IJECBE (2025), **3**, **4**, 667–679
Received (3 June 2025) / Revised (25 June 2025)
Accepted (1 July 2025) / Published (30 December 2025)
https://doi.org/10.62146/ijecbe.v3i4.128
https://ijecbe.ui.ac.id
ISSN 3026-5258

International Journal of Electrical, Computer and Biomedical Engineering

RESEARCH ARTICLE

Optimizing IT Risk Management through PDCA-Based Continuous Improvement Stages

Miftaffudin Yusuf Pratama* and I Gde Dharma Nugraha

Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok, Indonesia
*Corresponding author. Email: miftaffudin.yusuf@ui.ac.id

Abstract

In the face of the evolving dynamics of cyber threats, frameworks with traditional approaches to information technology (IT) risk management are often inadequate because they are less responsive. This research aims to optimize IT risk management through Plan-Do-Check-Act (PDCA) based continuous improvement stages in a hybrid framework based on ISO 27005, NIST SP 800-30, NIST SP 800-39, ISO 27002, and COBIT 2019. The research method includes designing a six-stage framework that includes continuous improvement as a key element, followed by implementation testing at XYZ Institution and validation through expert judgment. Results show that systematically applying PDCA to high-risk assets improves control effectiveness, supports system resilience, and promotes more adaptive governance. The integration of PDCA in the risk management framework proved effective in optimizing IT risk management, especially in the context of non-profit organizations that require a strategic and sustainable approach.

Keywords: Risk Management, Continuous Improvement, PDCA, Hybrid Framework

1. Introduction

Digital transformation in the government sector has led non-profit organizations, including public institutions, to increasingly rely on information technology systems to carry out their duties and provide public services. This dependency presents various challenges, especially in managing information security risks. Cyber threats, system failures, and weaknesses in IT governance processes can directly impact institutional credibility and the effectiveness of services to the public. Therefore, the implementation of structured and systematic risk management has become an urgent necessity.

Information technology (IT) risk management plays a crucial role in identifying, evaluating, and managing potential threats that could affect the integrity, confidentiality, and availability of data [1]. In addition, IT risk management is important for protecting corporate reputation and building customer trust through assured data security [2]. However, in many organizations—especially non-profit institutions—IT risk management is often viewed as a supporting function that is separate from strategic decision-making [3]. This creates a gap between risk management policies and day-to-day operational practices, which can lead to vulnerability to various digital threats. The inability to fully integrate risk management into the organizational framework often results in slow responses to security incidents and reduced system resilience [4].

Various risk management standards and frameworks have been developed, such as ISO/IEC 27005, NIST SP 800-30/39, ISO/IEC 27002, and COBIT 2019. Although each offers a solid approach, their focus tends to be limited. For example, ISO 27005 focuses solely on information security risk management without addressing overall IT risk [5]. NIST SP 800-30 emphasizes technical threat and vulnerability assessment [6]. while NIST SP 800-39 promotes an integrated approach but still has limitations in connecting risk management to the organization's business objectives [4]. The COBIT 2019 framework is more oriented toward strategic governance and does not specifically address evolving technical threat dynamics [7]. Given the absence of a single overarching framework that comprehensively covers all risk aspects, a more holistic, adaptive, and organizationally relevant approach is needed—particularly for non-profit organizations with limited resources.

This research aims to design an integrated information security risk management framework using a hybrid approach that combines the strengths of several international standards. The main value added by this framework is the integration of a continuous improvement cycle based on the PDCA methodology, which has not yet been widely or systematically adopted in IT risk management frameworks. This study focuses on non-profit organizations, which have unique characteristics in terms of risk exposure, decision-making structures, and resource constraints.

To ensure the relevance and feasibility of the proposed framework, this research uses a dual validation approach: (1) implementation testing at Directorate ABC, Institution XYZ, and (2) expert judgement involving key stakeholders at Directorate ABC. Validation results indicate that the proposed framework is well-suited to organizational needs, particularly in terms of flexibility, completeness of process stages, and support for continuous improvement. Unlike most frameworks, which are linear and static, this framework positions PDCA as a strategic component that is fully integrated into the risk management cycle. This approach not only ensures evaluative feedback but also builds organizational capacity to adapt security strategies and controls in response to evolving threat dynamics.

2. Review of Literature

2.1 PDCA (Plan-Do-Check-Act)

Plan-Do-Check-Act (PDCA) is a method introduced by Dr. Edwards Deming, an expert in the field of quality management in America in 1950. PDCA is useful as a

continuous improvement [8]. PDCA cycle is future-oriented, flexible, logical and reasonable to describe all elements of the plan that is prepared. so that PDCA is very supportive for continuous improvement. There are four stages contained in this cycle that are interconnected with each other as seen as figure 1 below:

Plan: consists of setting goals and strategies to achieve the desired results. Included in this stage is also identifying problems.

Do: this stage is a continuation of Plan, which is to carry out what has been planned or determined at the Plan stage, such as testing, implementing controls and others.

Check: This stage is an examination of the stages that have been carried out previously. At this stage it must be done carefully to ensure that the Do stage has been carried out properly.

Act: this stage is an evaluation of the Do and Check stages. This stage is not the end of this cyclical process, because PDCA is an iterative process.

Figure 1. PDCA Cycle [8]

2.2 PDCA as a Continuous Improvement Stage

Different international institutions such as ISO, OCTAVE, NIST, and COBIT have developed various risk management frameworks. Each framework, however, has its own characteristics, specifications, scope, and methodologies [4]. As a consequence, organizations always expend great amounts of time and energy in analyzing and deciding which framework could best suit their needs. Whereas an integrated approach would afford risk management processes to be adapted and tailored by organizations as they align various frameworks with their strategic goals-this is one of the central benefits of integration.

Most risk management frameworks do not directly incorporate the PDCA cycle. The ISO/IEC 27001:2022 standard articulates adoption of the PDCA cycle most clearly, even though it itself is not a risk management framework but rather a broad guideline for setting up an ISMS [9]. This is unlike the NIST Cybersecurity Framework (NIST CSF), which uses a cyclic construct of Identify, Protect, Detect, Respond, and Recover, though its architectural constructs do not symbolize explicit PDCA, yet shares similar iterative principles [10]. In essence, the PDCA cycle is an important tool for ICT risk management as it offers an organized way for assessing and aiding process improvement over time. Continually evaluating risk through an integrated

risk management process helps govern risk in a continuous series of actions rather than as one-time projects, fostering good governance and informed decision-making [9].

The use of the PDCA method has had several beneficial and noteworthy impacts on the Information Security Management System at SMAN 12 Bandung. By following the PDCA cycle, the school was able to systematically plan, do, check and act to make improvements to the existing information management system. As a result, the level of compliance with the ISO 27001:2013 standard reached 100%, and 81.43% of the procedures were successfully completed. In addition, user confidence in the security measures in place has increased with 80% of students and 88.2% of school operators believing that the aforementioned measures have been completed [11].

PDCA is used as continuous improvement and monitoring of company operations. For Occupational Health and Safety Management System, the Plan stage includes establishing occupational health and safety policies and company objectives, developing a Plan that includes resource allocation, coordination of skills and systems, hazard identification, risk assessment, and control. The Do stage includes implementing occupational health and safety programs. The Check stage focuses on evaluating performance and the responses given. Finally, the Act stage completes the cycle as a whole, as the system must be monitored in the context of continuous improvement and prepared for the next iteration of the cycle. [12]. This research shows that the PDCA method can be used as a continuous improvement innovation by incorporating the Safety Management System Model design to reduce the rates of safety.

Prior research on applying PDCA as a problem-solving methodology is necessary to fully comprehend the issue. Furthermore, they pointed out that PDCA is unable to handle numerous, intricate changes, especially when handling a large-scale study. The effect of PDCA implementation in this study is that researchers may systematically identify and analyze existing problems and provide more integrated solutions to improve efficiency and safety for smartcard users in Brunei Darussalam [13].

Base on the study result at Instansi XYZ, it is concluded that The PDCA method is very beneficial to document development and improve the process of the risk management and successful operation of risk management. The above-mentioned institution is an exception though as it seems the SPBE risk management, as observed in the course of this research, has only been implemented in a low level. In summary, this research illustrates, how, the use of PDCA can serve to enhance, Solidify and make effective, risk management documents and the way that risk management may be smoothly implemented [14].

Originally introduced by Deming in the field of quality management, PDCA has increasingly been recognized as a critical enabler for continuous improvement in dynamic and complex systems, including information security risk management. Within the realm of IT governance and risk, PDCA supports adaptive, structured responses, allowing organizations not only to implement controls but also to evaluate their effectiveness, monitor their impact, and revise their strategies accordingly. While frameworks like ISO/IEC 27001 and ISO 22301 include PDCA as a management principle, most risk-specific framework such as ISO/IEC 27005, NIST SP 800-30, and COBIT 2019, do not explicitly position PDCA as a central component. This

study seeks to fill that gap by formally embedding the PDCA cycle into the final phase of the hybrid risk management framework, establishing a sustainable feedback mechanism that links technical risk processes with strategic governance objectives.

3. Analysis

3.1 Stages of the Hybrid Risk Management and IT Governance Framework

The hybrid framework is a framework resulting from the integration of several frameworks, including ISO 27005, NIST SP 800-30, NIST SP 800-39, ISO 27002 and Cobit 2019. the framework design is carried out using identification, mapping and comparative analysis. then a hybrid framework can be prepared based on the existing IT risk management and governance framework. There are six stages of risk management in this framework. The purpose of this framework is to perform risk management by not only looking at the technical side but also from the governance and strategic side and decisions at the management level. The stages of risk management in this framework include Context Establishment, Risk Identification, Risk Analysis and Evaluation, Risk Treatment/Control Selection, Monitoring and Review and the last stage is Continuous Improvement as shown in the figure 2 below.

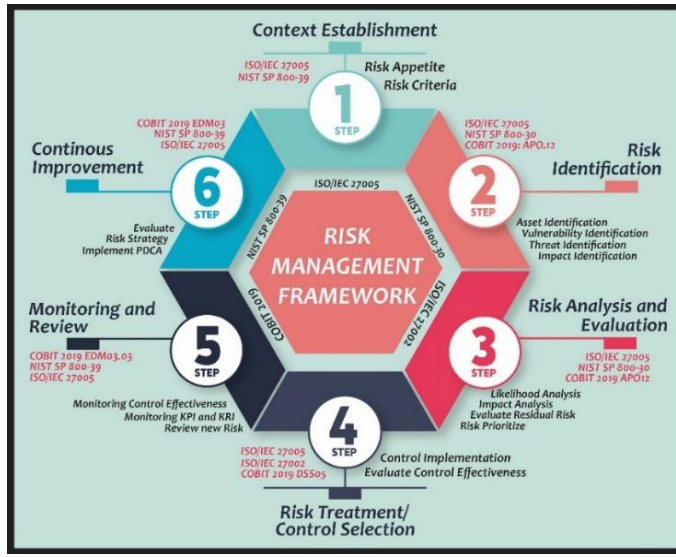

Figure 2. Risk Management Hybrid Framework

a) Context Establishment
This stage uses the adoption of ISO 27005 and NIST SP 800-30. The ISO 27005 framework defines the context setting stage to determine the scope, risk criteria, and environmental factors that affect organizational risk. NIST SP 800-30 defines risk context with a technical approach. The main activity in this stage is the determination of Risk Appetite and Risk Criteria. This is done so that the organization can determine and evaluate the risks to the organization's assets.

b) Risk Identification
This methodology entails recognizing resources, possible dangers, and weaknesses that might impact the ongoing provision of services. ISO 27005 alongside NIST SP 800-30 lays the groundwork for pinpointing technical risks, whereas NIST SP 800-39 and COBIT 2019 broaden the scope of identification to address strategic and governance-related risks.
c) Risk Analysis and Evaluation
This stage uses ISO 27005 to determine likelihood and impact, as well as residual risk after initial controls. The NIST SP 800-30 and NIST SP 800-39 methods are used to assess risk based on technical and system factors. COBIT 2019 is used to determine risk mitigation priorities based on business impact. Risk Level is calculated using likelihood and impact factors. Risk Level is used to determine how a risk affects the organization and determine the mitigation actions required. Risk Levels are categorized as Very Low, Low, Medium, High, and Very High, with higher levels indicating urgency for mitigation. Residual risk is also assessed, by comparing the risks that have been addressed after mitigation or control. Prioritization is determined by risk level, with "Very High" as the primary focus and "High" as a secondary focus.
d) Risk Treatment and Control Selection
This phase consists of choosing and putting into place suitable security measures. ISO 27005 and ISO 27002 offer control guidelines, while COBIT 2019 (DSS05) directs the application of controls within a governance framework. NIST SP 800-39 guarantees that there is consistency between risk reduction efforts and the strategic goals of the organization.
e) Monitoring and Review
The organization continuously monitors the effectiveness of implemented risk controls, including the use of Key Risk Indicators (KRIs) to assess performance. COBIT 2019 (specifically EDM03.03) and ISO/IEC 27002 provide guidance for periodic evaluation and adjustment of security controls, while NIST SP 800-39 enhances the strategic dimension of monitoring by ensuring that risk oversight remains aligned with organizational objectives and changing threat landscapes.
f) Continuous Improvement
The entity assesses how well the risk management strategies are working, utilizing Key Risk Indicators (KRI) as part of this evaluation. Both COBIT 2019 (EDM03.03) and ISO 27002 facilitate assessment efforts and regular modifications to these strategies, while NIST SP 800-39 enhances the overarching aspect of the monitoring procedures.

The application of the PDCA cycle at this stage essentially aims to strengthen the organization's security posture [15]. This includes the ongoing management of organizational assets in response to evolving risk exposures. In the hybrid risk management framework, the continuous improvement phase serves as an important integrative component, embedding the PDCA cycle to ensure that risk related processes are not only performed but also evaluated and improved periodically. In the Plan stage, organizations revisit their risk objectives, assess the performance of previous strategies, and identify newly emerging threats. The Do stage focuses on executing the updated

risk treatment plan and implementing relevant control measures. During the Check stage, KRI are analyzed, past incidents are reviewed, and the effectiveness of existing and new controls is critically assessed. Finally, the Act stage initiate the necessary corrective actions, security policy updates and knowledge-based improvements. PDCA is a cycle that continues to repeat itself, so after the Act stage, it does not stop there, the organization is required to repeat the risk checks that have been repaired to see whether there are still gaps or whether they have improved. This iterative process ensures that risk management remains dynamic, contextually relevant and strategically responsive, shifting the organization's approach from a static and reactive stance to one that is proactive and constantly evolving.

3.2 Framework Validation

This hybrid framework is validated using two methods: 1) Testing the implementation of the framework at Directorate ABC, Agency XYZ, and 2) using the expert judgment method from authorized persons in the organization for risk management. The purpose of this validation is to assess the feasibility and suitability of the risk management framework and IT governance in non-profit organizations. In addition, it is also carried out to ensure that the implementation of PDCA can optimize risk management.

3.2.1 Framework Implementing Test

In the first validation, a trial of the framework implementation was conducted at the ABC Directorate, XYZ Agency. The implementation test was conducted to ensure that the IT risk management and governance framework can be applied to non-profit organizations, in this case XYZ Agency which is a non-profit government organization. Risk management is carried out based on a hybrid framework with six stages and seventeen (17) activities. The stages implemented as shown in Figure 2 starting from Context Establishment, Risk Identification, Risk Analysis and Evaluation, Risk Treatment, Monitoring and Review and Continuous Improvement. The use of PDCA is closely related to the previous risk management stages and its implementation is driven by the results of risk evaluation and risk monitoring activities. Of the total 41 assets identified, the results showed that seven assets were included in the very high and high categories, which are the organization's priorities because they have a high risk to assets. This score indicates not only a high possibility of a security incident but can have an impact on the organization. The risk level is obtained from quantitative calculations with the following formula:

$$Risk\ Level = Likelihood\ Level \times Impact\ Level$$

The results of the risk level calculation are documented in table 1 below. The table shows seven assets that have the Very High and High risk categories as the main priority for mitigation and special treatment from the organization.

After the Risk Level is obtained, the process continues to the next stage, risk analysis and evaluation, control implementation, monitoring review using Key Risk Indicator (KRI), then continued to the Continuous Improvement stage. At this stage, the PDCA Cycle is applied to priority assets. These assets are obtained from the results

Table 1. Risk Level

No	Code	Asset	Likelihood	Impact	Risk Level	Risk Category
1	HW001	Server Database	5 (Very High)	5 (Very High)	25	Very High
2	HW007	Network-Attached Storage	5 (Very High)	5 (Very High)	25	Very High
3	HW012	Server Website XYZ	5 (Very High)	4 (High)	20	High
4	HW015	Server CSIRT	4 (High)	5 (Very High)	20	High
5	SW002	Aplikasi Simpeg	4 (High)	4 (High)	16	High
6	SW007	Aplikasi Lapor CSIRT	4 (High)	4 (High)	16	High
7	DOC001	Data Pegawai	5 (Very High)	5 (Very High)	25	Very High

of monitoring and review, which after control and KRI monitoring are carried out there is no change, or even an increase in the risk level. Table 2 shows the application of PDCA to priority assets. The table below shows the current conditions which then become the basis for implementing the plan stage. Then continued with Do, Check and Act. However, the PDCA process is not a process that is run once and finished. PDCA is a cycle that is carried out repeatedly. This allows the organization to conduct a review.

Table 2. Implementing PDCA

No	Code	Asset	Plan	Do	Check	Act
1	HW001	Server Database	Evaluate the effectiveness of data backup and disaster recovery.	Enhance backup systems with geographic redundancy.	Conduct data recovery trials and incident log analysis.	Refine backup policies with automation and real-time monitoring.
2	HW007	Network-Attached Storage	Identify weaknesses in data encryption protection.	Implement end-to-end encryption on NAS.	Test encryption effectiveness against unauthorized access.	Integrate periodic encryption key rotation policies.
3	DOC001	Data Pegawai	Evaluate employee data breaches and unauthorized access	Tighten access controls with multifactor authentication.	Conduct regular access audits of employee data	Adjust access policies based on the principle of least privilege.

No	Code	Asset	Plan	Do	Check	Act
4	HW015	Server CSIRT	Analyze the effectiveness of cyber incident detection and response.	Update SIEM systems for more accurate log correlation.	Evaluate incident response and perform forensics on attacks that occur.	Conduct regular CSIRT training and update incident SOPs.
5	SW002	Aplikasi Simpeg	Review API authentication and control mechanisms	Implement Role-Based Access Control (RBAC) and API Gateway Security.	Analyze unauthorized access attempts through APIs	Tighten API rate limiting and improve automated audit logs.
6	HW012	Server Website XYZ	Evaluate the effectiveness of protection against DDoS attacks	Adjust the configuration of the Web Application Firewall (WAF) and implement cloud-based load balancing.	Conduct simulation attacks (penetration testing)	Adopt threat intelligence to monitor traffic anomalies.
7	SW007	Aplikasi Lapor CSIRT	Identify potential manipulation of incident reports.	Strengthen report validation and implement immutable records-based logging	Evaluate the effectiveness of data validation and reporter authentication.	Apply AI to detect anomalous patterns in incident reports.

The assets documented in Table 2 are closely linked to the risk evaluation and monitoring stages, as these assets—having high residual risk levels—require continuous management. Risk evaluation and monitoring serve as the foundation for the Plan phase, where the organization analyzes existing control weaknesses and identifies more effective mitigation strategies, thereby initiating the implementation of the PDCA cycle.

At the Plan stage, organizations are required to formulate a control strategy, or determine limits based on residual risk analysis and KRI monitoring. This is done to consider existing control gaps, risk shifts, and current operational needs. For example, on the Database Server, the organization plans improvements to the backup system and disaster recovery plan by considering the shortcomings of existing controls.

The next stage is the Do stage, the organization is required to make the implementation of a mitigation plan through the application of both technical and administrative controls, such as reconfiguring the backup system, strengthening multifactor authentication, implementing data encryption or updating security software. This is done in a structured and documented manner that is in line with the organization's internal capacity and policies. The main thing that is also important is that the implementation

is prioritized based on the level of asset risk.

In the Check phase, the organization reviews the effectiveness of the controls deployed. Activities include security audits, log analysis, functionality testing (such as penetration testing or simulated attacks), and assessment of key performance indicators. These results are then compared against the security objectives outlined during the Plan stage. For instance, following the implementation of encryption on the NAS device, its effectiveness in preventing unauthorized access was evaluated and documented as part of the control assessment.

At the Act stage, this requires corrective action against what was produced at the Check stage. If the control is ineffective, the organization can revise the control, upgrade the device, revise the SOP or even if possible revise the policy, but this will be very complicated bureaucracy. At this stage it can also include employee training. So the implementation of PDCA is not only intended to overcome deficiencies in technical matters, but also to strengthen risk governance to be more strategic and adaptive to developing threats.

3.2.2 Expert Judgement Validation

Validation with expert judgment was carried out by involving four qualified people from XYZ Organization. The validation process was carried out using a structured questionnaire consisting of 34 implementation recommendations from 17 activities. Each validator was asked to assess each recommendation by selecting "Agree" or "Disagree" and was asked to provide feedback and suggestions for improvement through the column provided. All validators agreed on each implementation recommendation provided in this study. The validators consist of seven people, comprising four internal members from the ABC Directorate and three external members. The external validators are experts in the fields of risk management and cybersecurity with more than five years of experience.

After validation with expert judgment, calculations were performed using the Content Validity Index (CVI). CVI was chosen as the primary validation metric because it specifically measures expert consensus on the relevance of items, making it easy to interpret and apply in the development of research instruments. Additionally, CVI provides a clear indication of the proportion of experts who agree on the importance of each item, making it highly suitable for validation purposes [16]. From the calculations using the CVI method, an average CVI of 1.00 was obtained, which, based on the Lawshe Table, has a critical threshold value of 0.99 for seven validators. Thus, the validation results indicate that the recommendation for application within the hybrid framework is valid and has a strong level of content relevance. The CVI calculation result is 0.941 and falls into the “very good” category.

Based on the validation results, all validators have provided feedback and constructive recommendations regarding the implementation of the framework in XYZ Organization. The results show an agreement that the hybrid framework can be understood practically and easily used in organizations. In particular, experts recognized the inclusion of a special phase for continuous improvement in the framework, which allows organizations to proactively and continuously identify risks associated with critical assets.

4. Discussion

The PDCA cycle is integrated as the final phase of the hybrid framework developed in this research, with purpose to establishing a continuous improvement mechanism for information security risk management. The implementation of PDCA was tested at Directorate ABC, Institution XYZ, focusing on seven priority assets identified as having high to very high risk levels. The success of PDCA implementation was evaluated through three main dimensions: the regularity of the cycle's execution, the measurability of results, and the organization's ability to adapt to changing risks.

In the first dimension, the execution of the PDCA cycle demonstrates a systematic mechanism for redesigning risk mitigation steps. The Plan stage successfully reveals weaknesses in existing controls while also formulating improvement plans that are more aligned with organizational needs. In the Do stage, planned mitigation actions are implemented in a targeted manner, such as adjusting backup policies and reconfiguring access controls. The Check stage is then carried out through audits, log analysis, and functional testing to assess the effectiveness of the controls that have been implemented. The Act stage produces corrective actions such as policy updates, technical improvements, and the development of new procedures to strengthen system resilience in the long term.

Quantitatively, the application of PDCA has proven to increase the consistency of controls over high-value assets. Monitoring through a tracking table shows that all seven priority assets have undergone the entire PDCA cycle with measurable results. For example, for the Server Database asset, the effectiveness of backup controls increased significantly after the implementation of redundancy systems and data recovery testing. Meanwhile, the Simpeg application experienced a decrease in unauthorized access incidents thanks to the implementation of Role-Based Access Control (RBAC), which had previously been identified as a weak point in access management.

From the perspective of adaptive response, the PDCA cycle provides flexibility for the organization to adjust strategies in response to evolving risk dynamics. The iterative process of PDCA not only allows for revisions to technical controls but also encourages adjustments to work procedures and the strengthening of human resource capacity, such as retraining the CSIRT team. Thus, PDCA does not focus solely on evaluating technical aspects but also strengthens organizational governance and culture in facing risks.

Based on the implementation test results, the PDCA cycle has proven to play a crucial role in bridging risk evaluation outcomes with concrete improvement actions. Integrating PDCA as the final phase in the hybrid framework makes the risk management process more dynamic, proactive, and oriented toward continuous learning. The effectiveness of PDCA in the context of this research lies not only in the systematic nature of the cycle but also in its ability to build organizational resilience against continuously evolving threats.

5. Conclusion

This research has specifically succeeded in optimizing information technology risk management through the implementation of a continuous improvement stage based on the PDCA cycle within a hybrid framework. The results of implementation

at Directorate ABC, a government non-profit organization, demonstrate that this approach is effective in enhancing IT risk governance, particularly through adaptive capabilities in response to evolving threats and the strengthening of a culture of learning and continuous improvement. The hybrid framework, which integrates international standards such as ISO 27005, NIST SP 800-30, NIST SP 800-39, ISO 27002, and COBIT 2019, not only strengthens technical and compliance aspects but also ensures that the risk management process remains relevant to organizational needs.

The main contribution of this research is the demonstration that optimization of IT risk management can be achieved through the application of a hybrid framework that explicitly integrates a continuous improvement stage based on the PDCA cycle. The results of implementation and expert judgement validation at Institution XYZ indicate that this framework can be easily adopted, supports continuous improvement processes, and strengthens organizational resilience in the face of information technology risks.

For future research, it is recommended that this framework be tested in other organizations with different profiles in order to assess its scalability and flexibility. Additionally, organizations may consider the use of automation systems based on GRC (Governance, Risk, and Compliance), as well as real-time integration with risk indicator dashboards (KRIs), to further enhance the efficiency of risk monitoring.

References

[1] *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*. International Organization for Standardization, 2022.

[2] I. M. M. Putra and K. Mutijarsa. "Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005". In: *3rd 2021 East Indonesia Conference on Computer and Information Technology (EIConCIT)*. IEEE, 2021, pp. 14–19. DOI: 10.1109/EIConCIT50028.2021.9431865.

[3] M. L. Herman et al. *Managing Risk in Nonprofit Organizations: A Comprehensive Guide*. John Wiley & Sons.

[4] A. Fitri, K. Dewi, and Y. Suryanto. "Desain Kerangka Kerja Manajemen Risiko Keamanan Informasi Berdasarkan Kajian Risk Profiling pada Sektor Kesehatan". In: *Jurnal Keamanan Informasi* ().

[5] M. Al Fikri et al. "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization". In: *Procedia Computer Science* 161 (2019), pp. 1206–1215. DOI: 10.1016/j.procs.2019.11.234.

[6] M. Silaban. "Perancangan Desain Kerangka Kerja Keamanan Informasi untuk Mengukur Tingkat Kapabilitas dan Manajemen Risiko Berdasarkan Cobit 2019 dan NIST SP 800-30". Universitas Indonesia, 2023. URL: https://lib.ui.ac.id/detail?id=9999920526196&lokasi=lokal.

[7] Information Systems Audit and Control Association. *COBIT 2019 Framework: Introduction and Methodology*. ISACA, 2018.

[8] D. A. Taufik. *PDCA Cycle Method Implementation in Industries: A Systematic Literature Review*. 2020. URL: http://publikasi.mercubuana.ac.id/index.php/ijiem.

[9] R. Fauzi and M. Lubis. *Assessment Framework for Defining the Maturity of Information Technology within Enterprise Risk Management (ERM)*. URL: https://www.ijacsa.thesai.org.

[10] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. Tech. rep. National Institute of Standards and Technology, 2018. DOI: 10.6028/NIST.CSWP.04162018.

[11] A. C. Pamungkas, W. S. Hulu, and R. Samihardjo. "Information Security Risk Management Web-Based Final Semester Summative Assessment Application Using ISO 27001:2013". In: *Journal of Information Systems and Informatics* 6.1 (2024), pp. 349–362. DOI: 10.51519/journalisi.v6i1.668.

[12] L. Arteaga-Romani et al. "Model of a Safety Management System through Continuous Improvement (PDCA) for Artisanal Mining". In: *9th International Conference on Innovation and Trends in Engineering (CONIITI)*. IEEE, 2023. DOI: 10.1109/CONIITI61170.2023.10324037.

[13] F. A. Thani and M. Anshari. "Maximizing Smartcard for Public Usage: PDCA and Root Cause Analysis". In: *International Journal of Asian Business and Information Management* 11.2 (2020), pp. 121–132. DOI: 10.4018/IJABIM.2020040108.

[14] I. G. P. K. Juliharta et al. "Analysis and Design of Risk Management System of Electronic Government (E-Government)". In: *P-ISSN Journal* (2023).

[15] M. R. Lullah, I. W. W. Pradnyana, and N. T. Hadi. "Design of IT Risk Control in the Computer Laboratory Using the ISO 27001:2022 Framework". In: *International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*. IEEE, 2024, pp. 1056–1061. DOI: 10.1109/ICIMCIS63449.2024.10957330.

[16] W. D. Puspitasari and F. Febrinita. "Pengujian Validasi Isi (Content Validity) Angket Persepsi Mahasiswa Terhadap Pembelajaran Daring Matakuliah Matematika Komputasi". In: *Focus ACTion Of Research Mathematic* 4.1 (2021). DOI: 10.30762/factor-m.v4i1.3254.