Implementing NIST Framework and the People, Process, Technology approach in Indonesian Financial Services

Ferdynandus
Universitas Multimedia Nusantara, Tangerang, Indonesia
Johny Natu Prihanto
Universitas Multimedia Nusantara, Tangerang, Indonesia
Winarno
Universitas Multimedia Nusantara, Tangerang, Indonesia

Abstract: A financial services company in Indonesia was implementing digital transformation with various strategies. Regulators such as the Financial Services Authority have stipulated that financial services companies must ensure effective data security and smooth internal operations to counter evolving cybersecurity threats. The Gap Analysis results show that the Roadmap and Solution development will be focused starting from the Identify dimension of the NIST Framework, specifically in the asset management category. This research also uses a post-positivist paradigm with a mixed methods approach, which combines qualitative and quantitative research methods. This research will adopt two Digital Maturity Models. by considering the complementary elements of the two models, to create a Framework that is more holistic and in accordance with the specific needs of the organization. The benefit of this research is the development of a framework based on the NIST Cybersecurity Framework and Profile for Ransomware Risk Management, which will be integrated with the PPT Framework (People, Process & Technology) which is expected to improve cybersecurity maturity, especially in dealing with ransomware risks.

Keywords: Asset Management, NIST Framework, Cyber Attack, Digital Transformation, Ransomware.

Correspondents Author:
Ferdynandus, Universitas Multimedia Nusantara, Tangerang, Indonesia
Email : ferdynandus1915@gmail.com

Received May 31, 2024; Revised July 6, 2024; Accepted July 13, 2024; Published July 16, 2024

Introduction

Digital transformation has become a trend that dominates various industries, including the financial sector, which is adopting advanced technologies to expand markets, improve services, reduce costs, and drive innovation. Various studies have been conducted to address the challenges arising from digital transformation. This research includes developing strategies to expand markets, improving services through the adoption of advanced technologies, reducing operational costs, and driving innovation in the financial sector , these efforts reflect how the financial industry is using digital transformation to remain competitive and relevant in a changing business environment (Sánchez-García et al., 2023). A financial services company in Indonesia was implementing digital transformation with various strategies. In May 2023, the company experienced a ransomware attack that required them to shut down key systems to protect their data and operations. Regulators such as the Financial Services Authority have stipulated that financial services companies must ensure effective data security and smooth internal operations to counter evolving cybersecurity threats (Calliess & Baumgarten, 2020). In a Ransomware attack, the attacker attempts to lock the victim's data using a strong encryption algorithm and demands a ransom (usually in the form of a Bitcoin payment) so that the victim can get the decryption key (Li & Liu, 2021). This results in temporary or in some cases, permanent loss of access to information, disrupts normal system operations, and incurs financial losses (Chang & Huang, 2023;Humayun et al., 2021). Personal data protection is a central aspect in the cyber security domain. Effective regulation and the establishment of personal data protection are crucial in maintaining the information security of every citizen. The history of the personal data protection reflects the development of a global awareness of the importance of individual privacy, which grows along with technological advancements (Seun Solomon Bakare et al., 2024). previous research addressed the challenges highlighted in NIST SP 1800-5 regarding IT asset management, focusing on issues such as poor IT asset visibility and inconsistent patch management practices. These challenges exacerbate the impact of cyberattacks, underscoring the critical need for better asset management strategies in improving cybersecurity resilience (Oluomachi et al., 2024). In contrast, Aras and Büyüközkan elaborate that typically digital maturity models cover various aspects of the digital transformation journey, such as strategy, governance, and other sub-dimensions (Aras & Büyüközkan, 2023). Schallmo (2021) in his book "Digitalization: Approaches, Case Studies, and Tools for Strategy, Transformation and Implementation" explains that digitalization involves various approaches, case studies, and tools to achieve success in strategy, transformation, and implementation. All these elements combine to achieve Digital Maturity.

This research will adopt two Digital Maturity Models. Combining the two Digital Maturity Models (DMMs) can be achieved by considering the complementary elements of the two models, to create a Framework that is more holistic and suited to the specific needs of the organization. The benefits of this research include the development of a framework based on the NIST Cybersecurity Framework and Profile for Ransomware Risk Management, which will be integrated with the PPT Framework (People, Process & Technology). The evaluation of this framework is expected to improve cybersecurity maturity, especially in dealing with ransomware risks. In addition, this project will provide operational and functional benefits, such as improved coordination and process effectiveness, as well as academic benefits for researchers through the development of knowledge and skills related to IT Asset Management and cyber security.

Literature Review

The CIA triad, which includes confidentiality, integrity, and availability, is a model used to implement information security policies within an organization. Threat modelling is a methodological approach that identifies potential threats during the early phases of system design, CIA implementation, and operationalization undertaken by an organization. In the context of IT asset management in companies operating in the financial sector in Indonesia, the use of the NIST framework has proven to provide a systematic and structured approach. According to the National Institute of Standards and Technology (NIST), this framework not only sets guidelines for information security, but also provides a solid foundation for overall IT asset management. The implementation of this framework covers not only the management of technology, but also the processes that govern the use of technology and the important role of the human aspect in managing and securing IT assets (Toussaint et al., 2024).

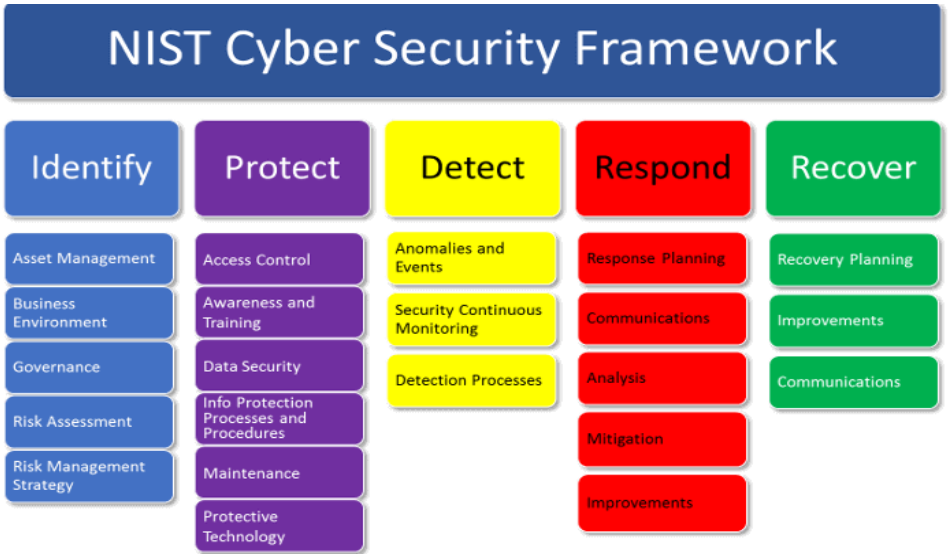

Figure 1 NIST Framework Core.

The People, Process, Technology (PPT) approach is also a key factor in the success of IT asset management in financial companies. The study emphasized the importance of balanced integration between policies and procedures (Process), employee expertise and skills (People), and supporting technology infrastructure (Technology) in ensuring the sustainability and effectiveness of IT asset management strategies. In the Indonesian context, financial firms face unique challenges in managing their IT assets, including strict regulatory compliance and improving preparedness for increasingly complex security threats. Successful implementation of the NIST framework and PPT approach can provide an integrated and sustainable solution to address these challenges. Solutions mitigating these various vulnerabilities and threats are then implemented to protect the underlying systems (Zahid et al., 2023). A study conducted by Yohanes and team (2021) revealed that the adoption of the NIST framework has become a strong foundation for financial companies in Indonesia in managing their IT assets. This framework not only helps in identifying, protecting, detecting, responding, and recovering IT assets, but also ensures alignment with increasingly stringent regulations in the financial sector. Successful implementation of the NIST framework is identified as key to improving overall security and operational efficiency (Ngamal & Maximus Ali Perajaka, 2021) . In addition, the People, Process, Technology (PPT) approach used in IT asset management is also the focus in the research conducted by Satrio et al. (2022). Cybersecurity governance refers to principles and is designed to protect digital assets and data (McIntosh et al., 2024). They emphasized the importance of integration between policies and procedures (Process), employee roles and skills (People), and appropriate technology infrastructure (Technology) to achieve the strategic goals of financial companies. Their results show that good coordination between these three components not only improves operational efficiency but also strengthens defences against increasingly complex security threats (Satrio Ronggo Buwono et al., 2022). The results of this literature consistently show that the integration of the NIST framework with the PPT approach is the key to meeting the complex challenges of IT asset management in Indonesia's dynamic and highly regulated business environment. This research not only provides an in-depth view of the practical application of the framework, but also provides a foundation for the development of strategies that are more adaptive and responsive to future technological and regulatory developments.

Research Method

The NIST Cybersecurity Framework was first developed by the National Institute of Standards and Technology (NIST) of the United States. The purpose of this framework is to provide guidance in implementing or improving cybersecurity programs in organizations. This framework is used to detect, reduce the impact of, and respond to cyber-attacks that may occur in the organization. The advantage of the NIST Cybersecurity Framework is its ease of use,

using clear and understandable language. It can also be integrated with an organization's existing cyberattack risk mitigation efforts (Cartwright et al., 2023). The core of the NIST Framework includes information on functions, categories, subcategories, and informative references that make the framework easy to use. The core framework provides recommended practices in the field of cybersecurity, both from a technical and managerial perspective. Tiers are used to assess the level of cybersecurity maturity that already exists in the organization, while Profiles serve to determine the current state of cybersecurity and the goals that the organization wants to achieve (Alqudhaibi et al., 2023).

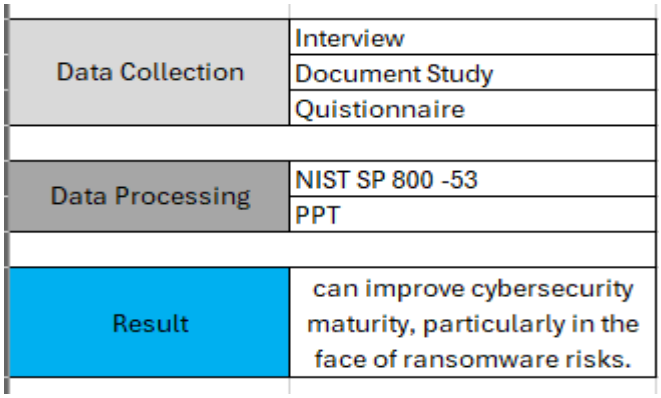

Figure 2 Process Flow of Research Methods

This framework is designed to help organizations achieve cybersecurity goals according to their needs, by combining elements such as Core, Tiers, and Profile. Thus, it is expected to help improve the organization's cybersecurity and achieve the set targets, see table 1 below.

Table 1. NIST Framework methodology categories

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identify Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Event
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Plaining
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements

RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Sample data was taken from 30 interviewees in the pretest stage. The data source used is primary data from 30 respondents within the population of internal employees of financial services companies. Respondents come from various departments such as Technology, Human Resources, Corporate Communications, General, and Finance. This research will use 30 variables related to the NIST Framework to measure the current state and future state. These variables will be included in a questionnaire consisting of 30 questions, each linked to 30 subcategories, 23 categories, and 5 dimensions of the NIST. Furthermore, these variables will be grouped into 3 PPT dimensions. The following is the relationship between the variables and the relevant subcategories, categories, and dimensions. After getting the results, the validation technique for the future state will be carried out. Future state validation techniques will be carried out using interview techniques. The interview technique is carried out to validate the expected conditions in the future. The interviews were conducted with several senior managers who are directly related to cybersecurity. Interviews are conducted to determine the expected maturity level.

Result and Discussion

A total of 30 respondents have participated in this data set. Most of them, 73.33% or 23 out of 30 respondents, are male with ages ranging from 28-43 years old, and work in the IT/Technology department. A total of 33.33% or 10 out of 30 respondents were from other departments in the organization. In terms of work experience, 40% or 12 respondents have more than 10 years of experience, indicating in-depth knowledge and senior positions. Meanwhile, 30% or 9 respondents have 5-10 years of experience, and another 30% or 9 respondents have less than 5 years of experience, reflecting a combination of mature experience and fresh ideas from new employees. In the context of female respondents, 10% or 3 out of 30 respondents have more than 10 years of experience, while 3.33% or 1 respondent has less than 5 years of experience. The female population in this data set represents a wide range of backgrounds. This method of measurement involves respondents who have relevant experience, especially related to Cyberattack incidents within financial services companies. The presence of respondents with more than 10 years of experience, both male and female, provides added value in the evaluation and planning of the company's long-term digital transformation strategy.

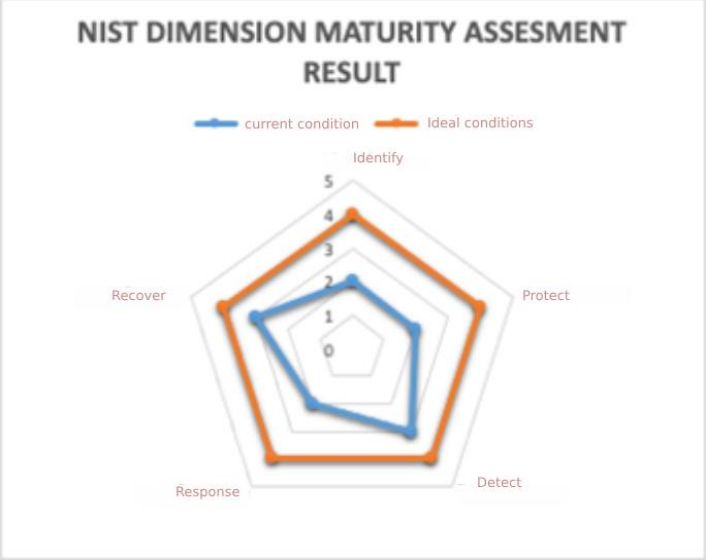

Figure 3 NIST Dimension Maturity Assessment Result

Based on the measurement results that have been analyzed, there are 8 dimensions in total, consisting of 5 dimensions from NIST and 3 dimensions from PPT. All dimensions will be evaluated both in the current state and future state based on responses from respondents, see figure 4 and table 1 below.

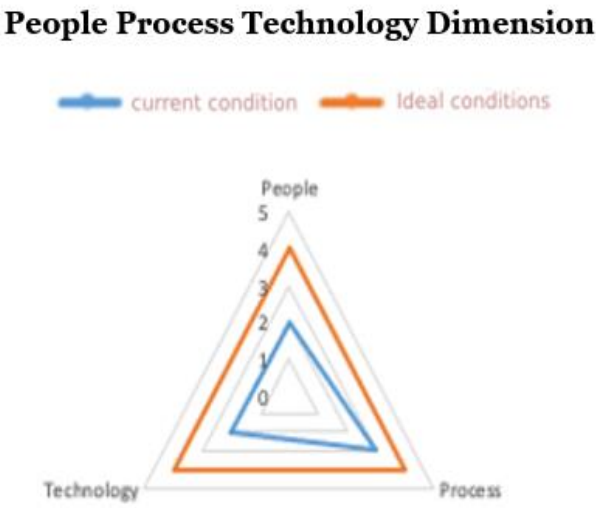

Figure 4 PPT Dimension Maturity Assessment Result

Table 2 Average maturity level calculation NIST Dimension

No	Subcategory	Category	Dimension	Current Conditions	Ideal Conditions
1	ID.AM-1	Asset Management (ID.AM)	Identify	2	4
2	ID.AM-2				
3	ID.AM-5				
4	ID.AM-6				
5	ID.BE-4	Business Environment (ID.BE)		3	4

6	ID.GV-1	Governance (ID. GV)		3	4
7	ID.RA-1	Risk Assessment (ID.RA)		2	4
8	ID.RA-2				
9	ID.RA-4				
10	ID.RM-1	Risk Management Strategy (ID.RM)		3	4
11	PR.AC-1	Identity Management, Authentication and Access Control (PR.AC)	Protect	3	4
12	PR.AC-3				
13	PR.AC-4				
14	PR.AT-1	Awareness and Training (PR.AT)		2	4
15	PR.DS-4	Data Security (PR.DS)		3	4
16	PR.DS-5				
17	PR.PT-1	Protective Technology (PR.PT)		2	4
18	DE.AE-3	Anomalies and Events (DE.AE)	Detect	3	4
19	DE.CM-3	Security Continuous Monitoring (DE.CM)		3	4
20	DE.CM-4				
21	DE.CM-8				
22	RS.RP-1	Response Planning (RS.RP)	Respond	3	4
23	RS.CO-1	Communications (RS.CO)		2	4
24	RS.CO-4				
25	RS.AN-1	Analysis (RS.AN)		3	4
26	RS.AN-2				
27	RS.IM-1	Improvements (RS.IM)		3	4
28	RC.RP-1	Recovery Planning (RC.RP)	Recover	3	4
29	RC.CO-2	Improvements (RC.IM)		3	4
30	RC.CO-3	Communications (RC.CO)		3	4

The Gap analysis results show that the focus of the Roadmap and Solution development will start from the Identify aspect of the NIST Framework, specifically on asset management. Interviews with several senior management also supported this finding. Although the current asset management system has been implemented, it still does not fully meet the requirements as some activities are still performed manually. In addition, there are deficiencies in the patching process of operating systems, applications, and asset updates. Currently, the asset management and patching processes run separately and are not applied to all devices, although this is necessary to meet the ISO 27001:2013 standard, especially regarding security and effective management of information systems. In addition, there is no software that can automatically deploy applications to the desktop. Therefore, optimization of the IT Asset Management solution is very important, , see table 3 below.

Table 3 Average maturity level calculation PPT Dimension

People	Current Conditions	Ideal Conditions
ID.AM-6	2	4
ID.RA-4	2	4
PR.AT-1	2	4
RS.CO-1	2	4

People	Current Conditions	Ideal Conditions
ID.BE-4	3	4
ID.GV-1	3	4
ID.RM-1	3	4
PR.AC-1	3	4

Technology	Current Conditions	Ideal Conditions
ID.AM-1	3	4
ID.AM-2	3	4
ID.AM-5	3	4
ID.RA-1	2	4

RS.CO-4	3	4
RC.CO-3	3	4
Average	2	4

RS.RP-1	3	4
RS.AN-1	3	4
RS.AN-2	3	4
RS.IM-1	3	4
RC.RP-1	3	4
RC.CO-2	3	4
Average	3	4

ID.RA-2	3	4
PR.AC-3	3	4
PR.AC-4	3	4
PR.DS-4	3	4
PR.DS-5	3	4
PR.PT-1	2	4
DE.AE-3	3	4
DE.CM-3	3	4
DE.CM-4	3	4
DE.CM-8	3	4
Average	2	4

Conclusions

The integration of the results from these two frameworks contributes to strengthening the Identify aspect, which is a key foundation in cybersecurity management. Both frameworks also support the prioritization of cybersecurity efforts in accordance with the principles of the NIST Framework as well as the determination of the level of access control needed in accordance with the concepts of the PPT Framework. Assets that have a higher level of sensitivity will require stricter protection and control. In addition, measurements from the DMM PPT (People, Process, and Technology) help raise awareness of cybersecurity risks, which is critical to building a solid security culture within the organization. that most of the sample came from the technology department. For future research, it is recommended that the sampling be expanded to cover more data, and the questionnaire variables or subcategories be expanded to increase the variety of data. Given the time.

References

Alqudhaibi, A., Deshpande, S., Jagtap, S., & Salonitis, K. (2023). Towards a sustainable future: developing a cybersecurity framework for manufacturing. *Technological Sustainability*, *2*(4), 372–387. https://doi.org/10.1108/TECHS-05-2023-0022

Aras, A., & Büyüközkan, G. (2023). Digital Transformation Journey Guidance: A Holistic Digital Maturity Model Based on a Systematic Literature Review. *Systems*, *11*(4), 1–31. https://doi.org/10.3390/systems11040213

Calliess, C., & Baumgarten, A. (2020). Cybersecurity in the EU the example of the financial sector: A legal perspective. In *German Law Journal* (Vol. 21, Issue 6). https://doi.org/10.1017/glj.2020.67

Cartwright, A., Cartwright, E., & Edun, E. S. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. *Computers and Security*, *131*. https://doi.org/10.1016/j.cose.2023.103288

Chang, K., & Huang, H. (2023). Exploring the management of multi-sectoral cybersecurity information-sharing networks. *Government Information Quarterly*, *40*(4), 101870. https://doi.org/10.1016/j.giq.2023.101870

Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, *22*(1), 105–117. https://doi.org/10.1016/j.eij.2020.05.003

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating Cybersecurity Frameworks for Opportunities, Risks, and Regulatory Compliance in Commercializing Large Language Models. *Computers & Security*, *144*(November 2023), 103964. https://doi.org/10.1016/j.cose.2024.103964

Ngamal, Y., & Maximus Ali Perajaka. (2021). Penerapan Model Manajemen Risiko Teknologi Digital Di Lembaga Perbankan Berkaca Pada Cetak Biru Transformasi Digital Perbankan Indonesia. *Jurnal Manajemen Risiko*, *2*(2), 59–74. https://doi.org/10.33541/mr.v2iiv.4099

Oluomachi, E., Ahmed, A., Ahmed, W., & Samson, E. (2024). Assessing the Effectiveness of Current Cybersecurity Regulations and Policies in the Us. *International Journal of Scientific and Research Publications*, *14*(2), 78–85. https://doi.org/10.29322/ijsrp.14.02.2023.p14610

Sánchez-García, I. D., Feliu Gilabert, T. S., & Calvo-Manzano, J. A. (2023). Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic mapping review. *Computers and Security*, *128*. https://doi.org/10.1016/j.cose.2023.103170

Satrio Ronggo Buwono, Abubakar, L., & Handayani, T. (2022). Kesiapan Perbankan Menuju Transformasi Digital Pasca Pandemi Covid-19 Melalui Financial Technology (Fintech). *Jurnal Poros Hukum Padjadjaran*, *3*(2), 228–241. https://doi.org/10.23920/jphp.v3i2.764

Seun Solomon Bakare, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, & Nkechi Emmanuella Eneh. (2024). Data Privacy Laws and Compliance: a Comparative Review of the Eu Gdpr and Usa Regulations. *Computer Science & IT Research Journal*, *5*(3), 528–543. https://doi.org/10.51594/csitrj.v5i3.859

Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity

frameworks review. *Journal of Industrial Information Integration*, *39*(March). https://doi.org/10.1016/j.jii.2024.100604

Zahid, S., Mazhar, M. S., Abbas, S. G., Hanif, Z., Hina, S., & Shah, G. A. (2023). Threat modeling in smart firefighting systems: Aligning MITRE ATT&CK matrix and NIST security controls. *Internet of Things (Netherlands)*, *22*(March), 1–18. https://doi.org/10.1016/j.iot.2023.100766

Schallmo, D. R., & Tidd, J. (2021). Digitalization. Cham: Springer International Publishing.