

Analysis of the Implementation of Governance, Risk, and Compliance (GRC) in Supporting Information Technology Governance at Bank Pembangunan Daerah Kalimantan Barat

Anistya Fitri Larasati^{1*}, Syarifah Novieyana², Lidya Sri Mulyani³, Marsela Diaz⁴

^{1,2,3,4}Department of Business Administration, Politeknik Negeri Pontianak, West Kalimantan, Indonesia

*Corresponding Author: anistyafitrlarasati@polnep.ac.id

Article History

Received: 22-09-2026

Revised: 27-09-2026

Published: 30-09-2026

ABSTRACT

This study analyzes how Governance, Risk, and Compliance (GRC) is implemented in supporting information technology (IT) governance at Bank Pembangunan Daerah Kalimantan Barat (Bank Kalbar), and how IT utilization supports the implementation of IT GRC. A qualitative approach with a descriptive method was used. Primary data were obtained through in-depth interviews with the Head of the Information Technology Division and an IT GRC staff member, selected through purposive sampling, and were complemented by the Bank's 2025 Annual Report and Governance Report and relevant regulations of the Financial Services Authority (OJK). Data were analyzed through data reduction, data display, and conclusion drawing and verification. The findings show that GRC is implemented through IT policies and procedures, risk identification, assessment, prioritization, control, and monitoring, compliance with regulator requirements and internal SOPs, and IT audits with follow-up. IT in turn supports IT GRC through access control, change management, backup and recovery, security monitoring, IT general and application controls tested through TDE and TOE, and the Digital Resilience Center. Constraints include limited IT development budgets, numerous unit requests, third-party delays, and the time required for audit follow-up. The findings indicate that IT GRC is a continuous process that requires priority setting, vendor monitoring, and follow-up tracking.

Keywords: *GRC, IT Governance, Risk Management, Compliance, Bank Kalbar Ublished*

INTRODUCTION

The development of information technology (IT) has changed banking services, marked by the growing use of digital services. Many banking activities are now supported by IT to facilitate transactions, widen access to services, and improve efficiency. IT is therefore no longer only a supporting tool but an integral part of how banking services are delivered. The

wider the use of IT in banking, the more important it becomes to manage that technology so that services run in a directed, secure, and compliant manner.

The same trend can be seen at Bank Pembangunan Daerah Kalimantan Barat (Bank Kalbar). One example is the use of QRIS to support payment transactions. According to Bank Kalbar as reported by ANTARA News Kalimantan Barat (2025), by 31 December 2024 the number of Bank Kalbar QRIS merchants had reached 14,364, spread across 14 regencies and cities in West Kalimantan and the Jakarta branch office. During 2024, Bank Kalbar recorded 1.33 million QRIS transactions worth IDR 211.96 billion. These figures show that technology-based services are widely used in the Bank's transactions and reach various service areas.

Bank Kalbar's use of IT is also supported by a range of systems and applications. Its annual report (Bank Kalbar, n.d.) states that the Bank has an IT Masterplan and IT Strategic Plan for 2023–2025 that are aligned with its business strategy and regulatory requirements. The Bank operates, among others, a Core Banking System, Banking Integration Services (BIS), mobile banking, virtual accounts, a Cash Management System (CMS), and EDC merchant devices, and in 2024 it developed a BIS Open API to support transactions through partner platforms. System development follows the System Development Life Cycle (SDLC) and takes regulatory requirements into account. For cybersecurity, the Bank refers to the NIST Cybersecurity Framework (CSF) 2.0 (Pascoe et al., 2024) and has applied information security standards, including ISO/IEC 27001 (International Organization for Standardization [ISO], 2022) certification for the CMS application. It established a cyber resilience and security function in April 2024 and was registered as a CSIRT with the National Cyber and Crypto Agency (BSSN) in September 2024.

This extensive use of IT means that banking activities increasingly depend on technology systems and infrastructure, so system availability has become a concern for service delivery. An example is the disruption of five Bank Kalbar ATMs in Ketapang on 14 December 2024, which prevented customers from withdrawing cash, transferring funds, or checking balances (Suara Ketapang, 2024). The Ketapang branch stated at the time that the disruption was related to maintenance from the head office and also affected other locations. The incident illustrates that technology disruptions can directly affect services used by the public.

The use of IT in banking must therefore be accompanied by management that sets the direction of technology use, controls risks, and ensures compliance with applicable regulations. In a case study of a bank in Indonesia, Nurdin (2018) mapped IT governance using COBIT 4.1 and fishbone analysis to identify obstacles, and concluded that stronger IT governance can improve the bank's capacity to deliver accurate and timely information that supports core banking operations and regulatory compliance. Wibowo et al. (2025), analyzing IT projects for digital banking at an Indonesian state-owned bank, identified operational, security, compliance, integration, and third-party or vendor dependency risks. Managing IT in banking thus concerns not only system development but also governance and the management of the risks that accompany it.

This management can be understood through three interrelated aspects: Governance, Risk, and Compliance (GRC). Governance concerns how an organization is directed and supervised in achieving its objectives; risk concerns identifying and managing risks that may affect those objectives; and compliance concerns fulfilling regulations, policies, and requirements. Racz et al. (2010) emphasize that GRC should be treated not as three separate domains but as interconnected organizational functions that require integrated consideration, while noting that the concept had not been adequately researched and lacked a common understanding among professionals. Evidence linking GRC and technology in Indonesian organizations is now emerging. Abdurrahman et al. (2024), using data from 322 respondents from 45 banks in Indonesia, found that digital transformation mediates the relationship between dynamic capabilities and banking performance, and that governance, risk management, and compliance factors further enhance these outcomes. In a study of a listed pharmaceutical company, Tursina (2025) found that IT investment correlated with improvements in GRC, although the small sample limits the validity of the results.

In this study, IT is understood as the use of systems, technology, and information to support banking activities. Governance of IT refers to directing and overseeing IT use so that it is consistent with organizational objectives; in COBIT 2019 this corresponds to the Evaluate, Direct, and Monitor (EDM) processes (ISACA, 2018). The general principles of good governance for commercial banks, namely openness (transparency), accountability, responsibility, independence, and fairness, are stipulated in OJK Regulation No. 17 of 2023 (OJK, 2023) and provide a further reference for interpreting how governance is practiced. IT risk concerns events that may disrupt the achievement of organizational objectives. OJK Regulation No. 11/POJK.03/2022 requires commercial banks to apply risk management in IT operations that covers, at a minimum, risk identification, measurement, monitoring, and control (Otoritas Jasa Keuangan [OJK], 2022). Compliance concerns ensuring that policies, systems, procedures, and activities conform to applicable regulations. OJK Regulation No. 46/POJK.03/2017 defines the compliance function as a set of preventive actions to ensure that a bank's policies, provisions, systems, procedures, and business activities comply with OJK regulations and laws (OJK, 2017), while OJK Regulation No. 11/POJK.03/2022 also requires banks to apply IT policies, standards, and procedures consistently and to review and update them periodically.

Previous studies have examined GRC from several angles. Muziardy and Yuniarti (2025), in a qualitative case study of a rural bank (PT BPR Panjawan Mitra Usaha) based on interviews with its Chief Director and Compliance Division Head, found that the governance function still faced obstacles in SOP implementation and reporting discipline, that risk management was manual and tended to be reactive, and that compliance responsibilities remained consolidated with little organizational culture to support them. They recommended an independent GRC unit and a stronger organizational culture. Fitriani et al. (2024), in a qualitative literature study, conclude that integrated GRC strengthens the effectiveness of internal audit by enhancing accountability, mitigating risks, and supporting organizational sustainability, and positions

internal audit as a strategic partner. Overall, these studies address GRC in a rural bank, in internal audit, and in a non-bank company, and the literature reviewed here offers limited evidence on how GRC is carried out in the day-to-day IT activities of a regional development bank.

The novelty of this study lies in three related emphases. First, it looks beyond the existence of rules and policies to how they are carried out in IT activities such as access control, data protection, system supervision, risk management, incident handling, and regulatory compliance. Second, IT is examined not only as an object governed by IT GRC but also as a means that supports governance, risk management, and compliance. Third, the study is conducted directly at Bank Pembangunan Daerah Kalimantan Barat and links the application of IT GRC to the security and continuity of the services received by customers.

Based on this framework, the study aims to analyze the implementation of GRC in supporting IT governance at Bank Kalbar and to analyze the utilization of IT in supporting the implementation of IT GRC at the Bank. The results are expected to give a clear picture of the activities the Bank undertakes to govern technology, control risks, safeguard data and transactions, and ensure compliance with applicable provisions.

RESEARCH METHOD

Research Design

This study uses a qualitative approach with a descriptive method. Qualitative research is used to understand the condition of the research object in its natural setting, with the researcher as the main instrument (Sugiyono, 2023). The approach was chosen because the study seeks an in-depth understanding of how IT Governance, Risk, and Compliance (IT GRC) is implemented in supporting IT governance at Bank Kalbar, the constraints encountered, and the efforts made to address them. The study does not aim at statistical measurement; the descriptive method is used to present the conditions and implementation of IT GRC based on information obtained from interviews and documentation.

Research Site and Informants

The study was conducted at the head office of PT Bank Pembangunan Daerah Kalimantan Barat (Bank Kalbar) in Pontianak. Bank Kalbar was selected because its banking activities are increasingly supported by IT, which calls for good governance, risk management, and compliance to keep services secure and running smoothly. The study focused on the Information Technology Division, which carries out the GRC function. Two informants were selected through purposive sampling based on their position, knowledge, experience, and involvement in the IT GRC function (Sugiyono, 2023): the Head of the Information Technology Division (Informant 1) and an IT GRC staff member (Informant 2). The research took approximately four months in accordance with the schedule set by the institution's Center for Research and Community Service, covering preparation, data collection, data processing, and analysis.

Data Sources and Instruments

Data consisted of primary and secondary data. Primary data were obtained through in-depth interviews with the two informants on the implementation of IT governance, risk management, and compliance, the constraints encountered, and the efforts made in implementing IT GRC. Secondary data were obtained from documents, namely the Bank's 2025 Annual Report and Governance Report (Bank Kalbar, n.d.), other IT and GRC documents that could be accessed, OJK regulations, and supporting literature. Documentation was used to complement and strengthen the information obtained through interviews (Bahri, 2018). The research instruments were an interview guide, field notes, and a laptop for recording and processing data. The interview guide was prepared according to the research focus so that interviews remained directed, and the analysis was organized around the aspects and indicators summarized in Table 1.

Table 1. Aspects and indicators of IT GRC used in the analysis

Aspect	Indicators	Basis
Governance	IT direction and policy; structure and division of responsibilities; IT decision-making; oversight and evaluation	COBIT 2019, EDM processes (ISACA, 2018)
Risk	Risk identification; risk assessment or measurement; risk monitoring; risk control	OJK Regulation No. 11/POJK.03/2022
Compliance	Conformity with regulations; policies, standards, and procedures; compliance monitoring and evaluation; review and follow-up	OJK Regulation No. 46/POJK.03/2017 and No. 11/POJK.03/2022

Source: Adapted from ISACA (2018) and OJK (2017, 2022)

Data Analysis Technique

Data were analyzed qualitatively and descriptively in three stages, namely data reduction, data display, and conclusion drawing and verification (Miles and Huberman in Sugiyono, 2023). In the first stage, data from the interviews and documents were selected and grouped according to the research focus, namely governance, risk, compliance, and IT utilization. In the second stage, the data were presented descriptively by linking the interview results with the documentation to identify patterns, conditions, and information related to IT GRC and IT utilization. In the final stage, conclusions were drawn and verified to answer the research objectives. Statements made by the informants were also cross-checked against the Annual Report and Governance Report to assess whether they were consistent with the available documentation.

Research Stages

The research was carried out in four stages. In the preparation stage, the researchers compiled the theoretical basis and literature review on IT GRC, IT governance, risk management, and compliance, determined the data sources, and prepared the interview guide and documentation checklist. In the data collection stage, interviews were held with the Head of the Information Technology Division and the IT GRC staff member, and relevant documents were collected and reviewed. In the data analysis stage, the data were reduced, displayed, and verified as described above. In the final stage, the research report was written and recommendations were formulated as input for strengthening IT GRC at Bank Kalbar.

RESULTS AND DISCUSSION

Overview of the Findings

The results are organized around the two research focuses: the implementation of GRC in supporting IT governance, and the utilization of IT in supporting IT GRC. The main data came from interviews with two informants, the Head of the Information Technology Division (Informant 1) and an IT GRC staff member (Informant 2), and were related to Bank Kalbar's 2025 Annual Report and Governance Report to check the consistency between the informants' statements and the available documents.

The findings show that IT GRC at Bank Kalbar is part of IT management through policies and procedures, risk management, compliance with regulator requirements, internal control, audit, and system and information security. IT GRC does not stand alone as an administrative activity; it is connected with the development, use, supervision, and evaluation of IT. Informant 1 explained that the function of IT GRC is to ensure that governance, risk, and compliance run according to requirements, while technical execution is handled by designated units or teams. Informant 2 reinforced this by explaining that IT GRC activities are carried out through monitoring, document checking, risk identification, compliance checks, and follow-up on evaluation results. The documentation is consistent with these statements: the Annual Report shows that the work process of each unit follows standard manuals that are reviewed periodically by the Internal Audit Division, and that the Bank maintains a Business Continuity Plan (BCP), a Disaster Recovery Plan (DRP), and a backup system.

Implementation of GRC in Supporting IT Governance

The first research focus is examined through how IT governance is directed and carried out, how IT risks are managed, how compliance with regulations and policies is applied, and how information security and system reliability are maintained. Monitoring, audit, and follow-up are also examined as forms of supervision over IT management. Table 2 summarizes the findings for each aspect.

Table 2. Summary of IT GRC implementation at Bank Kalbar

Aspect	Interview findings	Documentary evidence
Governance	IT policies are communicated to work units based on IT management procedures, and changes in provisions are immediately informed to the units concerned; IT GRC staff carry out daily monitoring; IT needs of each unit are weighed by business priority, risk level, system readiness, and budget.	Five governance principles (transparency, accountability, responsibility, independence, fairness) are stated in Bank documents; work processes follow standard manuals reviewed periodically by the Internal Audit Division.
Risk	Risks are identified from IT processes and activities (system disruption, information security, access, system changes, applications, infrastructure, third-party work) and prioritized by their impact on the Bank and its services; vendor delays require closer supervision.	Governance Report describes risk identification, measurement, monitoring, control, and reporting; an IT Risk Management function exists and the Cyber Resilience and Security function has been strengthened.
Compliance	OJK regulations are studied and their impact on policies, procedures, and systems is assessed; SOPs and guidelines serve as reference; compliance is checked through audits; certain systems and applications are objects of testing, supervision, and audit.	Discussion and audit of the CMS, Mobile Banking, and Xcard Web; discussion of the ISO 27001:2022 Information Security Management System.
Information security and reliability	Access control, change management, backup and recovery, network and infrastructure security, and security monitoring; layered passwords on customer accounts; quick recovery, activation of backup systems or the Disaster Recovery Center during disruption.	IT controls cover user access review, system change management, backup and recovery, network and infrastructure security, and security monitoring; BCP, DRP, and backup system exist; controls are adequate although security supervision still needs improvement.

Aspect	Interview findings	Documentary evidence
Monitoring, audit, and follow-up	Monitoring checks conformity with policies and procedures; incidents are evaluated for cause, handling, adequacy of controls, and needed improvements; audit findings are monitored until followed up.	Follow-up of OJK examination results meets commitment deadlines and is reported periodically at board meetings; the 2025 IT audit report records residual findings on the DRP and Core Banking System.

Source: Interview and documentation results, 2026

Governance in IT management

Governance in the implementation of IT GRC appears in the existence of policies, procedures, a division of duties, monitoring, and supervision of IT activities. Informant 1 stated that IT policies are communicated to work units by referring to the prevailing IT management procedures, and that any change in provisions is immediately informed to the units concerned so that the performance of duties remains aligned. In terms of accountability, the function of IT GRC is to ensure that IT governance takes into account risk mitigation, compliance with rules, and measurable supervision. Informant 2 added that IT GRC staff exercise oversight through daily monitoring, checking compliance and documents, assisting in risk mapping, and following up on findings from evaluations and audits.

The principle of responsibility is applied through routine monitoring and evaluation of the implementation of prevailing rules. When deviations are found, the unit concerned must immediately take corrective action. This shows that governance is not sufficient if it only issues rules; it must be followed by continuous supervision and guidance. Independence appears in monitoring that is based on rules rather than on the interests of a particular unit, while fairness is applied when the IT needs of each unit are assessed: every request is weighed by business priority, risk level, system readiness, and budget availability. These findings are consistent with Bank Kalbar's documents, which state the five governance principles of transparency, accountability, responsibility, independence, and fairness. In practice, these principles are embedded in the supervision and management of Bank activities, which always take risk factors into account.

Risk in IT management

The risk aspect appears in the processes of identifying, assessing, prioritizing, controlling, and monitoring IT risks. According to the interviews, risks are identified from IT processes and activities, including possible system disruptions, information security, access, system changes, applications, infrastructure, and work involving third parties. Informant 1 explained that risks are not treated equally: priority is determined by the risk level and its impact on the Bank, so risks with greater impact or the potential to disrupt operations and services are followed up first. Informant 2 gave a similar explanation, stressing that risks with potentially large impacts on services become the priority.

The main constraint in IT projects involving external parties concerns timeliness. The informants explained that vendors often complete their work late, which affects the completion schedule of the Bank's IT projects and calls for more intensive supervision and communication. The interviews also show that IT risk is not limited to technical disruption but is also related to the process of developing and changing systems. Risk management therefore needs to be carried out continuously because technology and business needs keep developing. The documentation supports these findings: the Governance Report explains that risk management is carried out through the identification, measurement, monitoring, control, and reporting of risks, and it shows a function and oversight related to IT Risk Management as well as the strengthening of the Cyber Resilience and Security function.

Compliance in IT management

Compliance in the implementation of IT GRC is carried out through adherence to regulator requirements, internal policies, SOPs, monitoring, and audits. Informant 1 explained that regulator provisions, especially those of OJK, are studied and their impact on existing policies, procedures, and systems is then assessed. Where adjustments are needed, internal follow-up is carried out. To ensure compliance in work units, IT GRC uses guidelines and SOPs as references, and implementation can be monitored and examined through audits. If inconsistencies are found, the unit concerned is directed to make improvements and follow-up. Informant 2 explained that this process requires coordination because not every inconsistency can be resolved directly.

Compliance is also applied to systems and applications. Informant 1 explained that certain applications or systems can become objects of testing, supervision, and IT audit, so compliance is judged not only from documents but also from the controls applied to systems. The documentation shows discussion and audit of several IT systems, including the Cash Management System (CMS), Mobile Banking, and Xcard Web, as well as discussion of the ISO 27001:2022 Information Security Management System. This reinforces the interview finding that compliance and system control are part of IT supervision.

Information security and system reliability

Information security is an important part of IT GRC implementation because IT supports a wide range of banking activities. Informant 1 explained that security is maintained through user access control, system change management, backup and recovery, network and infrastructure security, and security monitoring. Informant 2 described several layers of control, one of which is the use of layered passwords on customer accounts. To maintain service availability during disruption, Bank Kalbar has a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) together with a backup system. According to Informant 1, when a disruption occurs the first priority is to restore the system, followed by checking the cause and evaluating the event. The handling includes running quick recovery procedures, activating the backup system or Disaster Recovery Center, and moving operations to a backup server or facility so that services can be used again promptly.

The documentation strengthens these interview results. IT controls cover user access review, system change management, backup and recovery, network and infrastructure security, and security monitoring. These controls are adequate to support system reliability, although security supervision still needs to be improved.

Monitoring, audit, and follow-up

Monitoring and audit are important mechanisms in the implementation of IT GRC. The interviews show that monitoring is carried out to see whether implementation conforms to policies and procedures. When findings arise, they are followed up and their resolution is monitored. Informant 1 explained that after a disruption or incident, an evaluation is carried out to find the cause, the way it was handled, the adequacy of controls, and the improvements needed. Informant 2 added that audit results or findings are also monitored until a follow-up is made.

The documentation shows that follow-up on OJK examination results is carried out within the committed deadlines and that the results of follow-up are reported periodically at board meetings. The Bank also monitors the resolution of examination findings. In addition, the 2025 IT audit report records findings on the Disaster Recovery Plan and the Core Banking System that still have residual findings. The Core Banking System is the main system that directly processes all of the Bank's financial transactions, while the Disaster Recovery Plan is the technical plan for saving and restoring that system in the event of a disaster or disruption. Although the disaster handling plan is already running, the audit team still found some technical gaps that have not been fully closed by the IT team. This shows that monitoring and follow-up are continuing processes.

Utilization of IT in Supporting IT GRC

The second research focus shows that IT is not only an object supervised by IT GRC but also a means that helps carry out governance, risk management, and compliance. This utilization appears in the use of banking systems and applications, access control, backup and recovery, security monitoring, IT audit, and IT development planning. Table 3 summarizes how IT supports each aspect of IT GRC.

Table 3. Utilization of IT in supporting IT GRC at Bank Kalbar

Aspect	Forms of IT utilization and control	Evidence
Governance	Systems and applications developed in line with the Bank's strategic direction (API QRIS Host to Host, EDC Mini ATM, Virtual Account, BI-Fast, CMS, e-Form, mobile banking); IT development prioritized by benefit, risk, readiness, and budget.	IT Masterplan and IT Strategic Plan 2023–2025; interviews with Informants 1 and 2.

Aspect	Forms of IT utilization and control	Evidence
Risk management	Access control, backup and recovery, DRP, security monitoring, and system evaluation; post-incident evaluation to determine cause and corrective action.	Digital Resilience Center (DRC) and drill in March 2025; digital maturity assessment 2024 at level 2.
Compliance	Application of IT General Controls (ITGC) and application controls; Test of Design Effectiveness (TDE) and Test of Operating Effectiveness (TOE); systems and applications as objects of testing and audit.	2025 Annual Report; interviews with Informants 1 and 2.
Information security	User access control, change management, backup and recovery, network security, and security monitoring; strengthening of the cyber resilience and security function.	Governance Report (Cyber Resilience and Security Function, ISO 27001:2022 audit).

Source: Interview and documentation results, 2026

IT in supporting governance

The utilization of IT supports governance through the management of systems and applications that follow the Bank's strategic direction. Bank Kalbar has developed various IT-based services, including API QRIS Host to Host, EDC Mini ATM, Virtual Account, BI-Fast, CMS, e-Form, and mobile banking. This development shows that IT is used to support the Bank's business and service needs. According to Informant 1, the Bank continues to expand the digitalization of its services to support operational efficiency and convenience in transactions. The CMS makes it easier for treasurers of government agencies and schools to manage mass salary payments, while Virtual Account and e-Form speed up bill verification and online service registration. For remote areas, the Bank uses EDC Mini ATM in local agent networks to facilitate cash withdrawals, and daily transactions are accommodated through Mobile Banking that is integrated with BI-Fast for low-cost interbank transfers, with API QRIS Host to Host for payments at merchants, and with the digital purchase of routine needs.

However, the interviews show that IT development cannot proceed without priorities. The needs of each unit differ, while IT development requires a considerable budget. Development needs must therefore be arranged by priority, benefit, risk, readiness, and budget capacity. Informant 2 stated that not all development requests can be realized immediately. This shows that IT utilization in governance is not merely about adding applications or systems but about how IT development is directed, prioritized, and controlled to fit the Bank's needs.

IT in supporting risk management

IT supports risk management through access control, backup and recovery, the DRP, security monitoring, and system evaluation. These controls help the Bank reduce the risk of unauthorized access, system disruption, and data loss. The interviews show that risks are also monitored after a disruption or finding occurs, and that evaluation is carried out to determine the cause and decide on corrective action. IT utilization in risk management is thus not only preventive but also supports recovery and evaluation.

The 2025 Annual Report of Bank Kalbar shows that the Bank has a Digital Resilience Center (DRC) and carried out a drill in March 2025. The DRC is a facility that supports the continuity of IT systems and services if the main system is disrupted, while a drill is an exercise or simulation to test the Bank's readiness to face disruption and to ensure that recovery procedures can be carried out. The digital maturity assessment for 2024, which used the OJK Digital Maturity Assessment Worksheet, placed the Bank at level 2, which indicates that control and governance activities have generally been implemented but some aspects still need to be strengthened. One of them is the capacity of IT facilities and devices to support all IT activities and services, especially network infrastructure. This condition serves as a basis for the Bank to strengthen its infrastructure gradually according to needs and development priorities.

IT in supporting compliance

The utilization of IT in supporting compliance is evident in the controls applied to applications and systems and in the conduct of IT testing and audit. The 2025 Annual Report explains that IT General Controls (ITGC) are general controls applied to ensure that IT is managed and used securely, in an orderly manner, and reliably, while application controls are applied within applications to ensure that the processes and data handled by the system run according to the established provisions. In practice, Bank Kalbar conducts a Test of Design Effectiveness (TDE), which assesses whether control design is appropriate to address existing risks, and a Test of Operating Effectiveness (TOE), which ensures that the controls actually operate effectively. IT control is thus judged not only by the existence of systems and applications but also by the suitability of their design and their implementation in supporting compliance and the reliability of IT processes. Both informants also explained that certain applications and systems are objects of testing and audit, which shows that compliance is applied not only through administrative conformity but also through controls built into the systems.

IT in supporting information security

IT management at Bank Kalbar also covers information security. The controls implemented include access control, which regulates user rights to access systems and information; change management, which controls changes to systems or applications; backup and recovery, which covers data backup and the restoration of data or systems in the event of disruption; and network security and security monitoring, which observe the security condition of systems to detect disruptions or activities that require attention. These controls relate to efforts to keep information protected, free from improper changes, and available when needed.

The interviews show that IT security requires attention because technological development is accompanied by the development of various threats to systems and information. The informants explained that security monitoring and system strengthening are carried out to face these risks, and that the functions related to cybersecurity and resilience continue to be strengthened according to the Bank's IT management needs. This is supported by the Governance Report, which contains discussion and recommendations on Cyber Resilience and the Security Function (FKKS). Cyber resilience concerns the Bank's ability to prepare for, face, and recover its IT systems from disruptions or cyber threats, while the security function concerns the management and supervision of information and IT security. The report also records discussion of the ISO 27001:2022 audit, the international standard used as a reference for information security management.

Constraints in utilizing IT to support IT GRC

Although IT has been used to support governance, risk management, and compliance, the interviews show that implementation still faces several constraints. The first is the limited IT development budget, so needs from various work units must be adjusted to the available budget and priorities. The second is that some of the Bank's work uses third parties, so the completion of work can be affected by the time those parties need. The third is that the audit process takes time because it involves several stages, from examination and the submission of findings to coordination and the completion of follow-up. The interviews also show that system changes and developing technology needs require documentation and IT controls to be adjusted periodically. This is in line with the 2025 Annual Report, which notes that the refinement of technical documentation and a higher intensity of security monitoring remain areas to be strengthened. Table 4 summarizes these constraints and the strengthening efforts observed in the data.

Table 4. Constraints and strengthening efforts in IT GRC implementation

Constraint	Description	Strengthening effort observed
Limited IT development budget and numerous unit needs	Development requests differ across units and cannot all be realized immediately.	Requests are prioritized by urgency, benefit, risk, readiness, and budget capacity.
Third-party delays	Vendors sometimes complete work late, which affects the schedule of IT projects.	More intensive supervision and communication; coordination with work units and third parties.
Time required for audit and follow-up	Audit involves examination, submission of findings, coordination, and completion of follow-up.	Findings are monitored until followed up; results are reported periodically at board meetings.

Constraint	Description	Strengthening effort observed
Documentation and control adjustment	System changes and new technology needs require documentation and controls to be updated periodically.	Refinement of technical documentation, higher intensity of security monitoring, gradual infrastructure strengthening, continuous review of policies and SOPs, and efforts to build risk and compliance culture.

Source: Interview and documentation results, 2026

Discussion

Implementation of GRC in supporting IT governance

The results show that governance, risk, and compliance are interrelated in the management of IT at Bank Kalbar. Governance relates to policies, procedures, the division of roles, and the direction of IT management. Risk relates to the process of recognizing and managing risks that may arise from the use and development of IT. Compliance relates to fulfilling regulator provisions and the policies in force within the Bank. The relationship among the three can be seen in how IT management is carried out: policies and SOPs are used as guidelines for IT activities, monitoring and audit examine implementation and conformity, and the results of examinations become material for follow-up when something needs to be improved. IT risk is also one of the considerations when the Bank determines needs, development priorities, and the handling of system disruptions.

This indicates that GRC is applied not only at the examination stage but is also a consideration in the process of managing IT. When there is a need for IT development or change, the Bank must consider the risks that may arise, the provisions that must be met, the needs of work units, and the availability of budget. The pattern is consistent with the integrated view of GRC set out by Racz et al. (2010), in which governance, risk management, and compliance are interconnected functions, and with Nurdin (2018), who links stronger IT governance in a bank to the timely and accurate information that supports core operations and regulatory compliance. It also differs in an instructive way from the case reported by Muziardy and Yuniarti (2025), where risk management at a rural bank was manual and reactive and compliance responsibilities were consolidated with little cultural support. At Bank Kalbar, risks are prioritized by impact, controls are tested through TDE and TOE, and audit findings are tracked until follow-up, although post-incident evaluation remains part of the cycle. This difference may reflect differences in institutional scale and regulatory expectations, and, given that this is a single-case study with two informants, it should not be generalized to other banks. The role of audit and follow-up in Bank Kalbar's practice also resonates with Fitriani et al. (2024), who position integrated GRC as strengthening the contribution of internal audit to accountability and risk mitigation, although the residual findings on the DRP and Core Banking System show that closing audit findings takes time.

IT utilization strengthens the implementation of IT GRC

The utilization of IT at Bank Kalbar is closely related to the implementation of IT GRC. The systems and applications used in the Bank's activities not only support work but also need to be controlled so that they are secure and in line with regulations. According to the results, these controls include user access arrangements, change management, backup and recovery, security monitoring, application testing, and IT audit. From the governance side, technology supports the implementation of the Bank's digital plans and strategy. From the risk side, technology helps provide mechanisms for control and recovery. From the compliance side, technology becomes the object of testing and audit to ensure that controls run according to provisions. IT utilization and IT GRC therefore stand in a reciprocal relationship and cannot be separated. This is consistent with Tursina (2025), who found a positive correlation between IT investment and GRC improvements in a listed company, and with Abdurrahman et al. (2024), whose findings suggest that governance, risk management, and compliance factors enhance the outcomes of digital transformation in banks.

The results also show that IT development takes into account the needs of work units, risks, provisions that must be met, and budget capacity. The limited budget and the use of third parties in some work are considerations in implementing IT development. The dependence on third parties is in line with Wibowo et al. (2025), who identify third-party or vendor dependency as one of the risks in digital banking projects. IT utilization at Bank Kalbar thus runs together with the management of governance, risk, and compliance, so that technology is not only used to support the Bank's activities but also needs to be managed and controlled well.

Challenges and strengthening efforts

The results show that the implementation of IT GRC still faces internal and external challenges. Internal challenges include the limited development budget, the large number of IT needs, differences in needs among units, and the need to update documentation and controls. The external challenge is the delay of third parties in some work. In addition, the audit process takes time because the examination results must be followed up. This condition does not indicate that controls are not working; it shows that IT GRC is a continuous process that requires monitoring and improvement.

The strengthening efforts seen in the results include increased monitoring, follow-up of audit results, strengthening of technical documentation, increased security monitoring, infrastructure strengthening, and coordination with work units and third parties. The Bank's documentation also shows continuous review of the Bank Policy Guidelines (BPP) and SOPs and efforts to increase risk culture and compliance culture, which fits with Wulandari (2022), who notes that organizational structure and culture influence the acceptance and adaptation of IT. For the Bank, these findings imply that the prioritization of IT needs, the monitoring of third-party work, and the tracking of audit follow-up are the areas in which IT GRC implementation can be strengthened most directly.

CONCLUSION AND RECOMMENDATIONS

Conclusion

This study shows that the implementation of GRC in supporting IT governance at Bank Kalbar is carried out through three main elements: governance, risk, and compliance. Governance is realized through policies, procedures, the division of responsibilities, monitoring, and supervision. Risk is managed through the identification, assessment, prioritization, control, and monitoring of IT risks. Compliance is carried out through adherence to regulator provisions, internal policies, SOPs, audits, and documentation.

The utilization of IT in supporting IT GRC is carried out through the use of systems and applications that are accompanied by controls. In the governance aspect, IT is used to support IT plans and development. In the risk aspect, access control, change management, backup and recovery, and security monitoring are applied. In the compliance aspect, systems and applications are tested through IT General Controls (ITGC) and application controls using the Test of Design Effectiveness (TDE) and the Test of Operating Effectiveness (TOE). Bank Kalbar also has a Digital Resilience Center (DRC) and carries out drills as part of its readiness to face system disruption.

The implementation of IT GRC at Bank Kalbar still faces several constraints, namely the limited IT development budget, the large number of needs from work units, the delay of third parties in completing certain work, and the time required for the audit and follow-up process. These conditions become considerations in determining IT development priorities and in carrying out work related to IT GRC.

Research Limitations

This study has several limitations. First, not all internal data related to IT management could be obtained because part of the information is internal to the Bank; the study used the data and documents that Bank Kalbar could provide and the results of interviews with the informants. Second, the informants were limited to parties related to IT GRC, so the information obtained came mostly from those directly involved in managing IT GRC. To complement the interviews, the study also used supporting documents such as the Annual Report and Governance Report of Bank Kalbar. As a single-case qualitative study, the findings describe conditions at Bank Kalbar and should be generalized to other banks with caution.

Recommendations

Bank Kalbar is encouraged to set priorities for IT development needs based on their urgency and importance so that the limited budget can be used to meet the highest-priority needs. The Bank is also encouraged to set deadlines and assign a person in charge for every third-party job, and to monitor the completion of such work and the follow-up of audit results periodically so that delays can be addressed promptly. Future research could widen the range of informants, for example to internal audit, risk management, and business units, compare several regional development banks, and complement interviews with measures of IT GRC maturity.

ACKNOWLEDGMENTS

The authors thank Politeknik Negeri Pontianak for the support and funding provided for this research through its applied research funding program. The authors also thank Bank Kalbar, especially the parties who provided the opportunity, information, and data needed during the research, and the informants who took the time to explain the implementation of Governance, Risk, and Compliance (GRC) in IT management. The authors are also grateful to Subaidah, Gressnauli P, and Hany Septiya Putri, who assisted with administration, data collection, and data entry. It is hoped that the results of this research will be useful for Politeknik Negeri Pontianak, Bank Kalbar, and other interested parties as information and reference on the implementation of IT GRC and IT management in the banking sector.

REFERENCES

- Abdurrahman, A., Gustomo, A., & Prasetyo, E. A. (2024). Enhancing banking performance through dynamic digital transformation capabilities and governance, risk management, and compliance: Insights from the Indonesian context. *The Electronic Journal of Information Systems in Developing Countries*, 90(2), e12299. <https://doi.org/10.1002/isd2.12299>
- ANTARA News Kalimantan Barat. (2025, January 21). *Bank Kalbar catat transaksi QRIS 2024 sebesar Rp211,96 miliar*. <https://kalbar.antaranews.com/berita/619302/bank-kalbar-catat-transaksi-qr-2024-sebesar-rp21196-miliar>
- Bahri, S. (2018). *Metodologi penelitian bisnis: Lengkap dengan teknik pengolahan data SPSS*. ANDI.
- Bank Kalbar. (n.d.). *Laporan tahunan dan keberlanjutan* [Annual and sustainability reports]. PT Bank Pembangunan Daerah Kalimantan Barat. https://bankkalbar.co.id/laporan_tahunan.php
- Fitriani, F., Sandy, K. N., Amiruddin, A., & Syamsuddin, S. (2024). Governance, risk, and compliance: Pilar utama untuk audit berbasis nilai tambah. *Jurnal Akuntansi dan Keuangan Kontemporer*, 7(2), 374–385. <https://doi.org/10.30596/jakk.v7i2.24756>
- International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection: Information security management systems: Requirements*. <https://www.iso.org/standard/27001>
- ISACA. (2018). *COBIT 2019 framework: Governance and management objectives*. ISACA.
- Muziardy, E., & Yuniarti, R. (2025). Analysis of governance, risk, and compliance (GRC) implementation in rural bank management: A case study at PT BPR Panjawan Mitra Usaha. *Journal of Economics and Business UBS*, 14(4), 901–906. <https://doi.org/10.52644/joeb.v14i4.2781>
- Nurdin, A. (2018). Pemetaan tata kelola TI dan analisa faktor penghambatnya: Studi kasus PT Bank DNM, Tbk. *JIKA (Jurnal Informatika)*, 2(1). <https://doi.org/10.31000/jika.v2i1.1410>

- Otoritas Jasa Keuangan. (2017). *Peraturan Otoritas Jasa Keuangan Nomor 46/POJK.03/2017 tentang pelaksanaan fungsi kepatuhan bank umum*.
<https://ojk.go.id/id/regulasi/Pages/Pelaksanaan-Fungsi-Kepatuhan-Bank-Umum.aspx>
- Otoritas Jasa Keuangan. (2022). *Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang penyelenggaraan teknologi informasi oleh bank umum*.
<https://ojk.go.id/id/regulasi/Pages/Penyelenggaraan-Teknologi-Informasi-Oleh-Bank-Umum.aspx>
- Otoritas Jasa Keuangan. (2023). *Peraturan Otoritas Jasa Keuangan Nomor 17 Tahun 2023 tentang penerapan tata kelola bagi bank umum*.
<https://ojk.go.id/id/regulasi/Pages/Penerapan-Tata-Kelola-Bagi-Bank-Umum.aspx>
- Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.CSWP.29>
- Racz, N., Weippl, E., & Seufert, A. (2010). A frame of reference for research of integrated governance, risk and compliance (GRC). In B. De Decker & I. Schaumüller-Bichl (Eds.), *Communications and multimedia security* (Lecture Notes in Computer Science, Vol. 6109, pp. 106–117). Springer. https://doi.org/10.1007/978-3-642-13241-4_11
- Suara Ketapang. (2024, December 14). *ATM Bank Kalbar di Ketapang sering gangguan, nasabah keluhkan pelayanan*. <https://ketapang.suarakalbar.co.id/2024/12/atm-bank-kalbar-di-ketapang-sering.html>
- Sugiyono. (2023). *Metode penelitian kuantitatif, kualitatif, dan R&D* (2nd ed.). Alfabeta.
- Tursina, N. (2025). Pengaruh teknologi informasi terhadap tata kelola, risiko dan kepatuhan (GRC) yang dimoderasi kinerja keuangan. *COSTING: Journal of Economic, Business and Accounting*, 8(2), 901–918. <https://doi.org/10.31539/costing.v8i2.14325>
- Wibowo, A. P., Raharjo, T., Trisnawaty, N. W., Muhamad, G. A., & Faridy, A. (2025). Risk management in IT projects for digital banking: A case study of an Indonesian state-owned bank. *Applied Information System and Management*, 8(2), 231–244.
<https://doi.org/10.15408/aism.v8i2.46123>
- Wulandari, N. (2022). Sistem informasi, organisasi, dan strategi: Studi literatur permasalahan manajemen pada teknologi informasi. *JIKSI: Jurnal Ilmu Komputer dan Sistem Informasi*, 3(1), 1–6. <https://doi.org/10.61346/jiksi.v3i1.127>