

Evaluation of Cybersecurity Awareness and Training for Digital Branch Frontliners at Bank XYZ

Ayu Novira Shinta Permatasari^{1)*}, Alfa Ryano Yohannis²⁾

^{1)*2)}Universitas Pradita, Indonesia

^{1)*}ayu.novira@student.pradita.ac.id, ²⁾alfa.ryano@pradita.ac.id

ABSTRACT

The digital transformation in the banking sector has driven a shift in operations, including the establishment of digital branches that rely on information technology to deliver services to customers. However, the increased use of technology brings significant information security risks, particularly those stemming from human factors. This study aims to evaluate the level of cybersecurity awareness among 36 frontliners at Bank XYZ's digital branch using the ISO/IEC 27002:2022 framework, and to develop training recommendations based on NIST SP 800-50. The research was conducted using both quantitative and qualitative methods, involving questionnaires and observations of 36 frontliners. The evaluation results revealed that several controls, particularly Response to Information Security Incidents (ID 5.26), still showed low levels of understanding (60%), indicating the need for training intervention. Training recommendations were designed based on the Cybersecurity and Privacy Learning Program (CPLP) principles from NIST SP 800-50, which include visual approaches, role-based training, and digital learning media. The implementation of these recommendations for one of the controls showed a significant improvement in post-test scores (average ≥ 93), exceeding the 85% threshold. These findings validate CPLP-based approaches as effective strategies for enhancing cybersecurity readiness in digital banking frontlines.

Keywords: Cybersecurity Awareness, ISO/IEC 27002:2022, NIST SP 800-50, Frontliners, CPLP, Information Security Evaluation, Banking Industry

1. INTRODUCTION

In the digital era, the banking industry continues to adapt to meet customer demands for faster and more convenient services. Simatangkir, Afifah, and Faliha (2025) note that the advancement of digital technology has transformed banking operations, making them more efficient and accessible. One significant innovation is the digital branch—a bank branch that leverages technology to offer self-service banking with minimal physical interaction. In Indonesia, this model is exemplified by branches located in shopping malls, enabling customers to complete transactions digitally. Bank XYZ has equipped its digital branches with up-to-date technical security measures. However, despite the robustness of these systems, human factors remain a critical vulnerability. The extent to which frontliners understand how to prevent data leaks and safeguard sensitive information is an unresolved concern that could compromise overall security and result in reputational and financial loss.

According to the 2023 Verizon Data Breach Investigations Report, 74% of data breaches are attributed to human error, misuse of access privileges, or social engineering (Verizon, 2023). Frontliners at digital branches—who regularly interact with both customers and systems—may become entry points for cyber threats if their cybersecurity awareness is inadequate. Fathurohman dan Witjaksono (2020) emphasize that enhancing human resource capabilities is essential for strengthening cybersecurity. This challenge is further compounded by the rise of AI-based phishing attacks and the use of personal devices (BYOD), which often fall short of encryption or compliance standards. The lack of knowledge among frontliners in handling sensitive data not only increases security risks but may also lead to regulatory penalties under frameworks such as POJK No. 38/2016 on IT Risk Management.

While frameworks like ISO/IEC 27001 (International Organization for Standardization, 2022) are widely promoted to address cybersecurity risks, Fajri and Harwahu (2024) highlight the importance of ISO/IEC 27002:2022

* Corresponding author



[Creative Commons Attribution-NonCommercial-ShareAlike 4.0
International License.](https://creativecommons.org/licenses/by-nc-sa/4.0/)

as a supporting standard, particularly for evaluating human-related controls in information security. Clause 6 of ISO/IEC 27002:2022 emphasizes People Controls, including training, incident response, and asset management. Yet, its implementation in Indonesia's banking sector—especially within dynamic, tech-centric environments like digital branches—remains limited. Prior studies have focused predominantly on system-based safeguards such as firewalls and encryption. In contrast, assessments of human readiness as the first line of defense are often overlooked.

To address this gap, the present study evaluates cybersecurity awareness among 36 frontliners at Bank XYZ's digital branch using ISO/IEC 27002:2022. Based on the evaluation, this study also proposes a training program using the NIST SP 800-50 framework (Merritt et al., 2024), which offers a structured Cybersecurity and Privacy Learning Program (CPLP). CPLP emphasizes role-based training, awareness campaigns, experiential learning, and gamification—methods shown to be practical and adaptable in prior research (Astuti, 2019; Tan & Soewito, 2022). These recommendations aim to reduce cybersecurity risks, as supported by previous studies such as Pambudi and Ramli (2023).

Unlike prior studies focusing on system-based controls, this study directly addresses human-centric vulnerabilities in digital branches. The goal is to fill both academic and practical gaps by not only evaluating awareness but also providing tailored training recommendations aligned with ISO/IEC and NIST standards. These findings are intended to support the development of adaptive, scalable training programs that meet regulatory requirements while strengthening the human layer of cybersecurity in digital banking.

2. METHOD

Literature Review

Previous studies have evaluated information security implementation using ISO/IEC 27001 and ISO/IEC 27002 standards across educational, governmental, and private sectors. Paramita, Siregar, Damanik, and Irawan (2022) assessed information security readiness at SMA Negeri 6 Medan using the KAMI Index and found it to be "moderately adequate," while Fathurohman and Witjaksono (2020) emphasized the importance of ISMS compliance in local government, with a gap assessment showing 85% compliance. Although both studies applied ISO/IEC 27001:2013, their approaches differed: The first study focused on readiness evaluation, whereas the second addressed the need for structured ISMS implementation.

In contrast, Wiemas and Suroso (2022) and Kusnandar, Rochim, and Gunawan (2024) concentrated on information security risk management. The former used the PDCA approach based on ISO/IEC 27001:2022, while the latter employed the FMEA method. Both studies highlighted the need to improve access control and security awareness. However, they primarily addressed organizational-level controls, not individual roles such as frontliners. Similarly, studies by Santi, Alfresi, and Octariana (2023) and Kurniawan and Irmawan (2022) assessed the maturity of information security systems using CMMI and ISO/IEC 27002:2013, revealing level 2 maturity—an indication of insufficiently optimized controls. Clarissa and Wang (2023) reinforced these findings by identifying significant gaps in cryptography and incident management, stressing the urgency for more comprehensive training programs.

Jufri, Hendayun, and Suharto, (2017) in Indonesia revealed that ISMS awareness varies across organizational levels and is often lacking among non-technical personnel. This is further supported by Ho, Ko, Mazerolle, Gilmour, and Miao (2024), who proposed integrating situational crime prevention (SCP) strategies to strengthen cybersecurity from a human-behavior perspective. From a technical standpoint, Huang et al. (2019) introduced automation and visualization for risk management based on NIST SP 800-53 using the CSAT tool, promoting adaptability and efficiency. On the other hand, Catota, Granger Morgan, and Sicker, (2018) emphasized that incident response capabilities in the financial sector are hindered by limited staff awareness and training.

While these studies significantly contribute to improving security controls and risk management, most of them focus on technical and governance aspects at an organizational scale. None have specifically addressed cybersecurity awareness among frontliners in digital banking branches, despite these individuals serving as the primary point of contact in digital interactions with customers. This study aims to address that gap by utilizing the ISO/IEC 27002:2022 framework to measure awareness levels and providing training recommendations based on NIST SP 800-50. By emphasizing the human factor and proposing role-based training, gamification, and awareness campaigns, this research seeks to enhance frontline employees' capability and vigilance regarding cyber risks, while also supporting compliance with both national and international standards.

A digital branch in banking is a concept that leverages digital technology to enhance service efficiency and customer convenience, focusing on self-service machines, video banking, and digital apps rather than direct teller interactions. Unlike conventional branches with limited hours and physical staff interaction, digital branches often offer 24/7 access

* Corresponding author



[Creative Commons Attribution-NonCommercial-ShareAlike 4.0
International License.](https://creativecommons.org/licenses/by-nc-sa/4.0/)

and allow customers to perform transactions independently. Bank XYZ has been implementing digital branches since 2013, and as of 2023, it operates 37 branches located in malls, offices, campuses, and residential areas, reflecting its commitment to advancing digital banking and improving customer experience. The rise of mobile banking and demand for fast, flexible services make digital branches increasingly relevant, offering operational efficiency by reducing labor costs and minimizing human error through automation, while also enhancing transaction security.

ISO/IEC 27002 is an international standard that provides guidelines for implementing information security, cybersecurity, and privacy controls (International Organization for Standardization, 2022). This standard serves as a reference for developing an Information Security Management System (ISMS) based on ISO/IEC 27001. The 2022 version updates the approach to security controls by better aligning with evolving digital threats and offering greater flexibility in implementation.

In relation to security awareness, there are several controls that can be applied, most of which fall under people controls. The purpose is to ensure that individuals within the organization possess the necessary understanding, competence, and behavior to protect sensitive information. These selected controls are useful for helping the organization reduce information security risks originating from human factors, whether intentional or unintentional. This helps ensure that all employees have a clear awareness of and responsibility for safeguarding the organization's data and systems. The related controls about awareness and used in this study are Information security roles and responsibilities (5.2), Response to Information Security Incidents (5.26), Terms and Conditions of Employment (6.2), Information Security Awareness, Education, and Training (6.3), Disciplinary Process (6.4), Confidentiality or Non-Disclosure Agreements (6.5), Remote Working (6.6), Information Security Event Reporting (6.7) and Clear Desk and Clear Screen (6.8).

NIST SP 800-50 is a framework document titled Building a Cybersecurity and Privacy Learning Program, published in September 2024, replacing the previous version released in 2003, as stated by (Merritt et al., 2024). This document provides guidance to federal agencies and other organizations on developing and managing a Cybersecurity and Privacy Learning Program (CPLP). The program aims to enhance awareness, training, and education related to cybersecurity and privacy within an organization. The CPLP is designed to foster a culture of cybersecurity and privacy by instilling habits that reduce risks, increase awareness, and deliver role-based training to employees. There are four stages of NIST SP 800-50 which is Plan & Strategy, Analysis & Design, Development & Implementation, Assessment & Improvement.

* Corresponding author



[Creative Commons Attribution-NonCommercial-ShareAlike 4.0
International License.](https://creativecommons.org/licenses/by-nc-sa/4.0/)

Research Method

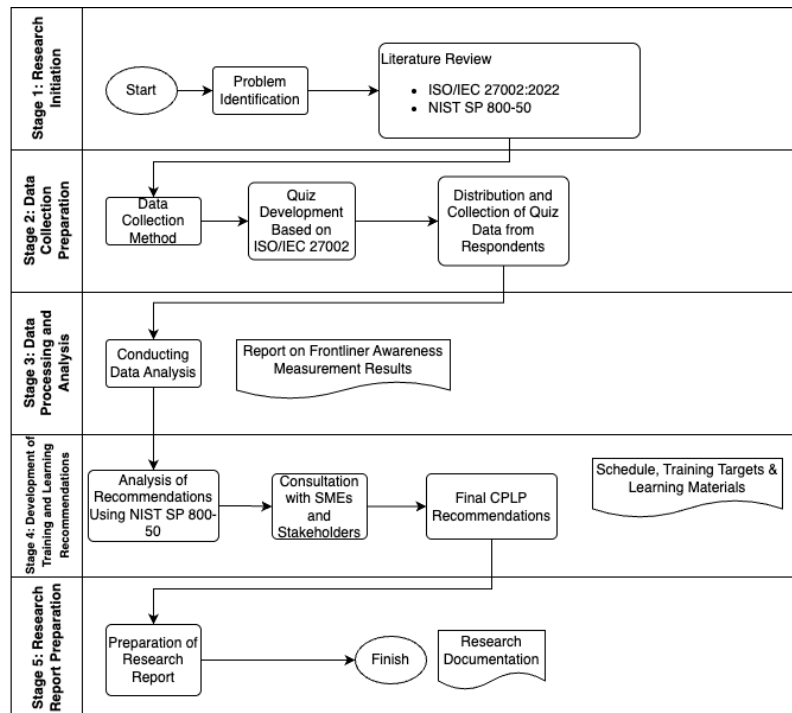


Fig. 1 Research Methodology

The first stage is the initial step of the research, beginning with the identification of issues related to cybersecurity awareness within the organization. To strengthen the foundation of the study, a literature review was conducted, referencing several key sources: cybersecurity literature analysis, ISO/IEC 27002:2022, and NIST SP 800-50. The purpose of this literature review is to understand the standards and best practices in enhancing cybersecurity awareness, as well as to determine the indicators that will be used in the research.

The second stage, a data collection method was planned to measure the level of cybersecurity awareness. The process began with the development of a quiz based on the controls in ISO/IEC 27002:2022, particularly those related to awareness. The questions were specifically tailored to match the roles and responsibilities of frontliners at Bank XYZ branch offices. A total of 28 questions were designed to assess their understanding and behavior regarding information security. After the quiz was finalized, it was distributed to the selected respondents to collect the necessary data for further analysis. The question have been evaluated using the KR-20 reliability analysis, and the result is 0.881, indicating a high level of internal consistency. Total respondents are 36 frontliners.

After the data was collected, it underwent a series of processing and analysis steps. First, the measurement data was evaluated using the ISO/IEC 27002:2022 framework to ensure alignment with established information security standards. The next step involved analyzing the questionnaire responses to identify patterns, trends, and areas requiring improvement in cybersecurity awareness. Based on the analysis, a report was then compiled to present the key findings, including the awareness levels of frontliners and the specific aspects that need further development.

Based on the results of data analysis, this phase focuses on formulating effective training and learning recommendations. The process began with an analysis guided by NIST SP 800-50, which served as the primary reference for designing a cybersecurity learning program. Further refinement was carried out through consultations with subject matter experts (SMEs). Subject Matter Experts (SMEs) are two key individuals from Bank XYZ. The first was Mrs. Beta (pseudonym), a Cybersecurity Awareness Specialist responsible for managing the bank's information security awareness programs, including material development, training, and socialization across all units. The second was Mr. Alpha (pseudonym), Head of Cybersecurity Assurance, who supervises the overall implementation of security activities—including awareness—to ensure compliance with bank-wide standards and regulations.

* Corresponding author



[Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.](https://creativecommons.org/licenses/by-nc-sa/4.0/)

The final stage of this research involves compiling a report that documents the entire research process and findings. The report includes the background and objectives of the study, the methods used, data analysis results, and the resulting recommendations. Once the report is completed, the research is considered finalized and can serve as a foundation for developing cybersecurity awareness programs within the organization.

3. RESULT AND DISCUSSIONS

Data collection in this study was conducted through the distribution of a questionnaire consisting of 28 questions related to cybersecurity awareness, designed based on the controls outlined in the ISO/IEC 27002 standard. The complete questionnaire can be found in the Appendix section. This questionnaire was targeted at frontliner employees at Bank XYZ's digital branches, given their strategic role in direct customer interaction and access to sensitive information. The data collection process took place over one week, with a total of 36 respondents. All participants were asked to answer the questions based on their understanding and attitude toward information security practices within their work environment. The data obtained from this method served as the basis for evaluating the level of cybersecurity awareness and identifying areas that require further reinforcement.

The analysis of the questionnaire results in this subsection refers to the ISO/IEC 27002:2022 framework, which provides best practice guidelines for implementing information security controls. Each question in the questionnaire was mapped to relevant controls based on the clauses of the standard, enabling a structured evaluation of cybersecurity awareness among frontliner employees. The findings were analyzed to determine the extent of respondents' understanding and compliance with existing security policies and procedures, both in day-to-day operations and in information security incident situations. This approach aims to provide a comprehensive overview of individual readiness in safeguarding data and information within the digital work environment.

Based on the mapping of the questionnaire to the controls outlined in ISO/IEC 27002:2022, the average scores of respondents' understanding across each information security control area were summarized. These results provide an overview of the extent to which frontliner employees are aware of and comply with key aspects of information security management. Among the nine controls analyzed, the highest average score was recorded in the “Clear Desk and Clear Screen” control (100%), followed by “Information Security Roles and Responsibilities” and “Confidentiality or Non-Disclosure Agreements,” both scoring 95%. Conversely, the “Response to Information Security Incidents” control showed the lowest level of understanding, with an average score of only 60%. These findings serve as an initial indicator of strengths and weaknesses in employees' understanding of information security control implementation and form the basis for developing a more targeted awareness improvement strategy. According to discussions with the relevant Subject Matter Experts (SMEs), a score of 85% is set as the threshold value—indicating that no improvement is required if the score exceeds this benchmark.

Table 1
The overall average score across all controls.

ID	Title	Average Score
5.2	<i>Information security roles and responsibilities</i>	95%
5.26	<i>Response to Information Security Incidents</i>	70% (need improveemnt)
6.2	<i>Terms and Conditions of Employment</i>	86%
6.3	<i>Information Security Awareness, Education, and Training</i>	82% (need improveemnt)
6.4	<i>Disciplinary Process</i>	70% (need improveemnt)
6.5	<i>Confidentiality or Non-Disclosure Agreements</i>	95%
6.6	<i>Remote Working</i>	82% (need improveemnt)
6.7	<i>Information Security Event Reporting</i>	86%
6.8	<i>Clear Desk and Clear Screen</i>	100%

* Corresponding author



[Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.](https://creativecommons.org/licenses/by-nc-sa/4.0/)

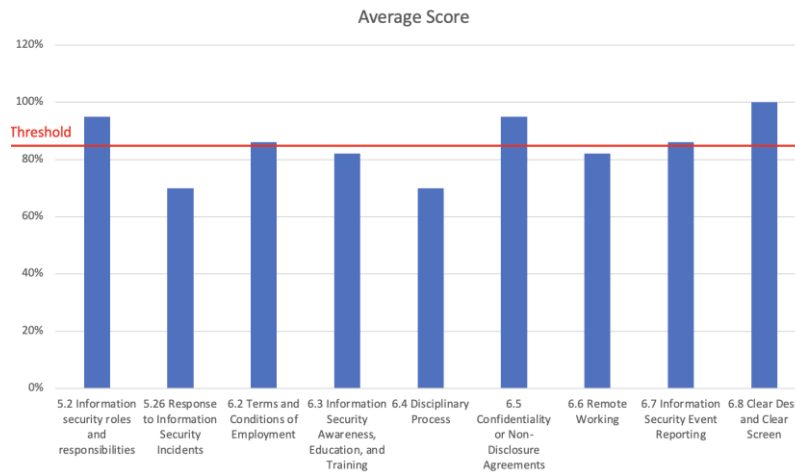


Fig. 2 The overall average score across all controls

Based on the evaluation results of cybersecurity awareness among frontliner employees and the validation process conducted with Subject Matter Experts (SMEs), this study formulates a final set of recommendations aligned with the Cybersecurity and Privacy Learning Program (CPLP) framework outlined in NIST SP 800-50r1. These recommendations are designed to address the need for continuous improvement in employee competence and awareness through a more structured and contextual approach, tailored to the operational characteristics of the Digital Branch at Bank XYZ. Each recommendation is developed based on the controls outlined in ISO/IEC 27002:2022, taking into account the available internal media and inputs provided by relevant technical stakeholders.

Response to Information Security Incidents (ID 5.26)

Plan & Strategy

In the context of frontliner operations, responding to information security incidents is a crucial element in ensuring service continuity and protecting customer data. Although the level of understanding regarding types of attacks is relatively adequate, the evaluation results indicate that frontliners are not yet fully aware of the importance of incident reporting as a necessary follow-up action. Therefore, this control is prioritized for enhancement through a practical and contextual learning approach, enabling them not only to understand incidents but also to take appropriate action in response.

Table 2

Plan & Strategy for Improving the Control: Response to Information Security Incidents (ID 5.26)

Element	Description
Strategic Plan	Minimize the impact and risks of information security incidents by improving the speed and accuracy of reporting by frontliners.
Strategic Goals	Enhance frontliners' understanding of types of security incidents and the importance of quick reporting to prevent incident propagation.
Objectives	80% of frontliners are able to identify and report incidents. Post-test scores increase to at least the 85% threshold.
Tactic	[T01] Visual Flowchart Procedure: An infographic displaying the steps for incident reporting, recommended by the SME to be placed as a desktop wallpaper or in secure yet visible internal work areas

Analysis & Design

Next is the analysis and design phase, tailored to the needs of the frontliners based on the evaluation results and the previously developed plan. This subsection will produce a document that outlines a detailed training plan, including material selection, duration, trainers, and an evaluation plan to measure the improvement outcomes. Based on observations and discussions with stakeholders, the following is the proposed recommendation plan.

* Corresponding author



[Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.](https://creativecommons.org/licenses/by-nc-sa/4.0/)

Table 3
Design of Training Materials and Implementation of Learning Tactic [T01]

Element	Description
Title	Cyberattack Incident Reporting Simulation
Learning Media	Online via HR Learning Application [Interactive Video Games / Scenario-based Simulation]
Stakeholders	Cybersecurity Awareness Team, HR, Frontliner manager.
Participants	All frontliners at Bank XYZ
Location	Online, accessible anytime and anywhere
Training Duration	26 – 44 working days
Training Cost	IDR 50,500,000 – IDR 71,000,000
Evaluation Metrics	Final quiz score with a 100% Post-test score increases with a minimum threshold of 85%
Training Material	Module Title: “Prevent Threats, Maintain Customer Trust” Part 1 – Introduction to Information Security and Cyber Incidents Part 2 – Scenario-Based Interactive Simulation Part 3 – Impact Education and Procedures Part 4 – Final Quiz and Reflection

Disciplinary Process (ID 6.4)

Plan & Strategy

The disciplinary process is part of organizational controls designed to ensure compliance with information security policies. Understanding the consequences of violations is crucial so that every employee is aware of their responsibilities. Learning in this control area aims to provide a more concrete and in-depth understanding of the risks and impacts of non-compliance with policies, through case study simulations that reflect real conditions in the work environment.

Table 4
Plan & Strategy for improving the Disciplinary Process control (ID 6.4)

Element	Description
Strategic Plan	Enforce a culture of information security discipline by fostering understanding of rules and violation sanctions.
Strategic Goals	Increase awareness of disciplinary policies and the consequences of violations.
Objectives	90% of frontliners understand common violations and their sanctions. Post-test scores increase to at least the 85% threshold.
Tactic	[T02] Case Study and Discussion Forum: Participants are given real cases of policy violations (e.g., unauthorized access, negligence in clear screen) and asked to analyze them in groups.

Analysis & Design

Next is the analysis and design phase, which is tailored to the needs of the frontliners based on the evaluation results and the plan previously made. This subsection will produce a document describing the training plan in detail, from material selection, duration, instructors, to the evaluation plan to measure improvement results. Based on observations and discussions with stakeholders, the following is the plan for preparing recommendations.

Table 5
Design of Training Materials and Implementation of Learning Tactic [T02]

Element	Description
Title	Case Study and Discussion Forum: Information Security Policy Violations
Learning Media	Group discussion sessions held either face-to-face (offline) or virtual (online meeting)

* Corresponding author



[Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.](https://creativecommons.org/licenses/by-nc-sa/4.0/)

Stakeholders	Cybersecurity Awareness Team, HR, Frontliner manager.
Participants	All frontliners at Bank XYZ
Location	Internal training room or online via official communication platform Can be conducted hybrid at the Learning Center with rotating schedules
Training Duration	10–12 working days
Training Cost	IDR 1,500,000 – IDR 3,000,000
Evaluation Metrics	Case analysis worksheet scores per group Post-test score increases with a minimum threshold of 85%
Training Material	Module Title: “Learning from Cases – Prevention is Better than Regret” Case Study 1 – Unauthorized Access by a Colleague A frontliner lends their login account to a colleague because they forgot their password. The system logs suspicious activity, but the colleague denies it. Discuss who is responsible and the consequences. Case Study 2 – Screen Left Open During Break: An employee leaves the computer active and unlocked, then returns to find the system used by someone else. Discuss how this could have been prevented and whether this is a serious violation.

Information Security Awareness, Education, and Training (ID: 6.3)

Plan & Strategy

Awareness and education are the foundational pillars of sustainable information security. This control aims to build a security-aware culture through continuous education reinforcement. Given that frontliners are the first line of interaction with customers, enhancing their knowledge and attitude toward social engineering threats becomes a primary focus. Therefore, the learning tactics are designed to be modular and lightweight, yet impactful in driving behavioral change.

Table 6
Plan & Strategy for improving the Information Security Awareness, Education, and Training (ID: 6.3)

Element	Description
Strategic Plan	Building continuous awareness of information security threats and fostering a secure mindset.
Strategic Goals	Increasing information retention and active participation in security awareness programs.
Objectives	100% of frontliners participate in at least one training module every two months. Post-test scores increase to at least exceed the 85% threshold.
Tactic	[T03] Continuous Modular Training: Weekly series via LMS/email discussing one threat topic per week (phishing, tailgating, shoulder surfing, etc.).

Analysis & Design

The next phase is analysis and design, which is tailored to the needs of frontliners based on previous evaluation results and established plans. This subsection will produce a document that outlines the training plan in detail, including material selection, duration, trainers, and an evaluation plan to measure improvement. Based on observations and discussions with stakeholders, the following recommendation plan has been developed.

Table 7
Design of Training Materials and Implementation of Learning Tactic [T03]

Element	Description
Title	Continuous Modular Training: Weekly Threat Topic Series
Learning Media	Lightweight modules in interactive PowerPoint (PPT) format uploaded to the LMS or distributed via internal email [Document-based learning]

* Corresponding author



[Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.](https://creativecommons.org/licenses/by-nc-sa/4.0/)

Stakeholders	Cybersecurity Awareness Team, HR, Frontliner manager.
Participants	All frontliners at Bank XYZ
Location	Online, modules accessible anytime and anywhere
Training Duration	3 months
Training Cost	IDR 0
Evaluation Metrics	Percentage of video/module views via LMS/email (target: minimum 80%) Post-test score increases with a minimum threshold of 85%
Training Material	Module Title: "Stay Alert Weekly: Cyber Threats Are Real" First 2 Weeks Example: Week 1 – Phishing • Examples of recent phishing emails • Quick tips to identify fake URLs • What to do if you receive a suspicious email Week 2 – Tailgating • Illustration of strangers entering the office • Polite procedures to deny entry without conflict Each Module Slide Includes: • Illustrative visuals + light narrative (internal tone) • Mini Quiz (1–2 questions) • Link to SOP material or summary of correct actions

Remote Working (ID: 6.6)

Plan & Strategy

With increasingly flexible work models, including remote work, the need to ensure security in accessing and using work devices has become more critical. This control emphasizes the importance of understanding and applying secure practices when working from locations outside the office. The training is designed to address specific challenges commonly encountered, such as the use of public networks, device storage, and authentication, through an interactive and scenario-based approach.

Table 8
Plan & Strategy for improving the Remote Working (ID: 6.6)

Element	Description
Strategic Plan	Ensuring data and connection security while working outside the office.
Strategic Goals	Cultivating secure remote work habits and understanding of common risks.
Objectives	100% of frontliners activate VPN and MFA. Post-test scores increase to at least exceed the 85% threshold.
Tactic	[T04] Secure Setup Tutorial Video: Step-by-step instructions on how to activate VPN, MFA, and password managers, presented through a screen-based tutorial video. This content will be included in the onboarding toolkit for new employees so that secure remote work habits are formed from the start.

Analysis & Design

The next stage is the analysis and design, which is tailored to the needs of frontliners based on previous evaluations and planned strategies. This subsection will result in a document that outlines a detailed training plan, including material selection, duration, facilitators, and evaluation plans to measure improvement outcomes. Based on observations and discussions with stakeholders, the following is the proposed plan for developing the training recommendations.

* Corresponding author



[Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.](https://creativecommons.org/licenses/by-nc-sa/4.0/)

Table 9
Design of Training Materials and Implementation of Learning Tactic [T04]

Element	Description
Title	Secure Setup Tutorial Video: Building Safe Habits from Day One
Learning Media	Screen-recorded video with narration MP4 format, 2–4 minutes per topic (max. 10 minutes total) Embedded in new employee onboarding e-learning (via LMS) and included in the employee digital toolkit
Stakeholders	Cybersecurity Awareness Team, HR, Frontliner manager.
Participants	All frontliners at Bank XYZ
Location	Online, modules accessible anytime and anywhere
Training Duration	9–12 working days
Training Cost	IDR 2,000,000 – IDR 4,000,000
Evaluation Metrics	Completion rate of onboarding videos (target: 100% of onboarding participants) Post-test score increases with a minimum threshold of 85%
Training Material	Module Title: “Start Your First Day Safely!” Video 1 – Setting Up Bank XYZ VPN Client (Duration: 3 minutes) Explains installation, first login, and basic troubleshooting Emphasizes VPN is mandatory when working remotely or on the go Video 2 – Activating MFA and Using a Digital Token (Duration: 3 minutes) Using OTP apps/tokens (e.g., Google Authenticator, Microsoft Authenticator, or internal system) Simulated login and two-step verification

Implementation and Improvement of ISO 27002:2022 Controls

The implementation and improvement efforts focused on one specific control from ISO 27002:2022, namely Response to Information Security Incidents (ID 5.26). The implementation was conducted with the same group of respondents from the beginning of the study, consisting of 36 frontliners. The instructional material design and learning tactic implementation used Tactic [T02], which is the Visual Flowchart of Incident Reporting Procedure. This material was developed based on SOP guidelines and discussions with relevant stakeholders. The poster was created and distributed to frontliner participants who had previously responded to the questionnaire.

The results from implementing the learning material show a significant improvement in post-test evaluation scores. The average participant post-test score reached 93%, exceeding the previously set threshold of 85%. This achievement serves as an indicator of the success of the material improvements and the chosen approach, which follows the principles of NIST SP 800-50, emphasizing the importance of visual communication strategies, message consistency, and contextual delivery relevant to frontliners’ daily tasks. Thus, it can be concluded that infographic- and visual



* Corresponding author



[Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.](https://creativecommons.org/licenses/by-nc-sa/4.0/)

flowchart-based learning methods in the context of incident reporting are effective in increasing awareness and response to information security incidents.

DISCUSSIONS

The findings of this study confirm that while the overall cybersecurity awareness of frontliners at Bank XYZ's digital branch is within a good range, there are notable gaps in specific controls—particularly in incident response and policy compliance. These results align with prior research that highlights human factors as persistent vulnerabilities in cybersecurity (Verizon, 2023; Fathurohman & Witjaksono, 2020). Compared to previous studies that emphasize organizational-level compliance, this research contributes by focusing on individual readiness through role-based evaluations. The application of NIST SP 800-50 principles in designing contextual training tactics—such as visual flowcharts, simulations, and modular content—demonstrated significant effectiveness, as shown by the post-test scores that exceeded the 85% threshold. These results suggest that targeted and practical learning interventions, grounded in international standards, are crucial in bridging the gap between awareness and behavior in cybersecurity practices. Furthermore, integrating CPLP strategies into onboarding and continuous learning may serve as a scalable model for improving human-centric controls in digital banking environments.

CONCLUSION

This study successfully addressed the first research question regarding the level of cybersecurity awareness among digital branch frontliners based on ISO/IEC 27002:2022. The findings show that, overall, information security awareness is in the "good" category, with most controls scoring above 80%. Notably high scores were seen in Information Security Roles and Responsibilities (95%), Clear Desk and Clear Screen (100%), Confidentiality or Non-Disclosure Agreements (95%), and Information Security Event Reporting (86%). However, some controls require serious attention, such as Response to Information Security Incidents (70%), Disciplinary Process (70%), Information Security Awareness, Education, and Training (82%), and Remote Working (82%). These results highlight a gap in understanding incident reporting procedures and the consequences of violating security policies, indicating the need for stronger and more consistent information security culture within the digital branch of Bank XYZ.

The second research question, regarding improvements using NIST SP 800-50r1, was also addressed. The study proposed learning tactics that are not only informative but also practical and tailored to the real-world context of frontliners. These tactics include interactive simulations, educational animated videos, visual flowcharts, and weekly lightweight PPT modules aligned with existing learning platforms such as the LMS, desktop wallpapers, email, and the SOP portal. Validation by Subject Matter Experts (SMEs) confirmed the content's relevance to organizational needs and supported effective implementation. All designs followed the CPLP stages—Plan & Strategy and Analysis & Design—as a foundation for developing a strategic, consistent, and measurable cybersecurity training program.

This study primarily relies on questionnaire-based assessments, which may not fully capture changes in real-world behavior. Future research should incorporate behavior-based evaluations in actual work environments, such as compliance audits or improvements in incident reporting quality. Moreover, expanding the CPLP approach to non-frontliner units—such as IT, marketing, or customer experience—offers valuable opportunities to broaden the impact and applicability of this cybersecurity awareness initiative across the organization. This study contributes to the growing field of human-centric cybersecurity by providing an empirical model for awareness evaluation and CPLP-based training design tailored to digital frontliners.

REFERENCES

- Astuti, D. W. (2019). *Penyusunan Rekomendasi untuk Meningkatkan Kesadaran Keamanan Informasi berdasarkan NIST SP 800-50 (Studi Kasus: Institut Teknologi Sepuluh Nopember)*. Institut Teknologi Sepuluh Nopember.
- Catota, F. E., Granger Morgan, M., & Sicker, D. C. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. *Journal of Cybersecurity*, 4(1). <https://doi.org/10.1093/cybsec/tyy002>
- Fajri, K. S. Al, & Harwahu, R. (2024). Information Security Management System Assessment Model by Integrating ISO 27002 and 27004. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, 4(2), 498–506. <https://doi.org/10.57152/malcom.v4i2.1245>

* Corresponding author



[Creative Commons Attribution-NonCommercial-ShareAlike 4.0
International License.](https://creativecommons.org/licenses/by-nc-sa/4.0/)

- Fathurohman, A., & Witjaksono, R. W. (2020). Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City). *Bulletin of Computer Science and Electrical Engineering*, 1(1), 1–11. <https://doi.org/10.25008/bcsee.v1i1.2>
- Ho, H., Ko, R., Mazerolle, L., Gilmour, J., & Miao, C. (2024). Using Situational Crime Prevention (SCP)-C3 cycle and common inventory of cybersecurity controls from ISO/IEC 27002:2022 to prevent cybercrimes. *Journal of Cybersecurity*, 10(1). <https://doi.org/10.1093/cybsec/tyae020>
- International Organization for Standardization. (2022). International Standard ISO/IEC 27001:2022. *Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*, 2022. <https://doi.org/10.2307/j.ctv30qq13d>
- Jufri, M. T., Hendayun, M., & Suharto, T. (2017). Risk-Assessment Based Academic Information System Security Policy Using OCTAVE Allegro and ISO 27002. *International Conference on Informatics and Computing (ICIC)*.
- Kurniawan, E., & Irmawan, A. (2022). Performance Measurement of Security Academic Information System using Maturity Level. *International Journal of Innovative Science and Research Technology*, 7(4). Retrieved from www.ijisrt.com65
- Kusnandar, A., Rochim, A. F., & Gunawan, V. (2024). Pengukuran Tingkat Risiko dan Keamanan Informasi Menggunakan Metode FMEA Berbasis ISO / IEC 27001 pada Instansi XYZ untuk Keamanan Sistem Informasi. *Jurnal Sistem Informasi Bisnis*, 04. <https://doi.org/10.21456/vol14iss4pp375-384>
- Merritt, M., Hansche, S., Ellis, B., Sanchez-Cherry, K., Snyder, J. N., & Walden, D. (2024). *Building a Cybersecurity and Privacy Learning Program*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-50r1. <https://doi.org/https://doi.org/10.6028/NIST.SP.800-50r1>
- Pambudi, R. D., & Ramli, K. (2023). Information Security Risk Management Design of Supervision Management Information System At Xyz Ministry Using Nist Sp 800-30. *Jurnal Teknik Informatika (Jutif)*, 4(3), 591–599. <https://doi.org/10.52436/1.jutif.2023.4.3.978>
- Paramita, S., Siregar, S. A., Damanik, R. A., & Irawan, M. D. (2022). Analisis Manajemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001:2013. *Bulletin of Information Technology (BIT)*, 3(4), 374–379. <https://doi.org/10.47065/bit.v3i1>
- Santi, R., Alfresi, A. I., & Octariana, B. (2023). INFORMATION SYSTEM SECURITY AUDIT USING ISO/IEC 27002:2013 AT UNIVERSITY OF XXX. *Jurnal Teknik Informatika (Jutif)*, 4(4), 733–750. <https://doi.org/10.52436/1.jutif.2023.4.4.689>
- Simatangkir, D. W. E., Afifah, E. F. N., & Faliha, N. S. (2025). Keamanan Siber Dalam Perbankan Serta Tantangan Dan Solusi Di Era Digital. *Jurnal Multidisiplin Ilmu Akademik*, 2(1), 33–42.
- Tan, T., & Soewito, B. (2022). Manajemen Risiko Serangan Siber Menggunakan Framework Nist Cybersecurity Di Universitas Zxc. *Journal of Information System, Applied, Management, Accounting and Research*, 6(2), 411–422. <https://doi.org/10.52362/jisamar.v6i2.781>
- Verizon. (2023). Verizon Data Breach Investigations Report (DBIR). *Verizon Enterprise Solutions*. Retrieved from <https://inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf>
- Wiemas, K. N. G., & Suroso, J. S. (2022). Analysis of Risk Management Information System Applications Using Iso/Iec 27001:2022. *Jurnal Ilmiah Indonesia*, 7(11), 14–20. <https://doi.org/10.56304/s0040363622080021>