Equivalent: Jurnal Ilmiah Sosial Teknik
Volume 8, Issue 4, 1489-1500
e_ISSN: 2775-0833
https://jurnalequivalent.id/index.php/jequi/index
DOI: doi.org/10.59261/jequi.v8i4.410

Assessing CI/CD Pipeline Governance Maturity Using the ITIL v4 Framework: A Case Study of an Indonesian Digital Wallet

Garvin Moses Tanuwihardjo*
Universitas Bina Nusantara, Indonesia

Sfenrianto
Universitas Bina Nusantara, Indonesia

***Corresponding author:**
Garvin Moses Tanuwihardjo, Universitas Bina Nusantara, Indonesia.
✉garvin.tanuwihardjo@binus.ac.id

Article Info:

Article history:
Received: July 09, 2026
Revised: August 27, 2026
Accepted: September 02, 2026
Available Online: September 07, 2026

Keywords:
CI/CD; Fintech; IT Governance; ITIL v4; Maturity Assessment.

This is an open access article under the CC BY-SA license.

Copyright © 2026 by Author. Published by Politeknik Siber Cerdika International

Abstract

Background: Digital wallet services depend on frequent software delivery while operating under stringent requirements for availability, security, and accountability. In such environments, extensive CI/CD automation does not necessarily imply an equally mature governance framework.
Objective: This study assesses the extent to which technical automation in a CI/CD pipeline is accompanied by mature governance practices in an Indonesian digital wallet organization using five ITIL 4 practice domains.
Methods: A single-case mixed-methods design combined Likert-scale maturity scoring with semistructured interviews, direct observation, and document review. The assessment covered Change Enablement, Release Management, Deployment Management, Continual Improvement, and Information Security Management, with quantitative findings triangulated against operational evidence.
Results: Change Enablement (3.4), Release Management (3.0), Deployment Management (3.4), and Information Security Management (3.2) were classified at the Defined maturity level, whereas Continual Improvement (2.6) remained at the Repeatable maturity level. Gap analysis against an ideal score of 4.5 identified the largest gap in Continual Improvement (1.9), followed by Release Management (1.5), Information Security Management (1.3), and Change Enablement and Deployment Management (1.1 each).
Conclusion: The case demonstrates that substantial CI/CD automation can coexist with uneven governance maturity. Governance is comparatively standardized across change, release, deployment, and security practices, but continual improvement remains less institutionalized, indicating that technical capabilities have advanced faster than systematic organizational learning and performance improvement.

To cite this article: Tanuwihardjo, G. M., & Sfenrianto. (2026). Assessing CI/CD Pipeline Governance Maturity Using the ITIL v4 Framework: A Case Study of an Indonesian Digital Wallet. *Equivalent: Jurnal Ilmiah Sosial Teknik*, 8(4), 1489-1500. https://doi.org/10.59261/jequi.v8i4.410

INTRODUCTION

Digital-wallet platforms operate in a high-availability environment in which software failures can interrupt payments, expose customers to service disruptions, and erode trust. As transaction volume and service dependence increase, release speed must therefore be balanced with reliability, security, and accountable change control (Belmonte et al., 2024; Loureiro et al., 2024).

The governance problem is therefore not simply how quickly or frequently a pipeline deploys software, but whether rapid delivery remains controlled, auditable, and aligned with service-management objectives. A pipeline can deploy frequently while still exhibiting weak

approval discipline, inconsistent rollback planning, incomplete security checks, or limited learning from failed changes. In a regulated digital-payment context, such weaknesses create operational and accountability risks (Santosa & Mulyana, 2023; Stamme, 2022).

Prior CI/CD research has primarily emphasized technical automation, toolchains, containerization, cloud deployment, and delivery performance (Fluri et al., 2024; Ghaleb et al., 2026; Manolov et al., 2025; Rostami Mazrae et al., 2023). These studies demonstrate the engineering value of automation but provide less evidence on how governance practices become institutionalized around automated pipelines, especially in high-risk financial services.

ITIL v4 provides a service-management perspective that can complement DevOps by evaluating how change, release, deployment, security, and continual improvement are governed as organizational practices rather than merely executed as technical steps (Baradari et al., 2023; Ernawati & Wang, 2023; Gazi et al., 2024). This perspective is relevant because automation may standardize execution without ensuring equivalent maturity in authorization, measurement, organizational learning, or security governance.

The research gap lies in this separation between technical CI/CD capability and organizational governance maturity. Existing studies have largely examined CI/CD from an automation perspective, whereas fewer studies treat the pipeline as a governed information-system artifact whose daily operation institutionalizes service-management controls. The present case uses operational records from January to September 2025, including deployments, rollbacks, and incidents, to examine whether automation is accompanied by mature governance practices.

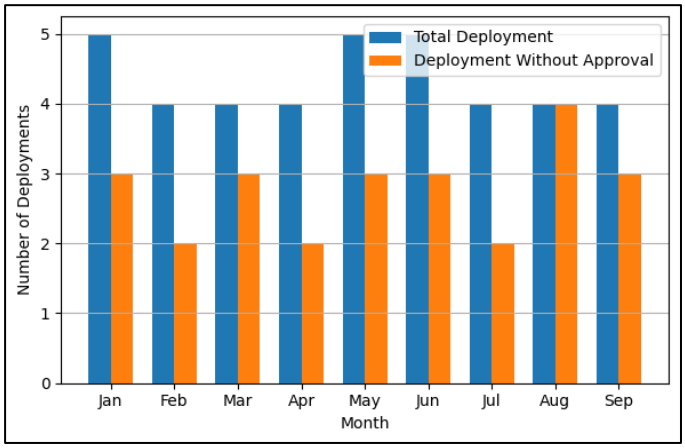

Figure 1. A side-by-side comparison of all deployments and those that were done without the formal organizational approval

Figure 1 displays the total number of deployments and the number of deployments carried out without formal organizational approval over a nine-month period. The pattern is readily apparent: deployments were not always approved, and such occurrences were not merely occasional. This suggests that the regulations governing authorization for changes tend to function more like recommendations than standard rules. This type of flexibility might assist teams in completing urgent work quickly, but it also indicates that the CI/CD pipeline's Change Enablement practice has not yet reached a high level of maturity. Individuals may perceive speed as more important than having a clear process for obtaining approval and maintaining accountability.

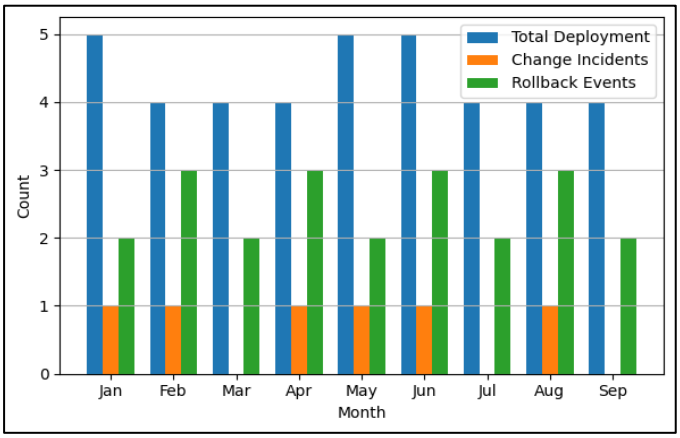

Figure 2. Total deployments, change incidents, and rollback events happen in the CI/CD pipeline.

Figure 2 builds on this by showing the total number of deployments alongside incidents that occurred after changes and rollback events that followed those changes. The relatively high number of rollbacks following deployments suggests that release-readiness checks and post-deployment controls may not always be applied consistently. Some rollbacks are expected in iterative delivery. However, the recurrence of these patterns indicates that Release Management and Deployment Management practices are not yet performing as effectively within the pipeline as they could be.

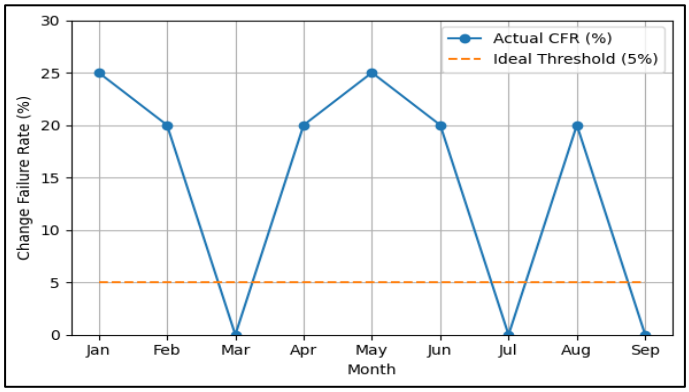

Figure 3. Change Failure Rate (CFR) in comparison with the ideal governance threshold.

Figure 3 adds another layer by showing how the monthly Change Failure Rate (CFR) compares with the target five-percent maturity threshold. In practice, the CFR exceeded this threshold more frequently than would be expected for a mature governance environment. This suggests that a substantial proportion of changes continued to negatively affect service performance. Such outcomes may be partly attributable to the speed of delivery. However, the repeated occurrence of threshold exceedances indicates a broader issue: evaluations of changes, structured feedback mechanisms, and risk awareness practices that could identify fragile releases at an earlier stage have not been implemented effectively.

These patterns illustrate the difficulty of integrating service governance into CI/CD environments. A digital-wallet company in Indonesia was examined in this study, and the findings indicate that extensive automation and frequent releases do not necessarily result in stronger governance. Deployments may occur even without formal authorization from the responsible manager or supervisor. Moreover, the criteria for determining when a change process should be concluded may differ across teams. Readiness assessments are not always conducted consistently, security scans do not necessarily cover the entire pipeline, and ongoing improvement activities are not always systematically documented.

This study conceptualizes the CI/CD pipeline as a governed information-system artifact and evaluates it through five ITIL v4 practices: Change Enablement, Release Management, Deployment Management, Information Security Management, and Continual Improvement. The central research problem is: To what extent does technical automation in CI/CD translate into

mature governance practices within an Indonesian digital-wallet organization?

Accordingly, the study aims to (1) quantify the maturity level of the five selected ITIL v4 practices, (2) identify governance gaps between the observed and target maturity levels, and (3) explain the operational causes of those gaps through interviews, observation, and documentary evidence. Its contribution is to extend CI/CD evaluation from technical delivery performance to the institutionalization of governance within an automated DevOps environment.

METHOD

The study employed a single-case mixed-methods design. Quantitative maturity scores provided a structured assessment of the selected ITIL v4 practices, while interviews, direct observation, and document review were used to explain why particular scores emerged and to verify whether reported practices were reflected in day-to-day operations (Denny & Weckesser, 2022; Naeem et al., 2023; Wright et al., 2026).

The case organization, anonymized as PT XYZ, was an Indonesian digital-wallet provider that operated a CI/CD pipeline supporting frequent application releases in a governance-sensitive financial-services environment. The organization was anonymized to protect confidentiality. A single-case design enabled close examination of approval practices, deployment controls, rollback behavior, security checks, and improvement routines, although the findings were analytically rather than statistically generalizable beyond the case.

The evaluation framework used service-management practices to provide a comprehensive perspective on the governance of IT-enabled services. This framework did not merely view the CI/CD pipeline as a *DevOps* tool; rather, it considered the pipeline a fundamental information-system artifact that affected governance. This perspective recognized that the pipeline performed functions beyond simply moving code from the commit stage to production. The pipeline shaped how services were delivered, how risks were managed, and how teams and stakeholders collaborated to create value while controlling operational risks.

According to the initial testing and review of ongoing operational issues, five ITIL v4 practices were selected for more in-depth investigation.

1) Change Enablement
2) Release Management
3) Deployment Management
4) Information Security Management
5) Continual Improvement

In short, these practices addressed several important governance issues, including how changes were handled, how quality was maintained, how deployments were performed consistently, how security requirements were addressed, and how improvement efforts were sustained over time. The study employed a five-level model consistent with ITIL v4, progressing from the Initial stage to the Optimized stage, to make governance maturity tangible rather than abstract. This structure was used to compare the current state of the CI/CD pipeline with a more organized and idealized governance state. Table 1 lists the characteristics of each maturity level used in this assessment.

Table 1
Description of Maturity Levels Used in the Assessment

Maturity Level	Description
Initial	Processes are performed in an ad-hoc manner and are not formally documented.
Repeatable	Processes are performed repeatedly but are not yet standardized across the organization.
Defined	Processes are formally documented and standardized.
Managed	Processes are monitored and performance is measured using defined metrics.
Optimized	Processes are continuously improved based on performance evaluation and feedback.

Data collection was conducted using triangulation, drawing on information from multiple sources rather than relying excessively on a single source. This approach is commonly used in information-systems evaluation because different types of evidence can reveal different aspects of organizational practice. The study used structured questionnaires, semi-structured interviews, and direct observation to compare formal responses with participants' accounts and actual day-to-day operations.

A structured questionnaire based on ITIL v4 practice components was used to collect quantitative data. The instrument was then adapted to better reflect the realities of a CI/CD pipeline. The questions were based on a five-point Likert scale aligned with the maturity levels. This approach made it possible to translate governance practices into measurable values that could be compared and analyzed across domains. The questionnaire functioned as a practice-level governance diagnostic rather than as a latent psychometric scale. For this reason, internal-consistency coefficients such as Cronbach's alpha were not treated as the primary validity criterion; instead, credibility was strengthened through triangulation with interviews, operational logs, direct observation, and organizational documentation.

Ten individuals who worked directly with the pipeline on a day-to-day basis were administered the questionnaire. The group included DevOps engineers, software developers, release managers, IT security officers, and IT governance personnel. Purposive sampling was used. For questions concerning governance maturity, the perspectives of individuals who owned the relevant processes and were responsible for their outcomes were considered more relevant than those of individuals who only observed the system from a distance. Participants were purposively selected because they had direct responsibility for CI/CD-related deployment, change, release, security, or governance activities and were familiar with the organization's operational governance processes. The respondent group included DevOps engineers, software developers, release managers, IT security officers, and IT governance personnel.

Semi-structured interviews explored how change approval, release decisions, deployment controls, rollback procedures, security checks, and improvement activities were performed in practice. Interview material was organized according to the five ITIL v4 practice domains so that the qualitative evidence remained directly linked to the quantitative evaluation framework.

Interview notes were coded thematically using the five ITIL v4 practices as a priori categories, with additional operational themes recorded when they helped explain discrepancies between questionnaire scores and observed practices. Qualitative findings were then triangulated with direct observation, Jenkins logs, deployment records, and available process documentation before being integrated with the maturity scores.

Direct observation of the CI/CD processes was conducted to identify practices beyond those described in written procedures. The study examined how the pipeline operated, how approvals were managed by the system, and how deployment, rollback, and security checks were handled under time constraints. The research therefore examined not only what participants reported but also how the pipeline was configured, how tools were used, and how the processes were documented. These materials helped connect the survey responses and interview accounts with actual operational practices, thereby increasing the reliability and credibility of the findings.

Quantitative and qualitative evidence were integrated sequentially. First, questionnaire ratings were averaged to obtain a maturity score for each ITIL v4 practice. Second, interview, observation, and documentary evidence were examined to confirm, qualify, or explain the score. This integration prevented maturity classifications from being interpreted solely as numerical self-reports.

The study employed gap analysis to assess conformity with governance expectations. In this step, the observed maturity level was compared with an ideal level of governance based on ITIL v4 [8], (Ernawati & Wang, 2023), [14]. The Managed-to-Optimized range was selected as the ideal target in this case. This range was considered appropriate for an environment characterized by frequent releases and high operational risk. The gap for each practice indicated how far the current implementation was from the target governance condition. It also indicated where governance improvements might be most needed.

$$GAP_j = Ideal\ Score_j - Actual\ Score_j$$

For practice j, the governance gap was calculated as G_j = I_j - A_j, where I_j is the target maturity score (4.5) and A_j is the observed average score. Larger positive gaps indicate greater distance from the target governance condition and therefore higher improvement priority. Average scores were mapped to the predefined maturity ranges shown in Table 2.

Table 2
Mapping of Average Scores to Maturity Levels

Average Score	Maturity Levels
1.00 - 1.99	Initial
2.00 - 2.49	Repeatable
2.50 - 3.49	Defined
3.50 - 4.49	Managed
4.50 - 5.00	Optimized

Maturity scores for each ITIL v4 practice were calculated as the arithmetic mean of respondent ratings across the predetermined indicators assigned to that practice. Equal weighting was used so that no individual questionnaire item was given greater influence without an empirically justified weighting scheme. Practice-level means were calculated within each domain before being compared with the maturity ranges in Table 2, thereby preventing a practice with more indicators from mechanically dominating another practice's score.

Gap analysis was used to identify differences between the observed maturity levels and the governance levels expected under ITIL v4. Each gap was measured and classified to facilitate the prioritization of improvement areas. This stage did not merely quantify differences; it translated the assessment results into actionable information about governance, indicating where improvement efforts were most likely to have the greatest impact.

Qualitative evidence from interviews, observations, and documents was analyzed thematically and cross-checked against the quantitative scores. Coding categories followed Change Enablement, Release Management, Deployment Management, Information Security Management, and Continual Improvement, with supporting operational evidence used to explain score patterns and identify inconsistencies between formal procedures and actual practices.

Throughout the analysis process, ethical standards were strictly followed. The identities of the organization and its members were kept confidential to protect individual privacy, and all participants provided informed consent before data collection. The statistical data collected during the research were used solely for analytical purposes. In addition to ethical considerations, the methodology was examined to ensure its effectiveness. The methodological rigor and reliability of the study were strengthened by using data from multiple sources, clarifying the indicators, and following established IT service-management principles.

RESULTS AND DISCUSSION

Results

Overall CI/CD Governance Maturity

The maturity assessment produced the following practice scores: Change Enablement 3.4 (Defined), Release Management 3.0 (Defined), Deployment Management 3.4 (Defined), Continual Improvement 2.6 (Repeatable), and Information Security Management 3.2 (Defined).

Four of the five assessed practices were classified as Defined, while Continual Improvement was classified as Repeatable. The corresponding gap scores against the 4.5 target are reported in Table 4.

ITIL v4 Practices Maturity Assessment

Table 3 shows the maturity assessment results for all ITIL v4 practices examined in this study. Practice scores were derived from the arithmetic mean of the respondent ratings across the indicators assigned to each practice, using equal indicator weights and the maturity thresholds presented in Table 3.

Table 3
CI/CD Pipeline Governance Maturity Based on ITIL v4 Practices

ITIL v4 Practice	Average Actual Score	Maturity Level
Change Enablement	3.4	Defined
Release Management	3.0	Defined
Deployment Management	3.4	Defined
Continual Improvement	2.6	Repeatable
Information Security Management	3.2	Defined

Based on the predefined ranges in Table 3, Change Enablement, Release Management, Deployment Management, and Information Security Management were classified as Defined, whereas Continual Improvement was classified as Repeatable.

Continual Improvement recorded the lowest maturity score (2.6) and the largest gap from the target (1.9).

Analysis of the Governance Gap

This analysis examines the observed maturity scores and compares them with the ideal conditions defined by ITIL v4 to provide a clearer assessment of the effectiveness of governance alignment. The target score was 4.5, which represents a maturity level between Managed and Optimized. This benchmark is appropriate for high-risk and high-frequency deployment environments, such as digital wallet services, where governance must be both rigorous and adaptable to continuous change.

Table 4
GAP Analysis of CI/CD Governance Practices

ITIL v4 Practice	Actual Score	Ideal Score	GAP	GAP Category
Change Enablement	3.4	4.5	1.1	Medium
Release Management	3.0	4.5	1.5	Medium
Deployment Management	3.4	4.5	1.1	Medium
Continual Improvement	2.6	4.5	1.9	High
Information Security Management	3.2	4.5	1.3	Medium

Table 4 reports the difference between each observed practice score and the target score of 4.5. Change Enablement and Deployment Management each had a gap of 1.1, Release Management had a gap of 1.5, Continual Improvement had a gap of 1.9, and Information Security Management had a gap of 1.3.

Change Enablement, Release Management, and Deployment Management fall into the medium gap category, with gap values ranging from 1.1 to 1.5. Specifically, Change Enablement and Deployment Management have gaps of 1.1, while Release Management has the largest gap within this category at 1.5. These results indicate that the organization has established processes for managing changes, coordinating releases, and executing deployments. Most of these practices have been documented and implemented consistently across the organization. However, there is still room for improvement, particularly in strengthening continuous monitoring, performance measurement, and process evaluation. Current governance in these practices is primarily focused on ensuring procedural compliance rather than achieving measurable operational outcomes, such as reducing change failures, improving deployment success rates, and delivering more reliable and predictable releases.

Information Security Management also falls within the medium gap category, with a gap value of 1.3. This indicates that fundamental information security controls and governance mechanisms have been implemented. Nevertheless, further improvements are required to enhance continuous risk monitoring, security performance measurement, and the integration of security practices into the organization's continual improvement initiatives.

In contrast, Continual Improvement has the highest gap among all assessed *ITIL v4* practices, with a gap value of 1.9, placing it in the high gap category. This result suggests that while some improvement activities have been carried out, they have not yet been implemented systematically or consistently throughout the organization. Improvement initiatives tend to be

reactive rather than driven by structured performance evaluation and measurable objectives. As a result, the organization has not fully established a culture of continuous improvement that supports ongoing service optimization and long-term operational excellence.

The numerical results therefore show an uneven maturity profile rather than a uniformly mature governance environment.

Change Enablement

Change Enablement achieved an actual score of 3.4, placing it at the Defined maturity level. This indicates that change request, approval, and documentation processes within PT XYZ's CI/CD pipeline have been formally established and standardized. Risk-based change approval and post-implementation evaluation received the highest scores (4.0), while preparing a rollback plan before every deployment received the lowest score (2.5), indicating inconsistent implementation. Furthermore, interviews with DevOps engineers and software developers, supported by observations of Jenkins logs, revealed that some changes are still implemented without formal risk assessment or approval. Therefore, although the process has been defined, consistent enforcement and monitoring remain key areas for improvement.

Release Management

Release Management achieved an actual score of 3.0, placing it at the Defined maturity level. This indicates that release planning and execution processes have been documented and are generally understood across the organization. The indicators for release authorization before implementation and complete release documentation and version notes received the highest score (4.0). In contrast, release schedule planning and post-release evaluation received the lowest score (2.0), indicating that these activities are not yet consistently implemented. Interview results confirmed the lack of clear standards for post-release evaluation and structured release scheduling. In addition, observations of Jenkins logs revealed that some releases were deployed without formal approval and that version tagging was not consistently applied. Therefore, although Release Management has reached the Defined maturity level, improvements are still needed to ensure consistent release governance and documentation.

Deployment Management

Deployment Management achieved an actual score of 3.4, placing it at the Defined maturity level. This indicates that deployment processes have been standardized and are largely automated through the CI/CD pipeline. The indicators for rollback mechanisms during deployment failures and systematic deployment processes for staging and production environments received the highest score (4.0). However, role-based access control for deployment received the lowest score (2.0), indicating that deployment permissions are not adequately restricted. Interviews with DevOps engineers confirmed that any employee with access to Jenkins can perform deployments, reflecting the absence of role-based access control. Furthermore, although rollback mechanisms are available, interviews and observations revealed that they are still performed manually rather than automatically. Therefore, while Deployment Management has reached the Defined maturity level, strengthening access control and automating rollback mechanisms remain important areas for improvement.

Continual Improvement

Continual Improvement achieved an actual score of 2.6, placing it at the Repeatable maturity level. This indicates that improvement activities have been implemented but are not yet carried out consistently or systematically across the organization. The indicator "The team actively provides feedback for pipeline improvement" received the highest score (4.0), demonstrating strong team participation in identifying improvement opportunities. However, the indicators related to regular evaluation of CI/CD pipeline effectiveness, prioritization of improvements based on evaluation and feedback, and scheduled pipeline evaluations each received the lowest score (2.0), indicating that continual improvement activities are still largely ad hoc. As a result, pipeline improvements tend to be driven by immediate needs rather than by a structured and ongoing improvement process. Therefore, establishing regular evaluation mechanisms and systematically prioritizing improvement initiatives are essential to achieving a

higher level of process maturity.

Information Security Management

Information Security Management achieved an actual score of 3.2, placing it at the Defined maturity level. This indicates that security practices have been established and integrated into the CI/CD pipeline, although some aspects still require improvement. The indicators for role-based access control to code repositories and deployment servers and comprehensive audit logging of user activities and deployment processes received the highest score (4.0), demonstrating effective access management and traceability. However, automated security scanning before code is merged or deployed received the lowest score (2.0), indicating that security validation has not yet been fully integrated into the pipeline. In addition, security testing before production releases and compliance with internal security policies each received a score of 3.0, suggesting that these practices have been implemented but are not yet fully consistent. Therefore, strengthening automated security controls and integrating security checks throughout the CI/CD pipeline remain important areas for improvement.

Summary of Results

The findings indicate that most *ITIL v4* practices have reached the Defined maturity level, showing that governance processes within the CI/CD pipeline are generally documented and standardized. However, their implementation is not yet fully consistent, particularly in monitoring, automation, and governance enforcement. Continual Improvement remains at the Repeatable level because improvement activities are still performed on an ad hoc basis rather than through a structured and continuous approach. Overall, PT XYZ has established a solid governance foundation for its CI/CD pipeline, but stronger governance consistency and continual improvement practices are needed to achieve a higher level of maturity.

Discussion

The results show that CI/CD governance maturity develops unevenly across practices: technical automation and standardized deployment controls can coexist with weaker institutionalization of continual improvement. This pattern supports treating the CI/CD pipeline not only as a delivery tool but also as an information system artifact through which governance routines are embedded, enforced, and measured.

CI/CD Pipelines as Governed Information System Artifacts

The findings indicate that the CI/CD pipeline should be viewed not merely as a software delivery mechanism but also as an information system artifact that embeds governance into daily software development activities. The relatively high maturity of Change Enablement, Release Management, Deployment Management, and Information Security Management demonstrates that governance practices become more standardized when they are integrated into CI/CD tools and automated workflows. Automated deployments, approval workflows, audit logs, and standardized deployment stages naturally encourage process consistency and procedural compliance. This finding is consistent with previous studies emphasizing that CI/CD tools facilitate governance by embedding standardized operational processes into technical workflows (Fluri et al., 2024; Hamsavath et al., 2025; Rostami Mazrae et al., 2023). The theoretical contribution is the distinction between automation maturity and governance maturity. The case indicates that automation can institutionalize repeatable execution, yet higher governance maturity requires organizational mechanisms for measurement, feedback, learning, accountability, and continual improvement that are not produced automatically by the pipeline itself. This extends CI/CD research beyond engineering efficiency toward the institutionalization of IT service management practices in DevOps environments.

However, the results also reveal that automation alone is insufficient to achieve mature governance. Although most operational processes have been standardized, interviews and observations identified inconsistencies in change approvals, release authorization, rollback automation, and automated security validation. These findings indicate that governance maturity depends not only on technical automation but also on organizational discipline and consistent process enforcement.

Governance Challenges Beyond Technical Automation

Among the assessed practices, Continual Improvement exhibited the lowest maturity and the largest gap from the target maturity level. While development teams actively provide feedback for improving the CI/CD pipeline, regular evaluations, structured prioritization of improvements, and scheduled review activities have not yet been institutionalized. Consequently, improvement initiatives remain reactive rather than continuous.

A similar pattern was observed in Information Security Management. Although this practice achieved the Defined maturity level, important security activities, such as automated security scanning, have not yet been fully integrated into the CI/CD pipeline. Previous studies have reported that organizations often prioritize delivery speed over continuous governance activities such as security monitoring and organizational learning, resulting in governance gaps despite highly automated deployment processes (Pan et al., 2024; Saleh et al., 2024; Santosa & Mulyana, 2023; Zmuda et al., 2025). The findings of this study reinforce this argument by showing that governance activities requiring continuous managerial commitment are generally more difficult to institutionalize than operational processes supported directly by automation.

Implications for ITIL v4 Implementation in DevOps Environments

This study demonstrates that ITIL v4 remains applicable in modern DevOps environments when its practices are adapted to automated software delivery processes. Practices closely aligned with CI/CD workflows, such as Change Enablement and Deployment Management, achieved higher maturity because many governance activities can be incorporated directly into the pipeline. Conversely, practices that depend primarily on organizational behavior, including Continual Improvement, showed lower maturity despite the existence of technical automation.

These findings support previous research suggesting that successful ITIL implementation in DevOps environments requires balancing technical automation with organizational governance mechanisms (Ernawati & Wang, 2023; Santosa & Mulyana, 2023; Stamme, 2022). Rather than replacing DevOps practices, ITIL v4 complements them by providing governance structures that improve control, accountability, and service quality.

Implications for Information Systems Governance

From an information systems perspective, this study suggests that governance maturity should not be evaluated as a single organizational capability but rather as a collection of interconnected governance practices that evolve at different rates. Even within the same CI/CD pipeline, operational practices reached higher maturity than organizational learning practices. This finding extends previous studies on information systems governance by demonstrating that governance maturity is multidimensional and influenced by both technical capabilities and organizational factors (Baradari et al., 2023; Capatina et al., 2024; Loureiro et al., 2024; Truong et al., 2024).

Therefore, improving CI/CD governance requires organizations not only to invest in automation technologies but also to strengthen governance mechanisms such as continuous evaluation, standardized monitoring, managerial ownership, and systematic organizational learning. These organizational capabilities are essential for achieving higher governance maturity and sustaining long-term software delivery performance.

CONCLUSION

This study assessed the governance maturity of the CI/CD pipeline at PT XYZ using selected ITIL v4 practices from an information systems governance perspective. Rather than viewing the CI/CD pipeline solely as a software delivery mechanism, this study considered it an organizational information system artifact that embeds governance into software development and deployment processes.

The results show that Change Enablement, Release Management, Deployment Management, and Information Security Management have reached the Defined maturity level, indicating that these governance practices are generally documented and standardized. However, implementation inconsistencies remain in areas such as approval enforcement, release evaluation, rollback automation, automated security validation, and role-based access control. In contrast, Continual Improvement remains at the Repeatable maturity level and exhibits the

largest governance gap, demonstrating that organizational learning and continuous evaluation have not yet been institutionalized.

These findings suggest that technical automation alone is insufficient to achieve mature CI/CD governance. While automation improves process consistency and operational efficiency, sustainable governance also requires continuous evaluation, organizational commitment, and consistent enforcement of governance practices. This study also demonstrates that ITIL v4 can effectively support governance in DevOps-driven environments when its practices are integrated with automated CI/CD workflows while maintaining organizational oversight.

This study is limited to a single case organization within the digital financial services sector. Future research may validate these findings across multiple organizations and industries, investigate governance maturity over longer periods, or extend the assessment by incorporating additional governance and regulatory frameworks to provide a more comprehensive evaluation of CI/CD governance maturity.

ACKNOWLEDGEMENT

The writer wants to say thank you to everyone who assisted with this study from the deep of their heart. We also do not forget to thank to the management and technical teams' organization who have participated and give their times to discuss with us and share their insight, experiences, as well as access to useful materials along the process of study. We thank to the people who assisted us with our analysis and provide us valuable feedback as well. This helped it be more focused and clearer. The author thanks everyone who took the time to fill out the survey or do an interview for their honesty and willingness to help with the research.

AUTHOR CONTRIBUTION STATEMENT

Garvin Moses Tanuwihardjo contributed to the conceptualization, research design, data collection, data analysis, interpretation of findings, and preparation of the original manuscript draft. Sfenrianto contributed to the development of the theoretical framework, methodological validation, critical review, refinement of the manuscript, and supervision of the research process. Both authors participated in revising the manuscript, approved the final version, and agreed to be accountable for all aspects of the research.

REFERENCES

Baradari, I., Shoar, M., & Nezafati, N. (2023). Defining the relationship between IT Service management and knowledge management: Towards improved performance. *Knowledge Management Research & Practice*, *21*(2), 384–396. https://doi.org/10.1080/14778238.2021.1903349

Belmonte, Z. J. A., Prasetyo, Y. T., Cahigas, M. M. L., Nadlifatin, R., & Gumasing, M. J. J. (2024). Factors influencing the intention to use e-wallet among generation Z and millennials in the Philippines: An extended technology acceptance model (TAM) approach. *Acta Psychologica*, *250*, 104526. https://doi.org/10.1016/j.actpsy.2024.104526

Capatina, A., Juarez-Varon, D., Micu, A., & Micu, A. E. (2024). Leveling up in corporate training: Unveiling the power of gamification to enhance knowledge retention, knowledge sharing, and job performance. *Journal of Innovation & Knowledge*, *9*(3), 100530.

Denny, E., & Weckesser, A. (2022). How to do qualitative research? Qualitative research methods. *BJOG: An International Journal of Obstetrics & Gynaecology*, *129*(7), 1166–1167. https://doi.org/10.1111/1471-0528.17150

Ernawati, Y., & Wang, G. (2023). Assessing IT services management with ITIL framework V3: A case study. *Journal of System and Management Sciences*, *13*(4), 152–164. https://doi.org/10.33168/JSMS.2023.0409

Fluri, J., Fornari, F., & Pustulka, E. (2024). On the importance of CI/CD practices for database applications. *Journal of Software: Evolution and Process*, *36*(12), e2720. https://doi.org/10.1002/smr.2720

Gazi, M. A. I., Al Mamun, A., Al Masud, A., Senathirajah, A. R. bin S., & Rahman, T. (2024). The relationship between CRM, knowledge management, organization commitment, customer profitability and customer loyalty in telecommunication industry: The mediating role of customer satisfaction and the moderating role of brand image. *Journal of Open Innovation:*

Technology, Market, and Complexity, *10*(1), 100227.

Ghaleb, T. A., Abduljalil, O., & Hassan, S. (2026). CI/CD Configuration Practices in Open Source Android Apps: An Empirical Study. *ACM Transactions on Software Engineering and Methodology*, *35*(2), 1–40. https://doi.org/10.1145/3736758

Hamsavath, P. N., Katti, V. S., & Pathak, A. (2025). Automated CI/CD Pipeline: A DevOps Approach for Deploy Containerized Applications. *Advances in Communication and Applications: Proceedings of ERCICA 2024, Volume 2*, *1398*, 201–210. https://doi.org/10.1007/978-981-96-4679-1_17

Loureiro, E., Gomes, B., Varajão, J., & Silva, C. (2024). Information systems project success surveys - Insights from the last 30 years. *Heliyon*, *10*(23), e40619. https://doi.org/10.1016/j.heliyon.2024.e40619

Manolov, V., Gotseva, D., & Hinov, N. (2025). Practical Comparison Between the CI/CD Platforms Azure DevOps and GitHub. *Future Internet*, *17*(4), 153. https://doi.org/10.3390/fi17040153

Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A Step-by-Step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research. *International Journal of Qualitative Methods*, *22*, 1–18. https://doi.org/10.1177/16094069231205789

Pan, Z., Shen, W., Wang, X., Yang, Y., Chang, R., Liu, Y., Liu, C., Liu, Y., & Ren, K. (2024). Ambush From All Sides: Understanding Security Threats in Open-Source Software CI/CD Pipelines. *IEEE Transactions on Dependable and Secure Computing*, *21*(1), 403–418. https://doi.org/10.1109/TDSC.2023.3253572

Rostami Mazrae, P., Mens, T., Golzadeh, M., & Decan, A. (2023). On the usage, co-usage and migration of CI/CD tools: A qualitative analysis. *Empirical Software Engineering*, *28*(2), 52. https://doi.org/10.1007/s10664-022-10285-5

Saleh, S. M., Madhavji, N., & Steinbacher, J. (2024). A Systematic Literature Review on Continuous Integration and Deployment (CI/CD) for Secure Cloud Computing. *Proceedings of the 20th International Conference on Web Information Systems and Technologies (WEBIST 2024)*, 331–341. https://doi.org/10.5220/0013018500003825

Santosa, I., & Mulyana, R. (2023). The IT Services Management Architecture Design for Large and Medium-sized Companies based on ITIL 4 and TOGAF Framework. *JOIV: International Journal on Informatics Visualization*, *7*(1), 30–36. https://doi.org/10.30630/joiv.7.1.1590

Stamme, F. (2022). Literature Review on Agile IT-Service Management. In *Seminar IT-Management in the Digital Age (Winter 2022)*. FH Wedel. https://www.fh-wedel.de/fileadmin/Mitarbeiter/Records/Stamme_2023_-_Literature_Review_on_Agile_IT-Service_Management.pdf

Truong, B. T. T., Nguyen, P. V, & Vrontis, D. (2024). Enhancing firm performance through innovation: the roles of intellectual capital, government support, knowledge sharing and knowledge management success. *Journal of Intellectual Capital*, *25*(1), 188–209.

Wright, R., Chapla, K., Booth, A., Nelson, K. E., Peeler, A., Swain, C., Won, S., & Wu, D. S. (2026). Enhancing rigor, quality, and patient engagement in qualitative research: A step-by-step guide to applying reflexive thematic analysis to the experience-based co-design methodology. *Qualitative Health Research*, *36*(9), 915–930.

Zmuda, R., Graves, R., Shepherd, M., & Brookes, S. (2025). SoK: Understanding CI/CD Security: A Comprehensive Review of Architecture, Attacks, and Defenses. *2025 IEEE Secure Development Conference (SecDev)*, 58–68.