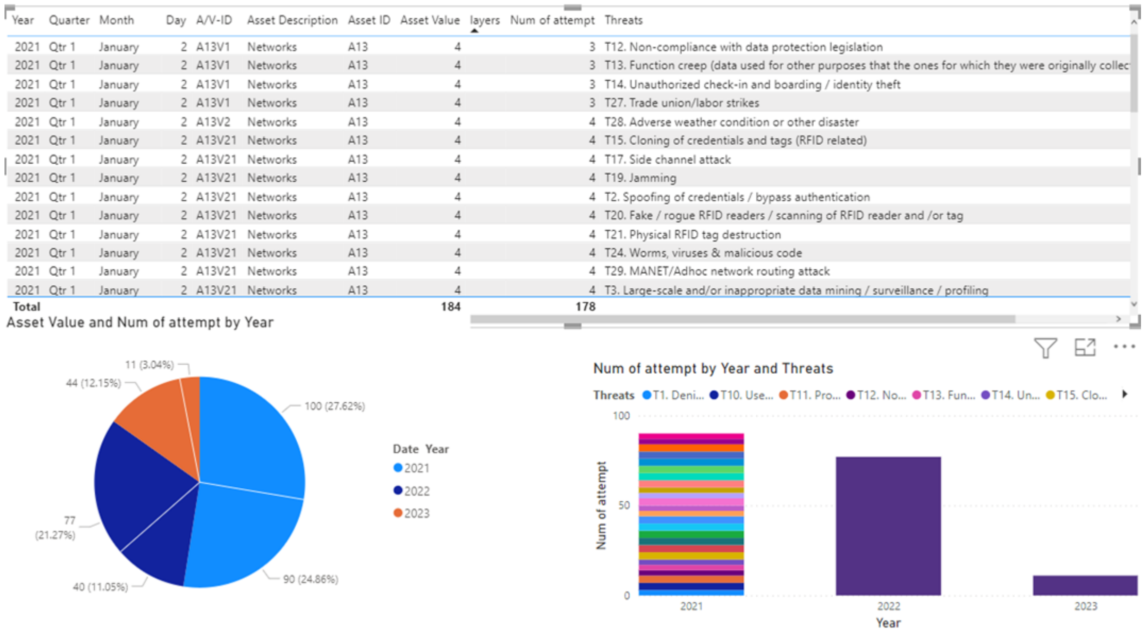
3. Evaluate Likelihood: Assess the likelihood of each identified threat occurring and the corresponding impact if it were to materialize. This can be done through qualitative or quantitative analysis, using historical data, industry reports, or expert judgment.

4. Prioritize Risks: Based on the likelihood and impact assessments, prioritize the identified risks. This helps allocate resources and focus on addressing the most critical risks first.

Show the table 4.4 which fill to determine the risk assessment in technical risks

Report about the difference years of monitoring system

The analysis of the information collected from the IT monitoring system at Yemen Telecoms highlights a concerning pattern of unauthorized access threats. These incidents involve unauthorized access, deletion, or modification of devices and data, posing a significant risk to the organization's security. The fact that both admin and user accounts were targeted indicates potential vulnerabilities across different user types. The varying number of



Year	Quarter	Month	Day	A/V-ID	Asset Description	Asset ID	Asset Value	layers	Num of attempt	Threats
2021	Qtr 1	January	2	A13V1	Networks	A13	4		3	T12. Non-compliance with data protection legislation
2021	Qtr 1	January	2	A13V1	Networks	A13	4		3	T13. Function creep (data used for other purposes that the ones for which they were originally collec
2021	Qtr 1	January	2	A13V1	Networks	A13	4		3	T14. Unauthorized check-in and boarding / identity theft
2021	Qtr 1	January	2	A13V1	Networks	A13	4		3	T27. Trade union/labor strikes
2021	Qtr 1	January	2	A13V2	Networks	A13	4		4	T28. Adverse weather condition or other disaster
2021	Qtr 1	January	2	A13V21	Networks	A13	4		4	T15. Cloning of credentials and tags (RFID related)
2021	Qtr 1	January	2	A13V21	Networks	A13	4		4	T17. Side channel attack
2021	Qtr 1	January	2	A13V21	Networks	A13	4		4	T19. Jamming
2021	Qtr 1	January	2	A13V21	Networks	A13	4		4	T2. Spoofing of credentials / bypass authentication
2021	Qtr 1	January	2	A13V21	Networks	A13	4		4	T20. Fake / rogue RFID readers / scanning of RFID reader and /or tag
2021	Qtr 1	January	2	A13V21	Networks	A13	4		4	T21. Physical RFID tag destruction
2021	Qtr 1	January	2	A13V21	Networks	A13	4		4	T24. Worms, viruses & malicious code
2021	Qtr 1	January	2	A13V21	Networks	A13	4		4	T29. MANET/Adhoc network routing attack
2021	Qtr 1	January	2	A13V21	Networks	A13	4		4	T3. Large-scale and/or inappropriate data mining / surveillance / profiling
Total							184		178	

Asset Value and Num of attempt by Year

Num of attempt by Year and Threats

However, after implementing the Procedures of Risk Prevention, Yemen Telecoms has experienced a reduction in threat attacks. The adoption of the framework has enabled the organization to implement enhanced security measures, including access controls, user privilege restrictions, regular security reviews, password complexity requirements, monitoring of admin activities, and restricted application access to databases. This Procedures of Risk Prevention provides a structured approach to identify and mitigate risks, strengthen defenses, and improve overall security posture.

The successful implementation of the framework has resulted in a decrease in the number and frequency of unauthorized access incidents. It demonstrates that the Procedures of Risk Prevention has been effective in enhancing the organization's security and mitigating potential vulnerabilities. To maintain a robust security posture, continued adherence to the Procedures of Risk Prevention, along with regular monitoring, assessment, and updates, is crucial. This will ensure the organization's ability to detect, prevent, and respond to future threats effectively and safeguard against unauthorized access incidents.

The SharePoint policy governs the usage and access controls for the organization's SharePoint environment. It ensures that proper security measures are in place to protect sensitive data stored in SharePoint sites and prevent unauthorized access. The policy may include guidelines for user attempts, ranging from 3 to 20, suggests an ongoing and persistent threat that requires immediate attention. The incidents also targeted multiple layers, demonstrating the need for a comprehensive security approach. The recurring nature of these incidents over several months underscores the importance of conducting further investigation and analysis to fully understand the impact, identify vulnerabilities, and implement effective security measures to mitigate future risks.

The finding

The cybersecurity risk assessment at Yemen Telecoms identified key IT assets requiring protection, potential threats, vulnerabilities in the infrastructure, potential impacts, and prioritized risks based on likelihood and impact.

Conclusions

In conclusion, the comprehensive cybersecurity risk assessment conducted at Yemen Telecoms revealed crucial insights into the organization's vulnerabilities, threats, and potential impacts. By identifying key IT assets requiring protection, assessing vulnerabilities, and analyzing the likelihood and impact of risks, Yemen Telecoms can prioritize resources for effective risk mitigation. The assessment highlights the importance of regular reassessment to adapt to a changing threat landscape and maintain robust cybersecurity measures. These findings provide a solid foundation for developing mitigation strategies, response plans, and compliance programs, enabling Yemen Telecoms to enhance its overall cybersecurity posture and safeguard its critical assets from potential threats.

- Risk assessments is the method of distinguishing, analyzing, and assessing potential dangers to an organization. It includes evaluating the probability and effect of dangers and deciding suitable hazard moderation techniques.
- Risk assessments help organizations understand their vulnerabilities and make informed decisions to minimize potential harm or loss.

References

[1] N. Abdulrahim, "Managing Cybersecurity as a Business Risk in Information Technology-based Smes," University of Nairobi, 2019.

[2] W. Shafik, "A Comprehensive Cybersecurity Framework for Present and Future Global Information Technology Organizations," in *Effective Cybersecurity Operations for Enterprise-Wide Systems*: IGI Global, 2023, pp. 56-79

[3] https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTSS-2020-4-PDF-E.pdf

[4] F. Aferudin and K. Ramli, "The Development of Cybersecurity Information Sharing Framework for National Critical Information Infrastructure in Indonesia," *Budapest International Research and Critics Institute-Journal (BIRCI-Journal),* vol. 5, no. 3, pp. 22859-22872, 2022.

[5] A. Ahmad, K. C. Desouza, S. B. Maynard, H. Naseer, and R. L. Baskerville, "How integration of cyber security management and incident response enables organizational learning," *Journal of the Association for Information Science and Technology,* vol. 71, no. 8, pp. 939-953, 2020.

[6] 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.

[7] B. Alhayani, S. T. Abbas, D. Z. Khutar, and H. J. Mohammed, "Best ways computation intelligent of face cyber attacks," *Materials Today: Proceedings,* pp. 26-31, 2021.

[8] S. K. Alhuqail and N. S. M. Jamail, "Implementation of an Effective Framework in Merging Cybersecurity and Software Engineering," in *2023 Sixth International Conference of Women in Data Science at Prince Sultan University (WiDS PSU)*, 2023: IEEE, pp. 31-36.

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

[10] I. 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.

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

[12] D. S. Anye, "Categorizing Cyber Threat on Critical Infrastructure: Assessing the Terrorist Threat against Cameroon's Telecommunications," Capitol Technology University, 2018.

[13] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics,* vol. 12, no. 6, p. 1333, 2023.

[14] [I. Atoum, A. Otoom, and A. A. Ali, "Holistic cyber security implementation frameworks: A case study of jordan," *International Journal of Information, Business and Management,* vol. 9, no. 1, p. 108, 2017.

[15] F. Baiardi and C. Telmon, "Risk management of an information infrastructure: a framework based upon security dependencies," *International Journal of System of Systems Engineering,* vol. 1, no. 1-2, pp. 237-256, 2008.

[16] C. 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: IEEE, pp. 275-282.

[17] I. Bashofi and M. Salman, "Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002," in *2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)*, 2022: IEEE, pp. 58-62.

[18] N. Belanova, "Risks of IT technology adoption," in *E3S Web of Conferences*, 2023, vol. 376: EDP Sciences, p. 05014.

[19] A. Beloglazov, R. Buyya, Y. C. Lee, and A. J. A. i. c. Zomaya, "A taxonomy and survey of energy-efficient data centers and cloud computing systems," vol. 82, pp. 47-111, 2011.

[20] K. Bezas and F. Filippidou, "Comparative analysis of open source security information & event management systems (SIEMs)," *Indonesian Journal of Computer Science*, vol. 12, no. 2, pp. 443-468, 2023.

[21] M. Bitzer *et al.*, "Managing the Inevitable–A Maturity Model to Establish Incident Response Management Capabilities," vol.