International Journal of Educational Management and Innovation
Vol.3, No.2, May 2022, pp. 155~168
e-ISSN: 2716-2338
DOI: 10.12928/ijemi.v3i2.5794

Cyber Resilience Evaluation Using Cyber Resilience Review Framework at University XYZ

Ahmad Maulana Fikri[1*], Lovinta Happy Atrinawati[*], M. Gilvy Langgawan Putra[3]
[1,2,3] Kalimantan Institute of Technology, Balikpapan, Indonesia
[1*]10171001@student.itk.ac.id, [2]lovinta@lecturer.itk.ac.id,
[3]gilvy.langgawan@lecturer.itk.ac.id

Article Info

Article history
Received February 25, 2022
Revised March 23, 2022
Accepted April 4, 2022

Keywords: CRR Assessment; Cyber Resilience; Cyber Resilience Evaluation; University XYZ

ABSTRACT

Cyber resilience is about protecting data and information owned by University XYZ and adapting business processes at University XYZ to ensure service continuity when cyber threats occur. However, University XYZ never evaluates its practices to implement security and data management. University XYZ needs to know its maturity level based on cyber resilience evaluation to improve its cyber resilience. Therefore, this research was carried out to evaluate cyber resilience at University XYZ using the Cyber Resilience Review (CRR) assessment by evaluating ten cyber resilience domains. The evaluation covers academic services that use the University XYZ academic information system. The evaluation process will be held through an interview with the process owner. The interview questions are based on CRR assessment. After the evaluation, we found that none of the domains in University XYZ had yet reached Maturity Indicator Level (MIL)-1. In addition, the overall performance percentage for each CRR domain had not yet reached 100%. An improvement recommendation for each domain has also been made, containing guidance for implementing incomplete and non-committed practices. University XYZ can implement cyber resilience practices according to recommendations so that the implementation process can run optimally, even though cyber threats occur from time to time.

1. INTRODUCTION

People's dependence on information technology can increase the possibility of cyberattacks on a system in society, organizations, or companies (Sep'ulveda-Estay et al., 2020), along with advances in information technology (Arianto, 2017). These cyber-threats have evolved to influence numerous aspects of cyberspace, including DDoS attacks, data theft, data code alterations, and computer virus attacks. The surge in cyberattacks in society will pose a new challenge in maintaining information availability, integrity, and confidentiality. Severe cyberattacks can have consequences in terms of service delivery if system operations stop (Annarelli, Nonino, and Palombi, 2020). Some organizations that rely on information technology will receive a considerable impact. For example, the cases are the State of Georgia in 2008 (Rahmawati, 2017), the company SZ DJI Technology Co., Ltd in 2017 (Adianto, Ali and Saptono, 2020), and the website Tiket.com (Perdani, Widyawan, & Santosa, 2018).

Researchers worldwide are increasingly looking for ways to design a resilient cyberinfrastructure and withstand stochastic failures and targeted attacks to counter cyber threats. (Choudhury et al., 2015). The ability of a system to prepare for, absorb, recover from, and adapt to unfavorable consequences, such as cyberattacks, is known as cyber resilience (Linkov & Kott, 2019). Cyber resilience refers to a system's ability to anticipate, absorb, recover from, and adapt to negative consequences, particularly those caused by cyberattacks (Linkov & Kott, 2019; Williams & Manheke, 2010). In addition, cyber resilience can also be interpreted as the ability to continue to provide the desired results despite a negative cyber incident (Björck et al., 2015). As it meets the requirement for security and reliability of corporate operations, cyber resilience is also an essential component of mission-critical infrastructure protection and a significant component of the value proposition for government partnerships (NIAC, 2009). The system must dynamically reconfigure itself in reaction to events inside and outside the environment, including non-hazardous environmental impacts and cyber incidents, to ensure cyber resilience of critical infrastructure and other systems (Koelemeijer, 2018).

Several researchers have conducted cyber resilience research to solve cyber threats problems. There are studies conducted to obtain recommendations for increasing cyber resilience, namely recommendations for cyber resilience in the energy sector (Hagen, 2018), the government sector (Tonhauser & Ristvej, 2019; Srinivas, Das, & Kumar, 2019), and the country's development sector (Chang & Coppel, 2020). An industrial control system or Industrial Control System (ICS) has also been carried out with research related to the formulation of the overall ICS network resilience metric (Haque, Shetty, and Krishnappa, 2019) and a tool to be able to assess and evaluate cyber resilience (Haque et al., 2018). Research related to cyber resilience is also carried out in the critical infrastructure sector, considering essential infrastructure based on guarantee cases (Koelemeijer, 2018) and evaluation through statistical assessments (Rehak et al., 2019). Finally, a cyber resilience assessment was also carried out using various methods, namely the Cyber Resilience Assessment Framework (Sep'ulveda-Estay et al., 2020) and the Data Flow Material Model (DFMM) (Alghamdi & Rastogi, 2020).

Good cyber resilience is needed for a university-level with very crucial data. In this research, we will discuss cyber resilience at University XYZ. Cyber resilience is utilized to minimize cyber threats that can harm University XYZ's operational activities. In addition, this can also impact the speed of service delivery, where the service in question is academic service. If an unexpected cyber threat occurs, it will undoubtedly impact various sectors and hinder one of University XYZ's missions to organize a technology-based education process. Previously, University XYZ had experienced a cyberattack, namely someone who tried to hack academic data at University XYZ. ICT at University XYZ has realized and improved the security system at University XYZ to protect academic data. If the data is successfully hacked, it will significantly affect various organizational units. Improving and improving data security takes a long time

and will deliver academic services at University XYZ. Therefore, University XYZ needs to improve cyber resilience to survive and adapt to a cyber threat. The level of maturity in preparing for cyber threats is the key to cyber resilience. However, University XYZ never evaluates its practices to implement security and data management. If cyber resilience at University XYZ has reached a high maturity, the process for restoring academic services can be faster than before. So, it can be said that the process of securing data and information at University XYZ has not been maximized.

People can use several methods to assess cyber resilience in an organization, namely the Industrial Control System Cyber Resilience Assessment Tool or ICS-CRAT, NIST Cybersecurity Framework, and Cyber Resilience Review or CRR. The ICS-CRAT tool is a qualitative simulation tool for evaluating cyber resilience in Industrial Control Systems (ICS). The ICS-CRAT simulation output can assist in understanding the application and reasoning of CRAT and offer an overview of its ability to provide a realistic assessment of ICS resilience. An organization that uses ICS can improve cyber resilience based on the evaluation results obtained using ICS-CRAT (Haque, Shetty, & Krishnappa, 2019).

After that, there is another method, namely the NIST Cybersecurity Framework. The NIST Cybersecurity Framework (NIST CF) is a framework for enterprises to manage better and reduce cybersecurity risks based on current standards, guidelines, and practices. NIST CF aims to enhance risk management and cybersecurity communication among internal and external organizational stakeholders and assist companies in managing and reducing risk. NIST created this framework through collaboration between industry and government. The methodology used to create the framework can assist critical infrastructure owners and operators in managing cybersecurity threats. This framework emphasizes using business drivers to direct cybersecurity efforts and the inclusion of cybersecurity risks in the risk management process (NIST, 2018).

ICS-CRAT can only be used by an organization that implements an industrial control system. University XYZ does not implement an industrial control system but rather an information technology commonly used by educational institutions. Therefore, the ICS-CRAT was not used in this study as an assessment method to maximize the results achieved. CRR further asserts that it was written to be a universal assessment approach that can evaluate the cyber resilience capabilities of diverse companies in terms of different vital services or critical infrastructure sectors and their size and maturity.

The NIST Cybersecurity Framework can also evaluate cyber resilience in an organization. NIST CF is also a universal method like CRR. However, cyber resilience is different from cybersecurity. Therefore, CRR adopted several approaches used by NIST CF to sharpen the assessment scope into cyber resilience. The CRR is in alignment with the NIST CF, where the CRR preceded the formation of the NIST CF, but the inherent principles and practices recommended in the CRR align with the core principles of the NIST CF. Thus, CRR becomes the

proper assessment method for evaluating and improving cyber resilience in University XYZ. In addition, research related to cybersecurity has been carried out at University XYZ, so cybersecurity as one of the essential processes at University XYZ also needs to be done.

Based on these problems, it can be concluded that University XYZ needs the proper steps to improve cyber resilience. The research will evaluate cyber resilience at University XYZ with the Cyber Resilience Review assessment. The research begins by evaluating the level of cyber resilience implemented at University XYZ. After that, a gap analysis will be carried out and recommended steps to improve cyber resilience in University XYZ. Finally, this research will produce a plan for University XYZ to improve cyber resilience with practices documented in the Cyber Resilience Review assessment. With the plan to increase cyber resilience at University XYZ through the Cyber Resilience Review assessment, University XYZ can prepare information and communication technology at University XYZ and respond well to a cyber threat. This research aims to facilitate the company's operational activities and achieve company goals, even though cyber threats occur from time to time.

2. METHODS

The Department of Homeland Security (DHS) developed the Cyber Resilience Review (CRR) as a lightweight assessment technique to evaluate critical infrastructure owners and operators' cybersecurity procedures and service continuity. CRR has 299 questions evaluating cybersecurity practices and provides two methods for conducting evaluations: a six-hour workshop facilitated by the DHS and self-assessment. Both methods contain the same questions, scoring mechanisms, and options for improvement. The CRR is an interview-based evaluation of a company's cybersecurity program. The purpose of the interviews was to understand better how cybersecurity services and their associated assets are managed, as they are crucial to the organization's mission success. The CRR focuses on important protections and sustainable practices that contribute to an organization's overall cyber resilience. CRR assesses essential cybersecurity capabilities and behaviors to give a valuable indicator of an organization's operational resilience in everyday and stressful situations. CRR uses maturity Indicator Levels (MILs) to offer enterprises estimates of the maturity of their cybersecurity processes across ten categories. Table 1 details the practice domains examined by the CRR. Each domain represents a critical capability that contributes to an organization's cybersecurity (Cybersecurity and Infrastructure Security Agency, 2020).

Table 1. Composition of CRR Domains (Cybersecurity and Infrastructure Security Agency, 2020)

CRR Domain	Number of Goals	Number of Practices MIL1	Number of Practices MIL2 – MIL5	Total Practice MIL1 – MIL5
Asset Management	7	65	13	78

Controls Management	4	25	13	38
Configuration and Change Management	3	27	13	40
Vulnerability Management	4	33	13	46
Incident Management	5	23	13	36
Service Continuity Management	4	18	13	31
Risk Management	5	13	13	26
External Dependencies Management	5	14	13	27
Training and Awareness	2	11	13	24
Situational Awareness	3	8	13	21

Source: Cybersecurity and Infrastructure Security Agency, 2020

CRR uses the Maturity Indicator Level (MIL) to provide enterprises with an estimate of the maturity of their operations in 10 data and information security categories. The degree to which cybersecurity practices are institutionalized in each domain within an organization determines the maturity. Institutionalization means becoming part of a more informed and permanent organization because cybersecurity practices are managed and supported in a meaningful way. The MIL scale uses six maturity levels, each with a defined, rigorous, incomplete component that is implemented, planned, managed, measured, and defined (Cybersecurity and Infrastructure Security Agency, 2020).

In general, this research consists of several stages, where the stages used are also sourced from the recommendations for the CRR stage. In Figure 1, the steps will be carried out in this study.

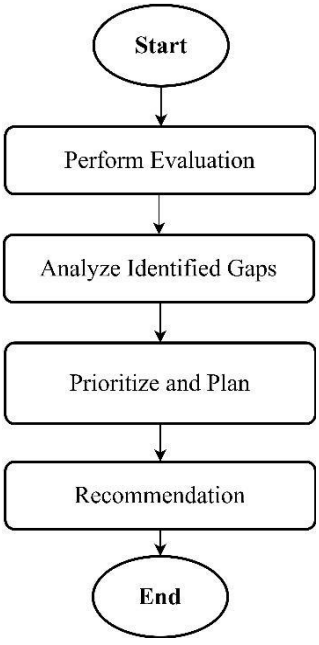

Figure 1. Evaluation Steps

Source: Cybersecurity and Infrastructure Security Agency, 2020

3. RESULTS AND DISCUSSION

RESULTS

The cyber resilience evaluation process consists of three stages: perform evaluation, analyze identified gaps, and prioritize and plan. The following are the results of the three stages.

3.1. Perform Evaluation

Before conducting the evaluation, planning is carried out, determining the evaluation's scope and identifying and preparing participants. Determining the scope of the evaluation is an essential process because answers to self-assessment questions must be provided concerning a particular service. In Table 2, three factors have been identified, including critical services, organization, and assets. Table 2 is obtained from observation and interviews with stakeholders.

Table 2. Scope of Evaluation

Scope	Statement
Critical Service	University XYZ Academic Services
Organization	University XYZ
Asset	● *People*: University XYZ Employee ● *Information*: Student data, grade data, course data, course syllabus, and course teaching materials ● *Technology*: University XYZ Academic Information System ● *Facilities*: Server, NAS, Router, Switch, LAN Cable, Public IP

After that, ten cyber resilience domains will be evaluated with the scope specified in Table 2. The first evaluation will be carried out on existing practices at MIL-1. The results of the MIL-1 evaluation at University XYZ can be seen in Table 3.

Table 3. MIL-1 Evaluation Results

Domain	Yes	Incomplete	No
Asset Management	28	4	33
Controls Management	17	3	5
Configuration and Change Management	16	4	7
Vulnerability Management	11	0	22
Incident Management	6	3	14
Service Continuity Management	4	5	9
Risk Management	0	0	13
External Dependencies Management	1	0	13
Training and Awareness	3	0	8
Situational Awareness	2	0	6

Table 3 is obtained from the interview with the business process owner for each domain. Based on the evaluation results in Table 3, the evaluation was only carried out up to MIL-1 questions. This decision is because there are "incomplete" and "no" practice answers. Thus, the

evaluation cannot be continued at the next level or MIL-2. The numbers in table 3 represent the number of CRR practices implemented by University XYZ.

3.2. Analyze Identified Gaps

Based on Table 1 and Table 3, the Maturity Indicator Levels (MIL) and overall performance percentage for each domain will be calculated. This calculation is carried out to evaluate how University XYZ is practicing CRR. In calculating the MIL, it is calculated by the following formula based on CRR Framework.

$$\frac{\text{Total "Yes"} + (0.5 \times \text{Total "Incomplete"})}{\text{Total Domain Practices at MIL n}}$$

Based on the above formula, the MIL can be seen in Figure 2.

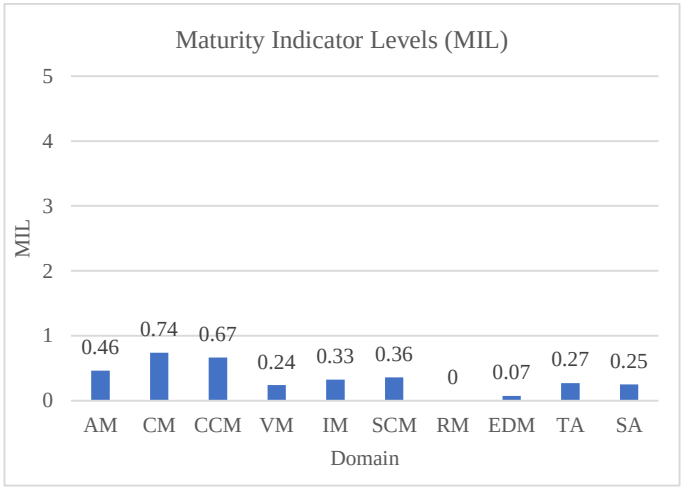

Figure 2. MIL of Each Domain CRR

From Figure 2, it can be concluded that none of the cyber resilience domains reached MIL1 at University XYZ. This condition will make it difficult for University XYZ to restore its original condition when a cyber threat occurs. MIL1 states that all practices have been carried out. If MIL1 has not been achieved, it can be concluded that University XYZ still has not implemented cyber resilience practices. The lack of data management at University XYZ, such as the absence of documentation in each domain, can be the first reason. If University XYZ wants to increase to MIL1, then University XYZ needs to implement practices that have not been done in each domain.

Next, the percentage of the domain's overall performance will be calculated, where this calculation will produce the percentage of the number of practices that have been carried out from all practices, starting from MIL1 to MIL5. Therefore, the formula based on the CRR framework for calculating the overall performance of each domain is as follows.

$$\frac{\text{Total "Yes"}}{\text{Total Practices MIL1} - \text{MIL5}} \times 100\%$$

Based on the above formula, the overall performance percentage of the domain can be seen in Figure 3.

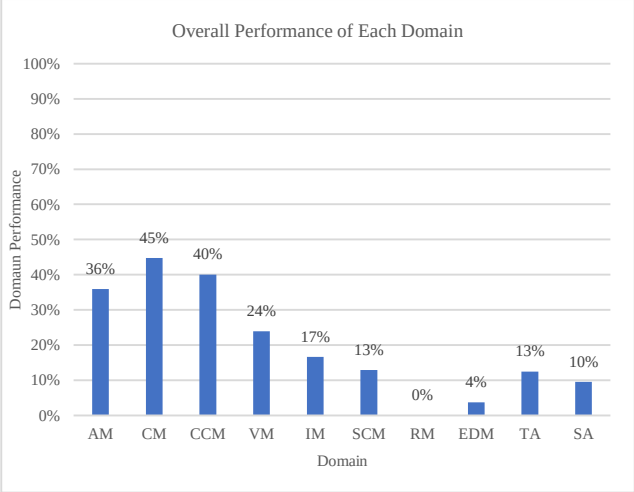

Figure 3. Percentage Performance of Each Domain CRR

From Figure 3, it can be said that University XYZ has not been optimal in paying attention to cyber resilience practices. This result is evidenced by every domain that has not reached a performance value of 100%. The values obtained represent the practices carried out from MIL1 to MIL5 in each domain. So, it can be recommended that University XYZ needs to pay attention to low-value domains. This recommendation aims to generalize the ability of University XYZ to increase cyber resilience.

3.3. Prioritize and Plan

A series of activities will be carried out to prioritize cyber resilience practices at this stage. After completing the gap analysis, the organization must prioritize the steps necessary to thoroughly apply the practices that enable the fulfillment of the desired capabilities in a specific area. Before prioritizing, criteria will be determined to assist organizations in prioritizing CRR domains. In Table 4, the scores for each criterion have been determined based on University XYZ standard criteria.

Table 4. Priority Criteria

Score	Description Organization Goals (OG)	Business Goals (BG)	Resource Availability (RA)
5 (*Very High*)	Domain goals strongly support the achievement of organizational goals.	Domain goals strongly support the achievement of business goals in the organization.	Resources on the organization are highly available to implement domain goals.
4 (*High*)	Domain goals can support the achievement of organizational goals.	Domain goals can support the achievement of business goals in the organization.	Resources on the organization are available to implement domain goals.
3 (*Moderate*)	Domain goals may support the achievement of organizational goals.	Domain goals may support the achievement of the organization's business goals.	Resources on the organization may be available to implement domain goals.

Score	Description Organization Goals (OG)	Business Goals (BG)	Resource Availability (RA)
2 (*Low*)	Domain goals do not support the achievement of organizational goals.	Domain goals do not support the achievement of business goals in the organization.	Resources on the organization are not available to implement domain goals.
1 (*Very Low*)	Domain goals strongly do not support the achievement of organizational goals.	Domain goals strongly do not support the achievement of business goals in the organization.	Resources in the organization are severely unavailable to implement domain goals.

These criteria will serve as a guide for determining the priority of each destination in each domain. The following are the prioritization results that have been carried out and are listed in Table 5. Data from table 5 is obtained from scoring each domain and match with table 4.

Table 5. Priority Results

Domain	Number of Goals	Score	Priority
Asset Management	7	4	80%
Controls Management	4	5	100%
Configuration and Change Management	3	3	60%
Vulnerability Management	4	2	40%
Incident Management	5	2	40%
Service Continuity Management	4	2	40%
Risk Management	5	5	100%
External Dependencies Management	5	3	60%
Training and Awareness	2	1	20%
Situational Awareness	3	1	20%

It can be shown in Table 5. that each domain gets its priority value. This value will be a reference for making plans to increase cyber resilience, where the domain that gets the highest score will be implemented first. The highest priority domains are the Risk Management and Control Management domains. The head of the relevant unit is the decision-maker for this priority outcome. They feel that this domain is critical and must be improved immediately.

DISCUSSION

Therefore, the remaining domains will be completed after the two highest-rated domains are completed. This research also has an output, namely a plan to increase cyber resilience at University XYZ. This plan can increase cyber resilience by implementing several incomplete or not carried out practices. Thus, the plans will contain incomplete or not carried out practices, along with guidelines for implementing these practices. The guidelines are sourced

from documents issued by the Cyber Resilience Review. The following are recommendations for each domain from the assessment results carried out.

Asset Management

The asset management domain defines an organization's inventory of high-quality assets and how those assets are managed throughout their lifecycle to ensure continuous productivity that supports the company's critical services. Defines. CRR defines four broad asset categories: people, information, technology, and facilities. It is good to create an inventory and assign permissions and responsibilities to assets in this area. In addition, it needs to establish a relationship between assets and services. The established relationship must include confidentiality, integrity, and availability requirements for all assets and services. XYZ University also needs to manage its inventory by setting criteria for changing each asset and updating the description of each asset.

Controls Management

The control management domain focuses on how enterprises to plan, define, analyze, and evaluate internally implemented controls. This guide focuses on resilience management, enabling XYZ University to operate during critical times rather than financial management related to an organization's budget or ROI. XYZ University needs to set some unimplemented management goals for some assets, especially technology and equipment. XYZ Universities also need to protect their data from leaks, so XYZ Universities must implement critical data management. For good control management, it needs to control media, communication, and network limits in addition to data.

Configuration and Change Management

Configuration and change management is maintaining the integrity of the hardware, software, firmware, and documentation associated with the configuration and change management process. CCM is an ongoing process of controlling and approving changes to information resources or related technologies and infrastructure that support a company's critical services. This process involves adding new assets, modifying assets, and deleting assets. XYZ Universities need to assess the resilience requirements of each asset change. Equipment maintenance and repairs should be recorded promptly using approved and controlled methods to ensure proper configuration and change control. An asset structure baseline must also be established to provide the basis for change.

Vulnerability Management

Vulnerability management domains focus on the processes organization uses to identify, analyze, and manage vulnerabilities in critical service operating environments. When discussing vulnerabilities, discuss the characteristics or conditions that can make an entity (that is, the entire organization or part of it) vulnerable to risk if exploited by a threat (natural or artificial). CRR focuses on essential, organization-specific services. XYZ Universities need to prepare for activities to analyze and eliminate weaknesses. To help prepare for vulnerability

management, you need a standard set of tools or methods to detect malicious code in your assets. Next, XYZ Universities need to identify and analyze existing weaknesses. You can manage these vulnerabilities and address the causes of the vulnerabilities accordingly.

Incident Management

The process of recognizing, analyzing, responding to, and improving disruptive events is known as incident management. The purpose of incident management is to reduce the impact of catastrophic events. To achieve this goal, XYZ University establishes event detection and identification, triage, and event analysis processes to determine if an incident is ongoing, respond to it, and organize it. It may improve your ability to respond to future incidents.

Service Continuity Management

Service continuity planning is one of the more critical aspects of resilience management because it provides the process of responding to both natural and artificial catastrophic events. Business disruptions can occur regularly, ranging from those with minimal impact to those too great for XYZ University to fulfill its mission. XYZ University provides predefined procedures for maintaining critical operational processes under various adverse conditions, from minor malfunctions to severe incidents with service planning continuity. For example, a power outage during repair or a failure of an IT component may require manual resolution steps. Due to a data center failure or loss of a company or facility hosting critical services, XYZ University may need to restore business or IT operations elsewhere.

Risk Management

The field of risk management focuses on how XYZ Universities identify, analyze, and mitigate risks to influence the probability of risk occurrence and the impact of confusion. Risk management is a fundamental activity of any organization. It is practiced at all levels of the organization, from executives to individuals in the business unit. XYZ Universities need to manage different types of risks to maintain their effectiveness and achieve their goals. XYZ Universities need to develop strategies to identify, analyze, and mitigate risk. After developing the strategy, you can establish risk tolerance by focusing on risk management at XYZ University.

External Dependencies Management

Service, development, and manufacturing outsourcing have become part of the day-to-day business for many companies. Outsourcing allows you to use your professional skills and equipment at a lower cost than in-house options. The CRR EDM domain provides a way for organizations to identify and prioritize these external dependencies and focus on managing and maintaining those dependencies. This area aims to establish a process for managing the appropriate level of management to ensure the sustainability and protection of services and assets that rely on the actions of external agencies. University XYZ can identify and prioritize external dependencies on critical service processes. You can then identify and manage risks based on external dependencies. XYZ Universities must also manage the performance of external institutions.

Training and Awareness

Training and awareness focus on the processes that organizations use to plan identify, implement, and improve training and awareness to ensure they understand and meet their operational requirements and cyber resilience goals. XYZ Universities need to plan and carry out training and awareness-raising activities to educate employees about their role in cyber resilience issues and guidelines. Employees also receive special training to perform their role in managing cyber resilience at XYZ University. Training and awareness aim to raise the skills and awareness of essential service support roles.

Situational Awareness

At XYZ University, activities are underway to identify the situation to provide timely and accurate information about the current state of the operational process. Activities need to support communication with various internal and external stakeholders to meet essential service reliability requirements. This domain proactively finds and analyzes information, ensures immediate operational stability and security, and coordinates this information company-wide so that all organizational units operate under the same operational status. The purpose is to do. XYZ Universities need to monitor threats that could attack XYZ Universities. After that, information about the threat must also be communicated to the entire team.

4. CONCLUSION

Evaluations at University XYZ have been carried out on each cyber resilience domain. It can be seen from the research results that no domain reaches 100% performance. In addition, in each cybersecurity domain at University XYZ, no one has yet reached MIL1. This result is because many practices have not been carried out or are incomplete at University XYZ. The lack of management data at University XYZ is one of the reasons why the scores are low. The need to implement cyber resilience practices is a way for University XYZ to improve cyber resilience. Therefore, each domain has been prioritized for the next step in improving cyber resilience at University XYZ. Priority criteria have been set to assist the priority process, namely organizational goals, business goals, and resource availability, on a scale of 1-5. Furthermore, each domain is also given an improvement recommendation that contains a complete program guide and additional references from the cybersecurity and resilience framework. Thus, University XYZ can implement cyber resilience practices according to priorities so that the implementation process can run optimally, even though cyber threats occur from time to time.

5. REFERENCES

Adianto, T., Ali, Y., & Saptono, E. (2020). Penilaian Risiko Serangan Siber Sistem Manajemen Keamanan Informasi PT. UAV. *Manajemen Pertahanan,* 6(1), 52-72.

Alghamdi, W. N., & Rastogi, R. (2020). An efficient data flow material model (DFMM) for cyber security risk assessment in a real-time server. Materials Today: Proceedings.

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the Management of Cyber Resilience Systems. *Computers & Industrial Engineering*.

Arianto, A. R. (2017). Cyber Security: Geometri Politik dan Dimensi Pembangunan Keamanan Dunia Era Horizontal Abad 21. *Jurnal PIR, 1*(2), 108-118.

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). New contributions in information systems and technologies. In *Cyber resilience–fundamentals for a definition* (pp. 311-316). Cham: Springer.

Chang, L. Y., & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers & Security, 97*.

Choudhury, S., Rodriguez, L., Curtis, D., Oler, K., Nordquist, P., Chen, P.-Y., & Ray, I. (2015). Action Recommendation for Cyber Resilience. In Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense.

Cybersecurity and Infrastructure Security Agency. (2020). *Cyber Resilience Review: Method Description and Self-Assessment User Guide*. Carnegie Mellon University.

Hagen, J. (2018). Building resilience against cyber threats in the energy sector. *International journal of critical infrastructure protection, 20*, 26-27.

Haque, M. A., Shetty, S., & Krishnappa, B. (2019). ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control System. Washington DC: The 4th IEEE International Conference on Intelligent Data and Security.

Haque, M. A., Teyou, G. K., Shetty, S., & Krishnappa, B. (2018). Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights. IEEE.

Koelemeijer, D. (2018). Enhancing the Cyber Resilience of Critical Infrastructures through an Evaluation Methodology Based on Assurance Cases. Elsevier.

Linkov, I., & Kott, A. (2019). Cyber Resilience of Systems and Networks. In *Fundamental Concepts of Cyber Resilience: Introduction and Overview* (pp. 1-25). Cham: Springer.

NIAC. (2009). *Critical Infrastructure Resilience Final Report and Recommendations.* National Infrastructure Advisory Council.

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1 ed.). National Institute of Standards and Technology.

Perdani, M. D., Widyawan, & Santosa, P. I. (2018). Blockchain untuk keamanan transaksi elektronik perusahaan financial technology. Yogyakarta: Universitas AMIKOM Yogyakarta.

Rahmawati, I. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense. *Jurnal Pertahanan & Bela Negara, 7*(2), 51-66.

Rehak, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing the resilience of critical infrastructure elements. *International journal of critical infrastructure protection, 25*, 125-138.

Sep´ulveda-Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A Systematic Review of Cyber-Resilience Assessment Frameworks. *Computers & Security*.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards, and recommendations. *Future Generation Computer Systems,* 92, 178-188.

Tonhauser, M., & Ristvej, J. (2019). Disruptive Acts in Cyberspace, Steps to Improve Cyber Resilience at National Level. Slovak Republic: Elsevier.

Williams, P. A., & Manheke, R. J. (2010). Small Business - A Cyber Resilience Vulnerability. Perth Western Australia: Proceedings of the 1st International Cyber Resilience Conference.