

EXAMINING TECHNOLOGY RISKS FROM COSO PERSPECTIVE: A CASE STUDY ON AUDIT AND ASSURANCE IN AN ISLAMIC FINANCIAL INSTITUTION IN MALAYSIA

Mohd Faizullah Bin Yusof^{1,a}, Muhammad Hafizuddin Bin Haris^{2,b}, Mohamad Khairol Aqil
Bin Ahmad^{3,c} and Zurina Binti Shafii^{4,d}

¹Faculty of Economics and Muamalat. Universiti Sains Islam Malaysia, Nilai, Negeri Sembilan, Malaysia

²Faculty of Economics and Muamalat. Universiti Sains Islam Malaysia, Nilai, Negeri Sembilan, Malaysia

³Faculty of Economics and Muamalat. Universiti Sains Islam Malaysia, Nilai, Negeri Sembilan, Malaysia

⁴Faculty of Economics and Muamalat. Universiti Sains Islam Malaysia, Nilai, Negeri Sembilan, Malaysia

^a3252096@raudah.usim.edu.my

^b3252033@raudah.usim.edu.my

^c3252036@raudah.usim.edu.my

^dzurina.shafii@usim.edu.my

*Corresponding Author: 3252096@raudah.usim.edu.my

Abstract: The purpose of this study is to examine technology risks from the perspective of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control–Integrated Framework within an Islamic Financial Institution (IFI) in Malaysia. Specifically, the study evaluates how governance structures, Enterprise Risk Management (ERM), Shariah Governance, the Institute of Internal Auditors (IIA) Three Lines Model, and the Global Internal Audit Standards (GIAS 2024) support technology risk management, internal control effectiveness, audit assurance, and regulatory compliance. ABC Islamic Bank (ABC-IB) was selected as the case study because of its well-established governance framework and significant digital banking operations. A qualitative case study approach was adopted using annual reports, corporate governance reports, audit committee reports, enterprise risk management disclosures, regulatory announcements, and enforcement actions issued between May 2024 and 2025. The study analyses technology-related incidents involving regulatory reporting, Central Credit Reference Information System (CCRIS) data integrity, digital banking service disruptions, operational resilience, and potential Shariah Non-Compliance (SNC) exposure by mapping these issues against the five components of the COSO Internal Control Framework. This happened because monitoring controls did not detect reporting errors before they reached the regulator indicate that the bank has established a comprehensive governance structure supported by the Board of Directors, Audit Committee, Risk Management Committee, Shariah Committee, Enterprise Risk Management, Internal Audit, and dedicated Technology and Cyber Risk Management Frameworks. Nevertheless, regulatory enforcement actions reveal weaknesses in Information and Communication, Control Activities, Monitoring Activities, and Risk Assessment, particularly in relation to data governance, technology resilience, automated controls, and regulatory reporting accuracy. These findings suggest that strong governance structures alone are insufficient without continuous enhancement of technology controls, cyber resilience, and audit assurance to address emerging digital risks. This study contributes to the existing literature by integrating the COSO Internal Control Framework, ERM, the Three Lines Model, Shariah Governance, and GIAS into a proposed Technology Risk Governance Assurance Model (TRGAM) for Islamic Financial

Institutions. The proposed model provides practical guidance for strengthening technology governance, improving operational resilience, enhancing regulatory and Shariah compliance, and supporting sustainable governance in the digital banking environment.

Keywords: Technology Risk; Islamic Financial Institutions; COSO Internal Control Framework, Enterprise Risk Management; Shariah Governance, Internal Audit, Operational Resilience - TRGAM

1. Introduction

This study examines how a leading IFI in Malaysia integrates governance, Shariah oversight, technology risk management, regulatory compliance, ERM, and Internal Audit (IA) practices through the implementation of the Three Lines Model (TLM) within an increasingly digital banking environment at ABC-IB. The study evaluates technology and cyber risks from the perspective of the COSO Internal Control Integrated Framework, focusing on governance effectiveness, operational resilience, internal controls, and regulatory compliance, particularly in relation to data governance, technology, and cybersecurity.

Islamic Financial Institutions (IFIs) operate within a more complex governance environment compared to conventional financial institutions because they must comply with both financial regulations and Shariah principles. Besides complying with requirements issued by Bank Negara Malaysia (BNM), Securities Commission Malaysia (SC), and the Islamic Financial Services Act 2013 (IFSA 2013), Islamic banks must ensure that all operational activities, products, governance processes, and technology systems continuously comply with Shariah requirements. This dual-governance obligation increases the importance of effective internal controls, technology resilience, compliance monitoring, and Shariah governance oversight.

This study adopts a qualitative case study methodology using annual reports, governance disclosures, audit committee reports, risk management reports, and BNM regulatory announcements relating to the bank between May 2024 and 2025. The study applies the COSO Internal Control Integrated Framework and the TLM as the primary analytical frameworks to evaluate governance accountability, technology risk management practices, Shariah governance structures, and audit assurance effectiveness. The analysis also incorporates selected regulatory enforcement cases involving inaccurate regulatory reporting, CCRIS data integrity weaknesses, prolonged system downtime, operational resilience failures, and potential indirect SNC exposure.

The findings indicate that ABC-IB has established a structured governance and assurance framework supported by the Board of Directors, Audit Committee, Risk Management Committee, Shariah Committee, compliance functions, ERM frameworks, cyber risk governance frameworks, and internal audit activities. The institution also demonstrates governance enhancement initiatives through the implementation of Technology Risk Management Frameworks (TRMF), Cyber Risk Management Frameworks (CRMF), cloud governance controls, system integration, and continuous monitoring practices.

However, the study identifies several weaknesses relating to technology resilience, data governance, regulatory reporting accuracy, operational monitoring, compliance execution, and incident recovery capability. Regulatory enforcement actions issued by BNM between 2024 and 2025 revealed repeated weaknesses involving inaccurate regulatory submissions, prolonged digital banking system disruptions, weak incident response capability, ineffective data validation controls, and reporting inaccuracies. These weaknesses affected several

COSO components, particularly Information and Communication, Control Activities, Monitoring Activities, Risk Assessment, and indirectly the Control Environment.

The study finds that although ABC-IB maintains a generally structured governance ecosystem, recurring technology-related disruptions and regulatory breaches indicate that certain internal controls were not sufficiently effective in preventing, detecting or timely correcting operational weaknesses. Increasing dependence on digital banking platforms, third-party technology providers, automation tools, cloud infrastructure, and artificial intelligence further increases operational complexity and cyber risk exposure within IFIs. From a Shariah governance perspective, technology weaknesses and inaccurate regulatory reporting may indirectly contribute to SNC exposure by affecting customer trust, operational reliability, and governance accountability.

Overall, the COSO-based GRC assessment concludes that the bank demonstrates a reasonably mature governance and risk management structure. However, major improvements remain necessary in technology resilience, automated monitoring controls, data governance, incident recovery capability, regulatory reporting integrity, and operational compliance management. The study recommends stronger automation controls, enhanced cyber resilience frameworks, integrated data governance practices, continuous Shariah monitoring, and improved governance over emerging technologies to strengthen long-term operational resilience, regulatory compliance, and stakeholder confidence.

2. Literature Review

Digital Transformation in Islamic Financial Institutions

The banking industry has changed rapidly over the last decade as digital technologies have become part of everyday banking operations. Today, Islamic Financial Institutions (IFIs) rely on mobile banking, cloud computing, artificial intelligence (AI), big data analytics and digital payment platforms to deliver faster and more convenient services. These technologies help banks improve efficiency, reduce operating costs and provide better customer experience.

Despite these advantages, digital transformation also creates new challenges. Banks now face greater exposure to cyberattacks, system failures, data breaches and technology disruptions. For Islamic banks, the challenge is even greater because every digital process must comply with both regulatory requirements and Shariah principles. As more banking services move online, technology risk has become an important governance issue that requires continuous oversight from the Board, management and Internal Audit.

Technology Risk in Islamic Financial Institutions

Technology risk is no longer viewed as an IT issue alone. It has become a business risk that can affect an organization's operations, financial performance, reputation and regulatory compliance. Weak system controls, poor data quality, cyber incidents and prolonged service disruptions may interrupt business operations and reduce public confidence in the banking system. For Islamic Financial Institutions, the impact can be even more significant. Technology failures may affect the accuracy of financial transactions, customer information and regulatory reporting. In some situations, these weaknesses may indirectly expose the bank to SNC because inaccurate information can affect fairness, transparency and accountability.

Our previous study on ABC-IB identified Technology and Cyber Risk as one of the bank's principal risks that require continuous monitoring by management, the Risk

Management Committee and Internal Audit. The study also highlighted that technology governance must evolve continuously as digital banking becomes more complex.

COSO Internal Control–Integrated Framework

Many organisations use the COSO Internal Control–Integrated Framework to strengthen governance, improve internal controls and manage risks more effectively. Rather than focusing only on financial reporting, COSO provides a comprehensive framework for managing operational, compliance and technology risks.

The framework is built around five components: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities. These components work together to help organisations identify risks, design effective controls and continuously monitor whether those controls remain effective.

This study applies the COSO Framework to assess how ABC-IB manages technology risks within its governance structure. The framework also provides a practical basis for evaluating whether technology controls remain effective as the bank continues to expand its digital banking services.

Enterprise Risk Management

Technology risk cannot be managed in isolation. It must be integrated into the organization's overall risk management framework because technology failures often affect several areas of the business simultaneously.

ERM provides this broader perspective by integrating strategic, operational, financial, compliance and technology risks into one governance framework. Through ERM, management can identify emerging risks, determine acceptable risk levels and develop appropriate responses before risks become significant issues.

According to our previous ABC-IB study, the bank applies an Enterprise Risk Management Framework (ERMF) supported by a Risk Appetite Statement (RAS), risk governance policies, and continuous monitoring. These practices help ensure that technology risks remain within the level of risk approved by the Board.

Three Lines Model and Internal Audit

Strong governance depends on clear roles and responsibilities. The IIA introduced the Three Lines Model to clarify how organizations manage risk and maintain effective internal controls.

Under this model, management forms the first line by identifying and managing operational risks. The second line consists of risk management, compliance and Shariah functions that oversee risk management activities and ensure compliance with internal policies and regulatory requirements. Internal Audit forms the third line by providing independent assurance to the Board and Audit Committee on the effectiveness of governance, risk management and internal controls.

Our previous study shows that these three lines work together to strengthen governance and improve accountability. As technology risks continue to increase, effective collaboration between the three lines becomes even more important in maintaining operational resilience and regulatory compliance.

Shariah Governance and Technology Risk

Shariah Governance is one of the main features that distinguishes Islamic banks from conventional financial institutions. Besides meeting regulatory expectations, Islamic banks must ensure that every product, transaction and operational process complies with Shariah principles.

Technology plays important role in supporting these activities. However, weaknesses in system controls, inaccurate customer information or poor regulatory reporting may indirectly increase the risk of Shariah Non-Compliance. Although technology failures may not directly involve prohibited transactions, they can reduce transparency, affect customer rights and weaken public confidence in the institution.

The governance structure adopted by ABC-IB demonstrates how the Board of Directors, Shariah Committee, Audit Committee and Risk Management Committee work together to oversee both regulatory and Shariah compliance.

Global Internal Audit Standards - 2024

The GIAS 2024 expand the role of Internal Audit beyond traditional financial auditing. Internal auditors are now expected to provide assurance over emerging risks such as cybersecurity, artificial intelligence, cloud computing, data governance and digital transformation.

This shift reflects the increasing reliance on technology across the financial sector. Internal Audit is expected not only to identify control weaknesses but also to provide valuable insights that strengthen governance and improve organizational resilience.

In ABC-IB, the Audit Committee revised the Internal Audit Charter to align with GIAS 2024, demonstrating the bank's commitment to maintaining high standards of governance and audit quality.

Research Gap

Previous studies have discussed technology risk, Enterprise Risk Management, COSO, Shariah Governance and Internal Audit separately. While these studies provide valuable insights, very few have examined how these frameworks can work together to strengthen technology governance in Islamic Financial Institutions.

Building on our previous ABC-IB case study, this research takes a more integrated approach by combining a few governance framework such COSO, GIAS and TRGAM as a practical framework that helps Islamic Financial Institutions strengthen technology governance, improve operational resilience, enhance regulatory and Shariah compliance, and build greater stakeholder confidence in an increasingly digital banking environment.

3. Methodology

Research Design

This study adopts a qualitative case study approach to examine technology risks and governance practices in an Islamic Financial Institution. A qualitative approach was selected because it allows the researchers to explore governance practices, internal controls, technology risk management, and audit assurance in depth using real organizational evidence rather than numerical data. The study focuses on ABC-IB because it is one of Malaysia's largest Islamic banks with a well-established governance structure, mature risk management practices,

and extensive digital banking operations. This case study also builds on our previous research on ABC-IB's governance, Three Lines Model, and audit information systems, providing a strong foundation for further analysis of technology risks using the COSO Internal Control–Integrated Framework

Research Framework

ABC Islamic Bank was selected because it is the largest Islamic bank in Malaysia, has mature governance practices, extensive digital banking operations, and provides comprehensive public governance disclosures. These characteristics make it an appropriate case for examining technology risk governance.

This study uses the COSO Internal Control–Integrated Framework as the main framework for analysing technology risks. The five COSO components—Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities—provide the basis for evaluating the effectiveness of governance and internal controls. To provide a comprehensive assessment, the study also incorporates ERM, the IIA Three Lines Model, Shariah Governance, and the GIAS 2024. Together, these frameworks help explain how governance, risk management, compliance, and audit functions work together to manage technology risks in an Islamic Financial Institution.

Data Sources

The study relies entirely on secondary data obtained from publicly available and reliable sources. These include annual reports, corporate governance reports, audit committee reports, sustainability reports, ERM disclosures, BNM's policy documents, enforcement actions, regulatory announcements, and other official publications issued between May 2024 and May 2025. Academic journal articles, professional standards, and industry publications were also reviewed to support the literature review and strengthen the analysis. Using multiple sources allows the researchers to compare information and gain a balanced understanding of the issues being studied.

Study Limitations

This study focuses on one Islamic Financial Institution and relies on publicly available documents. Future studies could include multiple Islamic banks, interviews with practitioners, or cross-country comparisons.

Sampling and Data Collection

Purposive sampling was used to select ABC-IB as the case study because the bank has comprehensive governance disclosures, a mature technology risk management framework, and publicly available regulatory information. The study also selected regulatory cases that relate directly to technology and cyber risks, including inaccurate regulatory reporting, weaknesses in CCRIS data quality, digital banking service disruptions, operational resilience, and potential SNC.

Sources based submission of statistical data to BNM using STATsmart Reporting, External Sector Statistics (ESS) and CCRIS requirements. These cases provide practical examples for evaluating the effectiveness of governance and internal controls, as follows:

Sample	Date	Issue	Penalty
1	11 Jul 2024	Regulatory breaches / inaccurate and incomplete data submission	RM4.32 million
2	29 Jul 2024	Non-compliance with IFSA & operational reporting weaknesses	RM4.32 million (same event linkage with sample 1)
3	14 Aug 2024	Prolonged system disruption / downtime	RM4.32 million
4	03 Mar 2025	CCRIS inaccurate customer credit information	RM1.2 million

Figure 1. Table showing cases of NCR with penalty from Bank Negara Malaysia

Data Analysis

The collected information was analysed using document analysis and thematic analysis. First, the researcher reviewed governance reports, risk management disclosures, audit reports, and regulatory findings to identify technology-related issues. Next, the identified issues were grouped into common themes such as data governance, cybersecurity, operational resilience, regulatory compliance, and Shariah governance.

Finally, each issue was mapped against the five components of the COSO Internal Control–Integrated Framework to determine whether existing governance practices effectively addressed the identified technology risks. This approach allows the researchers to identify strengths, weaknesses, and opportunities for improvement.

Sample	Finding / Issue	Key Weakness Observed	Control Environment (CE)	Risk Assessment (RA)	Control Activities (CA)	Information & Communication (IC)	Monitoring Activities (MA)
Sample 1	Inaccurate & incomplete regulatory/statistical data submission to BNM	Data governance & reporting quality weakness	Governance oversight over regulatory reporting not sufficiently effective	-	Weak validation controls before submission	Poor data integrity and reporting quality	Failure to detect inaccuracies before submission
	Late submission to BNM / ESS / CCRIS	Compliance management weakness	-	Compliance timeline risk not adequately assessed	-	Ineffective coordination between departments	Delayed detection of overdue submissions
Sample 2	Multiple unplanned system downtime exceeding RMIT threshold	IT resilience & operational weakness	-	IT resilience and continuity risks underestimated	Weak IT infrastructure & incident response controls	Poor incident escalation/reporting process	Weak real-time monitoring capability
	Failure to recover system effectively during disruption	BCM & DRP effectiveness issue	-	Recovery risk scenario planning inadequate	Weak disaster recovery & business continuity execution	-	Weak post-incident monitoring & lessons learned
Sample 3	Inaccurate customer credit information in CCRIS	Data validation & customer information weakness	-	-	Weak maker-checker validation process	Incorrect customer information submission	Failure to detect data errors timely
	Weak data integrity controls	Enterprise data governance gap	-	-	Weak reconciliations/system controls	Inconsistent reporting information	Weak exception monitoring
Sample 4	Potential Shariah Non-Compliance (SNC) exposure due to reporting weaknesses	Reputational & compliance exposure	Governance oversight over Shariah operational compliance impacted indirectly	SNC exposure not holistically assessed	Weak operational compliance controls	-	Weak compliance review process
	Weak data integrity controls	Enterprise data governance gap	-	-	Weak reconciliations/system controls	Inconsistent reporting information	Weak exception monitoring

Figure 2. COSO Analysis of Findings (5 COSO Components)

Trustworthiness of the Findings

To improve the credibility of the findings, the study used information from several independent sources instead of relying on a single document. Governance reports were compared with regulatory announcements, annual reports, and official publications to confirm the consistency of the findings. The study also applied recognized governance frameworks, including COSO, ERM, the Three Lines Model, Shariah Governance and GIAS 2024, to ensure that the analysis followed accepted professional practices. This process strengthens the reliability and trustworthiness of the conclusions.

Ethical Considerations

This study uses only publicly available information and does not involve interviews, surveys, or confidential organizational data. All information was obtained from official reports, published documents, and publicly accessible regulatory announcements. As a result, no personal information or confidential business information was collected. The researchers ensured that all sources were properly acknowledged and interpreted objectively to maintain academic integrity and minimize researcher bias.

Proposed Technology Risk Governance Assurance Model

The final stage of the study develops the TRGAM based on the findings from the case study. The proposed model integrates the COSO Internal Control–Integrated Framework, Enterprise Risk Management, the Three Lines Model, Shariah Governance and the 2024 into a single governance framework. The model aims to help Islamic Financial Institutions strengthen technology governance, improve operational resilience, enhance regulatory and Shariah compliance, and support effective audit assurance in an increasingly digital banking environment.

4. Results

Summary of Case Study Findings

This study reviewed four major regulatory cases involving technology and operational risks reported between May 2024 and May 2025. The cases included inaccurate regulatory reporting, prolonged digital banking service disruptions, weaknesses in CCRIS customer data, and non-compliance with reporting requirements under the Islamic Financial Services Act 2013 (IFSA 2013). These cases were selected because they represent real operational issues that may affect governance, internal controls, regulatory compliance, and customer confidence.

The findings show that although ABC Islamic Bank has established comprehensive governance policies and technology risk management frameworks, several technology-related weaknesses still occurred during the study period. Most of these issues were associated with inaccurate data reporting, weak monitoring controls, insufficient data validation, delayed incident response, and operational resilience. These weaknesses mainly affected four COSO components, namely Information and Communication, Control Activities, Monitoring Activities, and Risk Assessment.

Risk Management Practices

The study found that ABC Islamic Bank has implemented a structured Enterprise Risk Management Framework (ERMF), Risk Appetite Statement (RAS), Technology Risk

Management Framework TRMF, CRMF, and cloud governance framework to manage technology risks across the organisation. These frameworks are supported by clear governance responsibilities, Board oversight, continuous monitoring, and risk reporting.

Despite these strong practices, the regulatory cases indicate that some technology controls were not operating effectively. The inaccurate submission of regulatory reports, weaknesses in CCRIS data validation, and prolonged system disruptions suggest that certain operational controls failed to detect or prevent errors before they affected regulatory compliance. These findings indicate that technology governance should continue to evolve alongside digital banking services, particularly in data governance, automated controls, cyber resilience, and incident response capabilities.

Corporate Governance

The findings demonstrate that ABC Islamic Bank has a well-established corporate governance structure. The Board of Directors provides overall strategic direction and oversees the Audit Committee, Risk Management Committee, Shariah Committee, and Senior Management. These committees work together to ensure that business operations comply with regulatory requirements, corporate governance standards, and Shariah principles. The Audit Committee provides oversight over financial reporting, internal controls, and internal audit activities, while the Risk Management Committee oversees strategic, operational, credit, technology, and Shariah non-compliance risks. The governance structure reflects good governance practices and aligns with Bank Negara Malaysia's corporate governance expectations.

However, the regulatory enforcement cases indicate that having a comprehensive governance structure alone does not completely prevent operational failures. Governance must be supported by effective execution, continuous monitoring, stronger technology controls, and timely corrective actions.

Shariah Review

The study found that the Shariah Committee plays an important role in ensuring that the bank's products, contracts, business operations, and governance practices comply with Shariah principles. The committee reviews Islamic financial products, approves Shariah contracts, advises management, and provides continuous oversight of Shariah compliance.

Although none of the regulatory cases involved direct Shariah violations, the findings suggest that technology failures may indirectly increase the risk of SNC. Inaccurate customer information, weak data governance, delayed reporting, and prolonged system outages may affect fairness, transparency, accountability, and customer trust, which are important principles within Islamic finance. Therefore, technology governance should also be viewed as an important component of Shariah governance.

Overall Pattern of Governance, Risk and Control

Overall, the study found that ABC Islamic Bank demonstrates a reasonably mature Governance, Risk and Control (GRC) environment. Governance responsibilities are clearly assigned, Enterprise Risk Management is well established, Internal Audit provides

independent assurance, and the Three Lines Model supports accountability across the organisation.

However, the review of regulatory enforcement cases identified recurring weaknesses in several technology-related areas. These include inaccurate regulatory reporting, weak data governance, ineffective monitoring controls, operational resilience, and delayed recovery during system disruptions. Most of these issues relate to the COSO components of Information and Communication, Control Activities, Monitoring Activities, and Risk Assessment.

These findings indicate that while governance policies are generally effective, greater emphasis should be placed on strengthening technology governance through automation, real-time monitoring, data quality management, cyber resilience, and integrated governance practices. Such improvements will help reduce operational risk, improve regulatory compliance, and enhance stakeholder confidence.

Audit Opinion

Based on the overall findings, the researcher concludes that ABC Islamic Bank has established a sound governance structure supported by the Board of Directors, Audit Committee, Risk Management Committee, Shariah Committee, Enterprise Risk Management, Internal Audit, and dedicated technology governance frameworks. These governance arrangements provide a strong foundation for managing technology and operational risks.

Nevertheless, the regulatory cases demonstrate that several internal control weaknesses remain, particularly in data governance, regulatory reporting accuracy, technology resilience, monitoring activities, and automated control processes. Therefore, the overall audit opinion is "Generally Effective with Opportunities for Improvement."

The study recommends that ABC Islamic Bank continue strengthening its technology governance by improving automated monitoring, enhancing data quality controls, strengthening cyber resilience, expanding continuous auditing practices, integrating artificial intelligence for risk monitoring, and enhancing coordination between governance, risk management, Shariah oversight, compliance, and Internal Audit. These improvements will support the proposed TRGAM and enhance long-term operational resilience and regulatory compliance.

COSO Assessment Summary

COSO Component	Assessment	Key Finding
Control Environment	Strong	Well-defined governance structure and Board oversight
Risk Assessment	Moderate	Emerging technology risks require continuous updates
Control Activities	Moderate	Weaknesses in automated controls and data validation
Information & Communication	Moderate	Regulatory reporting and CCRIS data quality issues
Monitoring Activities	Moderate	Better continuous monitoring and incident response needed

Figure 3. Table showing the assessment for each COSO components.

Figure 3 summarises the assessment of the five COSO internal control components based on the analysis of the ABC Islamic Bank's technology risk governance practices. The assessment indicates that the Control Environment is strong due to effective governance structures and active Board oversight. However, the other four components are rated as moderate, highlighting the need for continuous improvements in technology risk assessment, automated controls, regulatory data quality, and continuous monitoring. These findings provide the basis for the proposed recommendations to strengthen technology risk governance and operational resilience

5. Conclusion

Technology has become an important part of modern Islamic banking. While it helps banks provide faster and better services, it also creates new risks that require stronger governance and oversight. This study examined how ABC Islamic Bank manages technology risks by applying the COSO Internal Control Integrated Framework together with ERM, the Three Lines Model, Shariah Governance, and the Global Internal Audit Standards (GIAS 2024). The review shows that the bank has established a strong governance structure supported by the Board of Directors, the Audit Committee, the Risk Management Committee, the Shariah Committee, and Internal Audit. These functions work together to manage technology risks and support compliance with regulatory and Shariah requirements.

The review also identified several areas that need more attention. Repeated issues involving regulatory reporting, CCRIS data quality, digital banking disruptions, and operational resilience show that some controls are still not working as effectively as intended. The bank should strengthen data governance, improve system monitoring, increase automation, and respond more quickly to technology incidents. These improvements will help reduce operational risks and improve customer confidence.

Based on the overall assessment, the audit opinion is "Some Improvement Needed." The bank has built a good governance and risk management framework, but it needs to improve how those controls operate in practice. Stronger cybersecurity, better data quality, continuous monitoring, and faster incident response will help the bank manage future technology risks more effectively.

This study also introduces the TRGAM as a practical guide for Islamic Financial Institutions. The model brings together COSO, ERM, the Three Lines Model, Shariah

Governance, and GIAS 2024 into one integrated approach. It can help banks strengthen governance, improve operational resilience, support better decision making, and maintain public confidence as digital banking continues to grow.

References

- Bank Negara Malaysia. (2013). Financial Services Act 2013 and Islamic Financial Services Act 2013 come into force. <https://www.bnm.gov.my/-/financial-services-act-2013-and-islamic-financial-services-act-2013-come-into-force>
- Bank Negara Malaysia. (n.d.). Home. <https://www.bnm.gov.my/>
- Maybank. (2025). Integrated annual report 2025. <https://www.maybank.com/en/investor-relations/reports.page>.
- Maybank. (n.d.). Islamic banking solutions. <https://www.maybank2u.com.my/maybank2u/malaysia/en/islamic/>
- Maybank. (n.d.). Maybank2u Malaysia. <https://www.maybank2u.com.my/>
- Securities Commission Malaysia. (n.d.). Corporate governance strategic priorities. <https://www.sc.com.my>.
- Securities Commission Malaysia. (n.d.). Home. <https://www.sc.com.my>.
- The Commissioner of Law Revision, Malaysia. (2013). Islamic Financial Services Act 2013 (Act 759). <https://lom.agc.gov.my>.