INTENSIF, Vol.10 No.2 2026
ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v10i2.28354

Network Infrastructure Security Audit at a Vocational School Teaching Factory Using the NIST Cybersecurity Framework

Received:
29 January 2026
Accepted:
15 July 2026
Published:
22 August 2026

[1*]Maya Destriani, [2]Bintang Najarul Haq Mulyadi, [3]Tazkia Salsabila Ardan
[1,2,3]Information Systems, Universitas Subang , Indonesia
E-mail: [1]mayadestriani@unsub.ac.id,
[2]bintangnajarul08@gmail.com, [3]tazkiaardan@unsub.ac.id

*Corresponding Author

Abstract— **Background**: The increasing dependence on public-facing network services exposes educational institutions to growing cybersecurity threats, highlighting the need for structured security evaluations. This study evaluates cybersecurity maturity in a vocational school Teaching Factory (TEFA) environment using the NIST Cybersecurity Framework (NIST CSF) 1.1. **Objective:** To assess the cybersecurity maturity of the network infrastructure at TEFA TKJ SMK Al-Mufti, determine its implementation tier, and develop practical security improvements. **Methods:** A qualitative–quantitative descriptive case study was conducted using observations, interviews, questionnaires based on NIST CSF categories and subcategories, and document analysis. Risk assessment followed NIST SP 800-30, while gap analysis compared the Current Profile with a Target Profile defined at Tier 3 across the five NIST CSF core functions. **Results:** Although questionnaire results produced an average score of 3.45 (Tier 3), qualitative validation indicated that cybersecurity practices remained informal and inconsistently documented, resulting in an actual maturity level of Tier 2 (Risk Informed). A one-level gap was identified across all NIST CSF functions. Key risks included weak authentication, the absence of formal cybersecurity policies, and manual log monitoring. Implementing centralized log monitoring using Graylog improved visibility and strengthened the Detect and Respond functions. **Conclusion:** NIST CSF effectively identifies cybersecurity gaps and supports targeted improvements in educational network infrastructures. Further research should evaluate the long-term effectiveness of implemented controls and extend assessments to multiple institutions.

Keywords— NIST Cybersecurity Framework; Network Security Audit; Cybersecurity Maturity; Centralized Log Monitoring; Educational Network Infrastructure

Corresponding Author:

Maya Destriani,
Departmen of Information Systems,
Universitas Subang,
Email: mayadestriani@unsub.ac.id
Orchid ID: https://orcid.org/0009-0003-0162-4034

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v10i2.28354

I. INTRODUCTION

The rapid advancement of information technology has significantly influenced various sectors, particularly education. Computer network infrastructure has become a critical component in supporting administrative activities, learning processes, data management, and digital services. The increasing reliance on internet-based services requires robust network security to ensure operational continuity, data protection, and service availability. Without adequate security mechanisms, network infrastructures are vulnerable to cyber threats that may disrupt educational activities and compromise sensitive information [1].

Teaching Factory (TEFA) TKJ SMK Al-Mufti is a school-based production unit specializing in computer and network technology. In addition to serving as a practical learning facility, TEFA operates a public internet service based on the RT/RW Net model under the name Smafti NET. This service extends network access beyond the school environment to the surrounding community, thereby increasing exposure to external threats. The use of public IP addresses further elevates security risks, including port scanning, brute force attacks, and malware propagation, as reported in prior cybersecurity studies [2].

Observations indicate that the existing security system at TEFA TKJ SMK Al-Mufti relies primarily on basic firewall configurations without centralized monitoring. The absence of log management systems, Intrusion Detection Systems (IDS), and automated alert mechanisms reduces the organization's ability to detect and respond to threats effectively. Similar limitations have been identified in other educational and organizational environments, where inadequate security controls lead to delayed incident detection and response [3][4].

Several recent studies have applied the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) to assess and improve cybersecurity maturity. Ratih Windari examined the implementation of NIST CSF in vocational schools, focusing on awareness and adoption aspects [5]. Handoyo and Nigrum [4] assessed cybersecurity risks in a university environment but emphasized primarily the Identify function. Putri et al. [6] combined NIST CSF with ISO/IEC 27001:2013 to conduct information security risk management in a government institution. Meanwhile, González-Granadillo et al. discussed the role of Security Information and Event Management (SIEM) in critical infrastructures, particularly related to the Detect and Respond functions of NIST CSF [7]. However, most of these studies focus on partial implementation of NIST CSF or combine it with other frameworks, and limited research has conducted a comprehensive audit of all five NIST CSF functions in a vocational school Teaching Factory environment that operates public internet services.

INTENSIF, Vol.10 No.2 2026
ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v10i2.28354

The difference between this research and previous research is that this study performs a holistic cybersecurity audit covering all five core functions of NIST CSF: Identify, Protect, Detect, Respond, and Recover, specifically within a Teaching Factory environment that manages public-facing network services. Furthermore, this study integrates quantitative assessment with qualitative validation to reveal discrepancies between perceived and actual cybersecurity maturity.

The purpose of this research is to evaluate the cybersecurity maturity of network infrastructure at TEFA TKJ SMK Al-Mufti using NIST CSF version 1.1, determine the current implementation tier, and provide practical recommendations to improve network security. This study adopts NIST CSF version 1.1 instead of the newer version 2.0 because version 1.1 remains widely implemented and provides a stable and well-established structure for assessing cybersecurity maturity, particularly in operational environments. Additionally, version 2.0 introduces the new "Govern" function, which focuses more on organizational governance and strategic policy aspects. Since this study emphasizes technical and operational evaluation of network infrastructure, version 1.1 is considered more suitable and aligned with the research objectives. The objectives of this study are to assess the current condition of network infrastructure security, determine the level of security implementation based on NIST CSF implementation tiers, and provide practical and applicable recommendations for improving network security [8]. The results of this study are expected to contribute to improving cybersecurity practices in educational institutions, particularly those managing public-facing network services, and to enrich academic references related to cybersecurity audits using standardized frameworks.

II. RESEARCH METHOD

A. Research Design and Approach

This study employed a qualitative [9]-quantitative descriptive [10] approach using a case study method to audit the security of network infrastructure at Teaching Factory (TEFA) TKJ SMK Al-Mufti. The research design focused on evaluating the current condition of network security controls and their level of implementation by applying the NIST Cybersecurity Framework (CSF) version 1.1, a framework developed by the National Institute of Standards and Technology (NIST) to guide organizations in managing cybersecurity risks and integrating them into organizational risk management processes [11]. The audit approach was selected to systematically assess governance, technical controls, and risk management practices in an educational network environment.

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v10i2.28354

B. Research Object and Scope

The object of this research was the network infrastructure managed by TEFA TKJ SMK Al-Mufti, including routers, switches, access points, servers, bandwidth management mechanisms, and security configurations. The scope of the study was limited to the evaluation of network security controls based on the five core functions of NIST CSF: Identify, Protect, Detect, Respond, and Recover [12].

Fig 1. Cybersecurity Framework Version 1.1

In contrast, COBIT 2019 (Control Objectives for Information and Related Technology), developed by the Information Systems Audit and Control Association (ISACA), primarily emphasizes information technology governance and management. COBIT provides extensive guidelines for aligning business objectives, risk management, audit requirements, and technical controls within an organization [13]. COBIT 2019 also introduces the Goal Cascade mechanism, which enables the transformation of stakeholder needs into enterprise goals and prioritized governance objectives. This approach supports the identification of priority IT governance domains by aligning organizational strategies with risk management and control requirements [14]. While COBIT 2019 is widely used for IT governance assessments [15], this study focuses specifically on network infrastructure security; therefore, NIST CSF is considered more suitable as the primary framework.

The application of NIST CSF enables organizations, particularly within the public and educational sectors, to assess their cybersecurity posture, identify gaps in existing controls, and enhance resilience against cyber threats. This approach supports service reliability and ensures the protection of critical data assets [16].

C. Subjects and Participants

The observed participants consisted of individuals directly involved in managing and operating the network infrastructure at TEFA TKJ SMK Al-Mufti. These included network

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v10i2.28354

administrators, IT support staff, and teaching personnel responsible for network operations. Participants were selected using purposive sampling [17]based on their roles, responsibilities, and direct involvement in network management. This selection ensured that the collected data accurately reflected the actual implementation of network security practices.

D. Data Collection Techniques

Data were collected using multiple techniques to ensure validity and triangulation:

1. Observation, conducted by examining network devices, configurations, and existing security mechanisms [18].
2. Interviews, carried out with key personnel to obtain information regarding security policies, procedures, and incident handling practices [19].
3. Questionnaires, developed based on NIST CSF categories and subcategories[20], using a Likert scale to measure the level of security implementation[21].
4. Document analysis, including network configuration files, security policies, and operational documentation ([22][23]).

E. Measurement Instruments and Variables

The primary variables measured in this study were the level of implementation of network security controls and the security maturity level[24]. Measurement indicators were derived from NIST CSF categories and subcategories. A five-point Likert scale was used, ranging from *not implemented* to *fully implemented*, allowing both qualitative and quantitative evaluation of security practices [25].

To map the quantitative Likert-scale results (1–5) to the NIST CSF Implementation Tiers (1–4), a normalization approach was applied. The average score obtained from the questionnaire was converted into maturity levels using the following interval classification:

Table 1. Mapping Likert → NIST Tier

Likert Score Range	Implementation Category	NIST CSF Tier
1,00 – 1,99	Cybersecurity practices are ad hoc and reactive	Tier 1 (Partial)
2,00 – 2,99	Cybersecurity practices are risk-informed	Tier 2 (Risk Informed)
3,00 – 3,99	Cybersecurity practices are defined and repeatable	Tier 3 (Repeatable)
4,00 – 5,00	Cybersecurity practices are adaptive and continuously improved	Tier 4 (Adaptive)

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v10i2.28354

F. Risk Assessment Method

Risk assessment was conducted using NIST Special Publication 800-30 Revision 1 as a reference framework. The assessment followed four stages: preparation, risk identification and analysis, communication of results, and maintenance of assessment results [26]. Risks were evaluated based on likelihood and impact, each scored on a scale of 1 to 5. The overall risk score was calculated using the formula:

$$\textit{Risk Score} = \textit{Likelihood} \times \textit{Impact}$$

Risk levels were then classified into low, medium, and high categories to prioritize security controls using a risk-based selection approach [27].

G. Gap Analysis Technique

A gap analysis was conducted by comparing the Current Profile and Target Profile defined in NIST CSF. This comparison identified discrepancies between existing security practices and the expected standard. The results of the gap analysis were used to determine priority areas for improvement and to formulate security enhancement recommendations [28].

H. Data Analysis Method

Quantitative data obtained from questionnaires were analyzed using descriptive statistical methods, including mean score calculations and categorization of implementation levels. Qualitative data collected through interviews and observations were examined using thematic analysis to support and interpret the quantitative results. The overall security maturity level was determined by mapping the findings to the NIST CSF Implementation Tiers, ranging from Tier 1 (Partial) to Tier 4 (Adaptive). Accordingly, this study is limited to evaluating network infrastructure security based on the five core functions of the NIST Cybersecurity Framework and determining the security maturity level using the Implementation Tiers, without addressing broader organizational governance aspects beyond the TEFA network environment [29]. Non-network information systems outside the TEFA environment were not included in this study

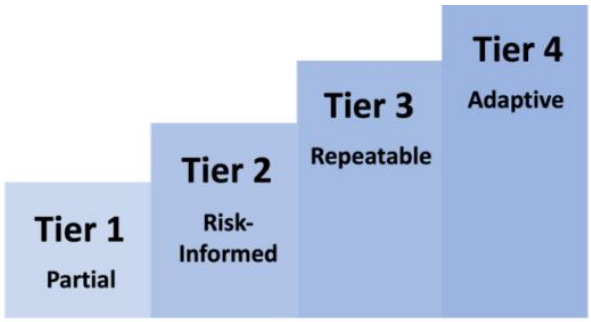

Fig 2. CSF Tiers for cybersecurity risk governance and management

INTENSIF, Vol.10 No.2 2026
ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v10i2.28354

I. Research Procedure

The research procedure consisted of the following steps:

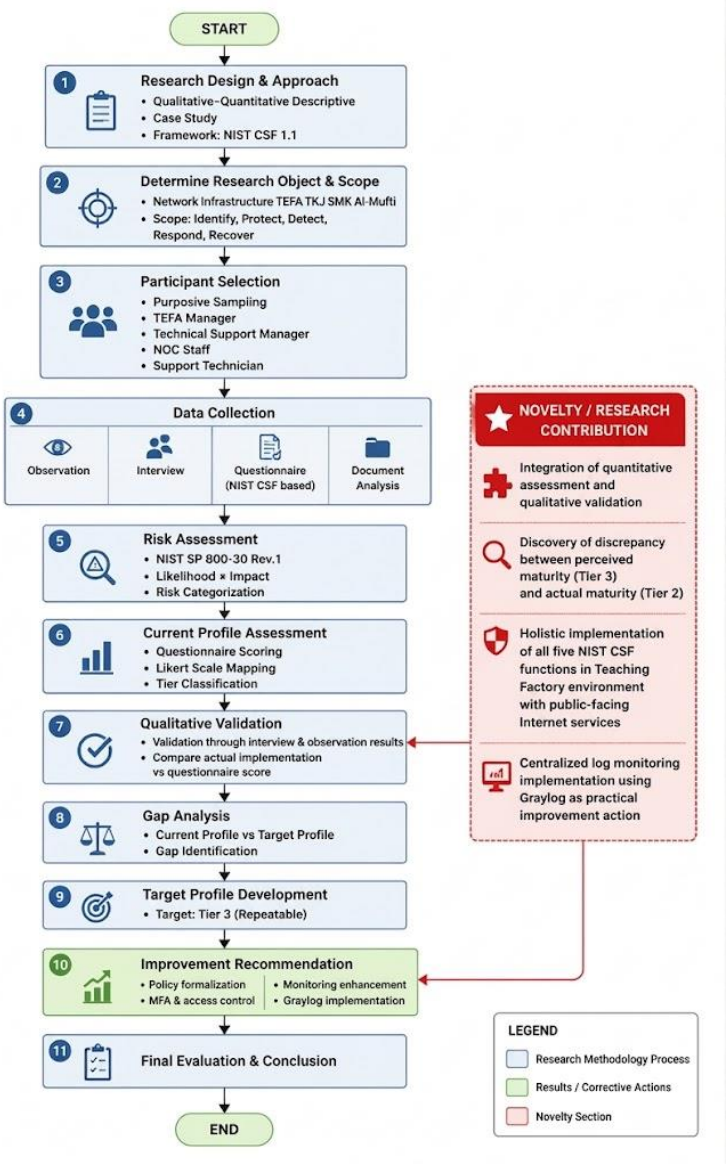

Fig 3. Research Procedure

III. RESULT AND DISCUSSION

A. Prioritize and Scope

The Prioritize and Scope stage aims to determine the focus and scope of the cybersecurity audit based on the level of risk faced by the organization. In this study, this stage was conducted to map the network security condition of TEFA TKJ SMK Al-Mufti by considering critical assets, potential threats, and existing security controls.

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v10i2.28354

Data obtained from observations and interviews were analyzed using a risk-based selection approach. This approach was applied to interpret the collected information and provide an overview of the actual network security condition. The results of the risk analysis were then used to identify and prioritize the most relevant categories and subcategories of the NIST Cybersecurity Framework (CSF) version 1.1, ensuring that the evaluation of the five core functions-Identify, Protect, Detect, Respond, and Recover-was conducted objectively based on actual risk levels.

The analysis identified several critical assets, including Mikrotik routers, Optical Line Terminal (OLT), wireless backhaul devices, managed switches, access points, local servers, and network configuration data. Risk evaluation was performed by assessing likelihood and impact on a scale of 1–5, with the risk level calculated as the product of both values. Assets with high risk scores, particularly core network devices and backbone infrastructure, were prioritized for further evaluation.

Based on the risk assessment results, relevant NIST CSF categories and subcategories were selected, focusing on asset management, governance, risk assessment, access control, data protection, continuous monitoring, incident response, and recovery planning. This prioritization ensured that the audit concentrated on areas with the most significant potential impact on network availability, integrity, and confidentiality.

Overall, the application of risk analysis at the Prioritize and Scope stage enabled a focused, measurable, and contextual audit process. This approach ensured that the evaluation of network security at TEFA TKJ SMK Al-Mufti was efficient, objective, and aligned with the organization's actual cybersecurity risks, forming a solid foundation for subsequent assessment stages and improvement recommendations.

B. Orient

The Orient stage was conducted to understand the operational context, organizational structure, and current condition of the network infrastructure at TEFA TKJ SMK Al-Mufti. This stage focused on identifying the relationship between critical assets, business processes, and existing security controls to ensure that the audit was aligned with the actual technological environment.

TEFA TKJ SMK Al-Mufti operates as a practice-oriented unit providing computer and network services, supported by integrated infrastructure consisting of Mikrotik routers, OLT, point-to-point wireless links, managed switches, access points, local servers, and network configuration data. These assets play a vital role in supporting both project-based learning activities and service operations, making their security essential for operational continuity.

The results of the previous risk evaluation were mapped to operational processes to identify critical assets with the highest impact on service availability, particularly core network and

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v10i2.28354

backbone devices. The evaluation showed that basic security controls such as firewalls, authentication, backups, and physical protection were implemented, while centralized monitoring, VLAN segmentation, and security awareness remained partially implemented.

Identified risks were categorized into technical, physical, and human factors, with technical and human-related risks being the most dominant. This stage provided the foundation for developing the Current Profile and determining appropriate mitigation strategies in subsequent NIST CSF assessment stages.

C. Create a Current Profile

The Current Profile was developed using a mixed-method approach. Five participants were selected via purposive sampling based on RACI roles (managerial and technical). Based on the RACI (Responsible, Accountable, Consulted, Informed) mapping, the roles and responsibilities of participants in network security management were clearly identified. The mapping results indicate that a total of 5 participants were involved in this study, consisting of:

- 1 TEFA Manager, acting as the primary decision-maker and accountable authority for network security policies
- 1 Technical Support Manager, responsible for overseeing the implementation and control of technical security mechanisms
- 1 Network Operations Center (NOC) staff, serving as the core operator for network monitoring, log analysis, and anomaly detection
- 2 Support personnel (Support NOC and Field Technician), directly involved in incident handling and physical network maintenance

Data were collected using 26 NIST CSF-based questionnaire items with a 5-point Likert scale. Based on numerical mapping, this score corresponds to Tier 3 (Repeatable).

Table 2. Tier Result

NIST CSF	Avg Score	Implementasi (Tier)
Identify	3,6	Tier 3 (*Repeatable*)
Protect	3,1	Tier 3 (*Repeatable*)
Detect	3,5	Tier 3 (*Repeatable*)
Respond	3,03	Tier 3 (*Repeatable*)
Recover	4,05	Tier 4 (*Adaptive*)
Avg Score	**3,45**	**Tier 3 (*Repeatable*)**

The quantitative result shows an average score of 3.45 (Tier 3 – Repeatable) across all functions. However, qualitative validation revealed that practices were informal, undocumented, and

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v10i2.28354

inconsistently applied. Thus, the actual maturity level is more accurately classified as Tier 2 (Risk Informed), indicating awareness of risks but lacking standardized procedures and governance.

D. Conduct a Risk Assessment

The risk assessment was conducted in accordance with NIST CSF 1.1 and NIST SP 800-30 to identify, analyze, and prioritize cybersecurity risks affecting TEFA TKJ SMK Al-Mufti's network infrastructure. Critical assets—including routers, switches, OLT, wireless links, configuration files, backups, and monitoring systems—were evaluated against identified threats and vulnerabilities. Key threats involved malware, brute-force attacks on public IP access, misconfiguration, hardware failure, and power disruption, while major vulnerabilities included weak passwords, irregular updates, lack of formal security policies, manual log monitoring, limited security training, and the absence of multi-factor authentication. Risk levels were determined using impact and likelihood scoring, revealing high risks related to weak authentication and missing cybersecurity policies, with medium risks associated with monitoring, updates, and human factors. Mitigation priorities focus on strengthening technical controls, formalizing cybersecurity governance, and improving personnel awareness to reduce risk exposure and support progression toward Tier 3 (Repeatable).

E. Create a Target Profile

The Target Profile was developed to define the desired cybersecurity posture of TEFA TKJ SMK Al-Mufti and to serve as a benchmark for gap analysis against the current condition. This profile represents the ideal state of network security to be achieved in order to enhance service availability, prevent security incidents, and ensure sustainable network operations. The Target Profile supports strategic decision-making by prioritizing security improvements based on risk severity and operational impact.

Scope of the Target Profile

The scope of the Target Profile was determined based on the results of the risk assessment, which identified critical weaknesses in authentication mechanisms, the absence of formal cybersecurity policies, irregular system updates, and non-automated log monitoring. Accordingly, the Target Profile prioritizes strengthening authentication controls, formalizing cybersecurity governance, improving centralized monitoring and anomaly detection, and enhancing personnel cybersecurity awareness. Network infrastructure management—including IP addressing, VLAN segmentation, firewall configuration, and configuration management—was also included to improve overall network resilience. All scope elements were aligned with the five core functions of NIST CSF 1.1: Identify, Protect, Detect, Respond, and Recover.

INTENSIF, Vol.10 No.2 2026
ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v10i2.28354

Risk-Based Security Priorities

High-priority risks were associated with weak credential management, lack of formal cybersecurity policies, and limited monitoring capabilities. Medium-priority risks involved insufficient security awareness, incomplete network segmentation, and inconsistent backup practices. These risks were translated into targeted mitigation priorities focusing on technical controls (e.g., MFA, firewall hardening, automated monitoring), managerial controls (formal policies and SOPs), and human factors (regular security training).

Target Security Posture Based on NIST CSF

The Target Profile aims to achieve Tier 3 (Repeatable) maturity across all NIST CSF functions.

1. Identify: Assets, configurations, and risks are documented, periodically reviewed, and supported by formal governance and defined responsibilities.
2. Protect: Strong access controls, role-based access, encrypted data handling, routine training, secure configurations, and comprehensive logging are consistently applied.
3. Detect: Network traffic and logs are monitored in real time using integrated systems, with automated alerts and structured incident detection processes.
4. Respond: Formal incident response procedures are documented, communicated, and executed consistently, including analysis, mitigation, and internal coordination.
5. Recover: Recovery plans are defined and tested, supported by secure backups, structured communication, and post-incident evaluations to enable continuous improvement.

Overall, the Target Profile reflects a structured, risk-informed, and repeatable cybersecurity approach tailored to the operational context of TEFA TKJ SMK Al-Mufti, providing a clear roadmap for improving network security maturity in alignment with NIST CSF 1.1.

F. Determine, Analyze, and Prioritize Gaps

Gap analysis shows that the organization is at Tier 2, while the target is Tier 3, resulting in a uniform gap of one level across all functions.

Key gaps include:

- Lack of formal policies and governance
- Inconsistent access control
- Limited monitoring and detection
- Absence of structured incident response

Although the gap appears uniform, this is partly due to score aggregation. Qualitative findings reveal variation at the subcategory level, where some controls are more mature than others. Thus, the gap reflects both methodological aggregation and actual distributed weaknesses.

The findings of this research are that although quantitative assessment indicates Tier 3 maturity, qualitative validation reveals the actual level is Tier 2, characterized by informal and inconsistent

INTENSIF, Vol.10 No.2 2026
ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v10i2.28354

practices. The results of this research are in line with or supported by prior studies showing that self-assessment tends to overestimate cybersecurity maturity without formal governance, documentation, and continuous monitoring [30], [31].

G. Implementation Action Plan

Based on the identified gaps, a risk-based action plan was developed to support progression from Tier 2 to Tier 3. Improvements include policy formalization, strengthened access control, regular risk assessment, training, and structured incident management.

The primary focus was the implementation of centralized log monitoring using Graylog to address weaknesses in the Detect function. Logs from network devices were integrated via Syslog into a centralized system for real-time monitoring and analysis.

System evaluation shows improved visibility and anomaly detection. A monitoring SOP was developed to ensure consistent and repeatable operations. Overall, this implementation strengthens the Detect and Respond functions and provides a practical roadmap for improving cybersecurity maturity.

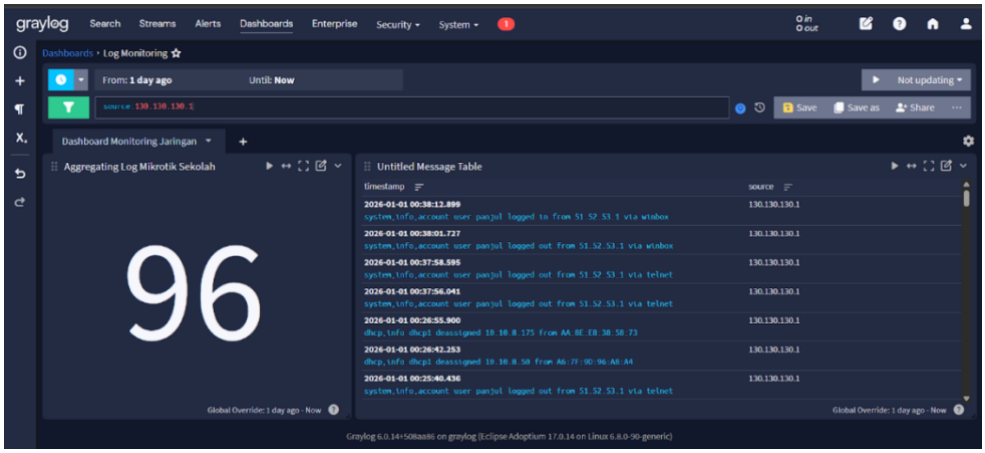

Fig 4. Dashboard Monitoring

IV. CONCLUSION

This study demonstrates that the application of the NIST Cybersecurity Framework (CSF) version 1.1 provides an effective and structured approach for evaluating and improving network infrastructure security within a vocational school Teaching Factory environment that operates public-facing internet services. The assessment confirms that while TEFA TKJ SMK Al-Mufti has established basic cybersecurity awareness and implemented several technical controls, the absence of standardized documentation, consistent procedures, and integrated monitoring limits the overall effectiveness of its security management.

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v10i2.28354

By mapping the existing security condition to NIST CSF Implementation Tiers, this research establishes that the organization's actual cybersecurity maturity aligns more accurately with Tier 2 (Risk Informed), rather than higher maturity levels suggested by quantitative scores alone. This finding highlights the importance of combining quantitative measurements with qualitative validation to obtain a realistic representation of cybersecurity maturity.

The implementation of a risk-driven action plan, particularly through centralized log monitoring using Graylog, demonstrates a practical pathway to strengthening the Detect and Respond functions and reducing reliance on manual and reactive security practices. This approach contributes to improved visibility, earlier anomaly detection, and more structured incident handling, supporting the transition toward Tier 3 (Repeatable) cybersecurity maturity.

From a broader scientific and engineering perspective, this study contributes to the field of cybersecurity engineering by demonstrating the applicability of NIST CSF in educational network infrastructures with real-world service exposure. The findings reinforce the value of integrating risk assessment, maturity evaluation, and actionable technical improvements to achieve sustainable cybersecurity enhancement. This research provides a replicable reference model for similar educational institutions seeking to align network security practices with internationally recognized standards while addressing operational and resource constraints.

Author Contributions. *Maya Destriani*: Contributed to conceptualization, research design and methodology, supervision, and manuscript preparation including writing, review, and editing. *Bintang Najarul Haq Mulyadi*: responsible for software implementation, field investigation, data collection, data curation, and drafting the original manuscript. *Tazkia Salsabila Ardan*: contributed to investigation support, data curation, and validation of research findings.

Funding: This research received publication support from the Directorate General of Research and Development, Ministry of Higher Education, Science, and Technology of the Republic of Indonesia, through the Journal Publication Assistance Program 2025. No specific research grant was provided for the conduct of this study**.**

Conflicts of Interest: The authors declare no conflict of interest.

Data Availability: The data supporting the findings of this study are available from the corresponding author upon reasonable request. Due to institutional policies and the need to protect the privacy and security of the network infrastructure and participants involved, the data are not publicly available.

Informed Consent: Informed consent was obtained from all participants involved in the study. A detailed explanation of participant selection and data collection procedures is provided in the Methods section.

Animal Subjects: There were no animal subjects involved in this research.

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v10i2.28354

ORCID:
Maya Destriani: https://orcid.org/0009-0003-0162-4034
Bintang Najarul Haq Mulyadi: https://orcid.org/0009-0009-6081-2856
Tazkia Salsabila Ardan: https://orcid.org/0000-0001-5436-1352

REFERENCES

[1] N. O. Miracle, "The Importance Of Network Security In Protecting Sensitive Data And Information," International Journal Of Research And Innovation In Applied Science, Vol. Ix, No. Vi, Pp. 259–270, 2024, Doi: 10.51584/Ijrias.2024.906024.

[2] Muhammad Rifqi Maulana And Abdul Kholiq, "Analisis Dan Implementasi Keamanan Jaringan Mikrotik Dengan Metode Ip Filtering Dan Port Knockiing (Studi Kasus Barokah.Net)," Jurnal Limits, Vol. 19, No. 02, Pp. 71–80, Feb. 2023, Doi: 10.59134/Jlmt.V19i02.199.

[3] F. Panjaitan And A. Aprilo, "Analisis Manajemen Risiko Keamanan Jaringan Menggunakan Framework Nist," Jurnal Ilmiah Matrik, Vol. 24, No. 1, Pp. 71–81, Apr. 2022, Doi: 10.33557/Jurnalmatrik.V24i1.1682.

[4] E. Handoyo And Izza Eka Nigrum, "Penilaian Risiko Keamanan Siber Kampus Menggunakan Framework Cybersecurity Nist 1.1," Jurnal Coscitech (Computer Science And Information Technology), Vol. 4, No. 3, Pp. 677–685, Jan. 2024, Doi: 10.37859/Coscitech.V4i3.5628.

[5] R. Windari And Sriyanto, "Tinjauan Implementasi National Institute Of Standards And Technology (Nist) Dalam Meningkatkan Keamanan Jaringan Dengan Cybersecurity Framework (Csf) : Studi Kasus Smkn4 Bandar Lampung," Jurnal Ilmu Komputer, Sistem Informasi, Teknik Informatika, Vol. 3, No. 1, Pp. 27–40, Mar. 2024.

[6] T. S. Putri, N. M. Mutiah, And D. P. Prawira, "Analisis Manajemen Risiko Keamanan Informasi Menggunakan Nist Cybersecurity Framework Dan Iso/Iec 27001:2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat)," Coding Jurnal Komputer Dan Aplikasi, Vol. 10, No. 02, P. 237, Oct. 2022, Doi: 10.26418/Coding.V10i02.54972.

[7] G. González-Granadillo, S. González-Zarzosa, And R. Diaz, "Security Information And Event Management (Siem): Analysis, Trends, And Usage In Critical Infrastructures," Sensors, Vol. 21, No. 14, P. 4759, Jul. 2021, Doi: 10.3390/S21144759.

[8] A. Ibrahim, C. Valli, I. Mcateer, And J. Chaudhry, "A Security Review Of Local Government Using Nist Csf: A Case Study," J. Supercomput., Vol. 74, No. 10, Pp. 5171–5186, Oct. 2018, Doi: 10.1007/S11227-018-2479-2.

[9] R. Safarudin, Zulfamanna, M. Kustati, And N. Sepriyanti, "Penelitian Kualitatif," Innovative: Journal Of Social Science Research, Vol. 3, No. 2, Pp. 9680–9694, 2023.

[10] J. L. Sidel, R. N. Bleibaum, And K. W. C. Tao, "Quantitative Descriptive Analysis," In Descriptive Analysis In Sensory Evaluation, Wiley, 2018, Pp. 287–318. Doi: 10.1002/9781118991657.Ch8.

[11] M. P. Barrett, "Framework For Improving Critical Infrastructure Cybersecurity, Version 1.1," Gaithersburg, Md, Apr. 2018. Doi: 10.6028/Nist.Cswp.04162018.

[12] J. L. Salas-Riega, Y. Riega-Virú, M. Ninaquispe-Soto, And J. M. Salas-Riega, "Cybersecurity And The Nist Framework: A Systematic Review Of Its Implementation And Effectiveness Against Cyber Threats," International Journal Of Advanced Computer Science And Applications, Vol. 16, No. 6, 2025, Doi: 10.14569/Ijacsa.2025.0160672.

[13] Z. Illési, "Digital Evidence Management For Organizational Legal Compliance," Interdisciplinary Description Of Complex Systems, Vol. 23, No. 3, Pp. 217–229, 2025, Doi: 10.7906/Indecs.23.3.3.

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v10i2.28354

[14] M. Destriani And Y. H. Putra, "Rencana Audit Tata Kelola Sistem Informasi Di Universitas Subang Menggunakan Framework Cobit 2019," Jurnal Tata Kelola Dan Kerangka Kerja Teknologi Informasi, Vol. 9, No. 1, Pp. 19–33, May 2023, Doi: 10.34010/Jtk3ti.V9i1.9164.

[15] R. Ramadhana, B. V. Izaac, G. W. Tangka, And J. Y. Mambu, "Information Technology Governance Analysis Using The Cobit 2019 Framework At Pt. Daya Adicipta Wisesa," Jurnal Informasi Dan Teknologi, Pp. 141–146, Nov. 2023, Doi: 10.60083/Jidt.V5i3.414.

[16] M. Fadya And D. N. Utama, "Towards Secure Information Systems: Developing And Implementing An Information Security Evaluation Model Using Nist Csf And Cobit 2019," Tem Journal, Pp. 182–191, Feb. 2025, Doi: 10.18421/Tem141-17.

[17] R. Ksanjaya And E. T. Rahayu, "Motivasi Siswa Dalam Kegiatan Ekstrakurikuler Futsal Di Sma Negeri 1 Blanakan," Jurnal Pendidikan Dan Konseling, Vol. 4, No. 5, Pp. 6094–6099, 2022.

[18] Y. Thomas, H. Debar, And B. Morin, "Improving Security Management Through Passive Network Observation," In First International Conference On Availability, Reliability And Security (Ares'06), Ieee, 2006, Pp. 8 Pp. – 389. Doi: 10.1109/Ares.2006.74.

[19] C. Hove, M. Tarnes, M. B. Line, And K. Bernsmed, "Information Security Incident Management: Identified Practice In Large Organizations," In 2014 Eighth International Conference On It Security Incident Management & It Forensics, Ieee, May 2014, Pp. 27–46. Doi: 10.1109/Imf.2014.9.

[20] L. Bernardo, S. Malta, And J. Magalhães, "An Evaluation Framework For Cybersecurity Maturity Aligned With The Nist Csf," Electronics (Basel)., Vol. 14, No. 7, P. 1364, Mar. 2025, Doi: 10.3390/Electronics14071364.

[21] A. Joshi, S. Kale, S. Chandel, And D. Pal, "Likert Scale: Explored And Explained," Br. J. Appl. Sci. Technol., Vol. 7, No. 4, Pp. 396–403, Jan. 2015, Doi: 10.9734/Bjast/2015/14975.

[22] L.-F. Kwok, P. P. K. Fung, And D. Longley, "Security Documentation," In Advances In Information Security Management & Small Systems Security, Boston, Ma: Springer Us, 2001, Pp. 127–139. Doi: 10.1007/0-306-47007-1_10.

[23] T. S. Ardan, D. F. Zahra, F. R. Junaedi, And S. R. Widianto, "Dokumentasi Software Testing Berstandar Ieee 829-2008 Untuk Learning Management System Fakultas Ilmu Komputer Universitas Subang," Jurnal Multinetics, Vol. 6, No. 2, Pp. 179–191, Jan. 2020, [Online]. Available: Www.Publishing.Gramediana.Com.

[24] C. Schmitz, M. Schmid, D. Harborth, And S. Pape, "Maturity Level Assessments Of Information Security Controls: An Empirical Analysis Of Practitioners Assessment Capabilities," Comput. Secur., Vol. 108, P. 102306, Sep. 2021, Doi: 10.1016/J.Cose.2021.102306.

[25] I. Kusmaryono, D. Wijayanti, And H. R. Maharani, "Number Of Response Options, Reliability, Validity, And Potential Bias In The Use Of The Likert Scale Education And Social Science Research: A Literature Review," Int. J. Educ. Method., Vol. 8, No. 4, Pp. 625–637, Nov. 2022, Doi: 10.12973/Ijem.8.4.625.

[26] M. Al Fikri, F. A. Putra, Y. Suryanto, And K. Ramli, "Risk Assessment Using Nist Sp 800-30 Revision 1 And Iso 27005 Combination Technique In Profit-Based Organization: Case Study Of Zzz Information System Application In Abc Agency," Procedia Comput. Sci., Vol. 161, Pp. 1206–1215, 2019, Doi: 10.1016/J.Procs.2019.11.234.

[27] I. D. Sánchez-García, J. Mejía, And T. San Feliu Gilabert, "Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, And Validation," Applied Sciences, Vol. 13, No. 1, P. 395, Dec. 2022, Doi: 10.3390/App13010395.

[28] F. N. Sitorus And R. Harwahyu, "Analysis Of Employee Capacity Gap In Managing Network Security And Its Implementation Towards Insider Threat Prevention," Malcom: Indonesian Journal Of Machine Learning And Computer Science, Vol. 5, No. 2, Pp. 635–644, Apr. 2025, Doi: 10.57152/Malcom.V5i2.1878.

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v10i2.28354

[29] National Institute Of Standards And Technology, "The Nist Cybersecurity Framework (Csf) 2.0," Feb. 2024. Doi: 10.6028/Nist.Cswp.29.

[30] N. Chaiwut And W. Rueangsirarak, "M-Ses: An Online Cybersecurity Self-Evaluation System To Mitigate The Risk Of Cybersecurity Attacks In Thailand," Science, Engineering And Health Studies, P. 25020008, Dec. 2025, Doi: 10.69598/Sehs.19.25020008.

[31] M. N. Y. Marican, S. A. Razak, A. Selamat, And S. H. Othman, "Cyber Security Maturity Assessment Framework For Technology Startups: A Systematic Literature Review," Ieee Access, Vol. 11, Pp. 5442–5452, 2023, Doi: 10.1109/Access.2022.3229766.