

**FinSure Integrated Adaptive Security Governance
Framework: A Hybrid ITIL 4 and ISO/IEC 27001
Approach for Cloud First Banking Security,
Governance, and Compliance**

Student Name:	MD Monsuruzzaman
Student ID:	2504658
Programme:	MSc Cybersecurity and Digital Forensics
Institution:	University of Wales Trinity Saint David London
Module:	Data Security, Governance and Compliance
Module Code:	ACCA7028
Lecturer:	Dr. Ayman Al Hajjar
Submission Date:	29 April 2026

Table of Contents

Abstract	3
I. Introduction	4
II. Research into Security Frameworks and Models	5
2.1 ISO/IEC 27001: Strong for Rules but Not Flexible	8
2.2 ITIL 4: Effective for Services but Weak for Security	8
2.3 NIST Cybersecurity Framework (CSF 2.0)	9
2.4 COBIT 2019: Strong Governance but Complex	9
2.5 Critical Summary and Banking Impact	10
III. Proposed Approach for FinSure Bank	11
3.1 Design of the FinSure Integrated Adaptive Security Governance Framework (FIASGF)	11
3.2 FIASGF Mapping to FSB Requirements and Brief Factors	12
3.3 Design Rationale	13
3.4 Originality	13
3.5 Implementation Roadmap	14
3.6 How FIASGF Solves FSB Problems	14
IV. Critical Evaluation	15
V. Critique, Analysis, and Discussion: Why Constantly Updating Regulations and Standards Is Effective Practice	16
VI. Conclusion	18
References	19

Abstract

FinSure Bank (FSB), a rapidly expanding digital-first financial institution operating predominantly within cloud-based environments and Bring Your Own Device (BYOD) practices, faces significant challenges in ensuring data security, regulatory compliance, and operational resilience. The increasing reliance on distributed systems and third-party services has expanded the organisational attack surface, exposing the bank to threats such as ransomware, data breaches, and governance fragmentation. This report critically evaluates established security frameworks, including ISO/IEC 27001, ITIL 4, NIST Cybersecurity Framework (CSF 2.0), and COBIT 2019, supported by recent literature (2023–2026). The analysis shows that no single framework fully meets governance, compliance, and real-time security requirements. To address these limitations, the FinSure Integrated Adaptive Security Governance Framework (FIASGF) is proposed.

The framework integrates governance, risk management, compliance, and operational security into a unified model, incorporating KPI-driven monitoring, zero-trust principles, and continuous compliance mechanisms.

The findings emphasise that static, audit-driven approaches are insufficient in modern cybersecurity contexts. Instead, adaptive, integrated, and continuously monitored frameworks are essential to ensure resilience against evolving threats and regulatory changes.

Keywords: Data security governance, ISO 27001, ITIL 4, compliance, risk management, hybrid framework, cloud banking, BYOD

I. Introduction

The rapid growth of digital banking has significantly increased reliance on cloud infrastructure, mobile technologies, and third-party services. While these developments enhance scalability and operational efficiency, they simultaneously expand the attack surface, exposing financial institutions to increased risks such as cyberattacks, data breaches, and regulatory non-compliance [11], [12], [13].

FinSure Bank (FSB) operates within a predominantly cloud-based environment and adopts Bring Your Own Device (BYOD) practices, allowing employees and external partners to access organisational systems through personal devices. Although this approach improves flexibility and productivity, it introduces substantial security challenges, particularly in maintaining consistent governance, enforcing access controls, and ensuring compliance with regulatory frameworks. FSB currently lacks unified governance, structured risk management, and continuous compliance monitoring, resulting in fragmented security and limited risk visibility. This report addresses these challenges through two key objectives. First, it critically evaluates established security frameworks, including ISO/IEC 27001, ITIL 4, NIST Cybersecurity Framework (CSF 2.0), and COBIT 2019. Second, it proposes a hybrid framework the FinSure Integrated Adaptive Security Governance Framework (FIASGF) designed to integrate governance, risk management, and operational security into a cohesive model. The study assumes that FSB must comply with regulatory requirements such as GDPR and PCI-DSS, that cloud providers maintain baseline certifications without fully enforced security agreements, and that senior management will support implementation within a 12-18 month timeframe.

The report is structured as follows: Section II presents a critical analysis of existing frameworks, Section III introduces the proposed FIASGF model, Section IV evaluates its strengths and limitations, and Section V discusses the importance of adaptive governance in response to evolving threats and regulations.

II. Research into Security Frameworks and Models

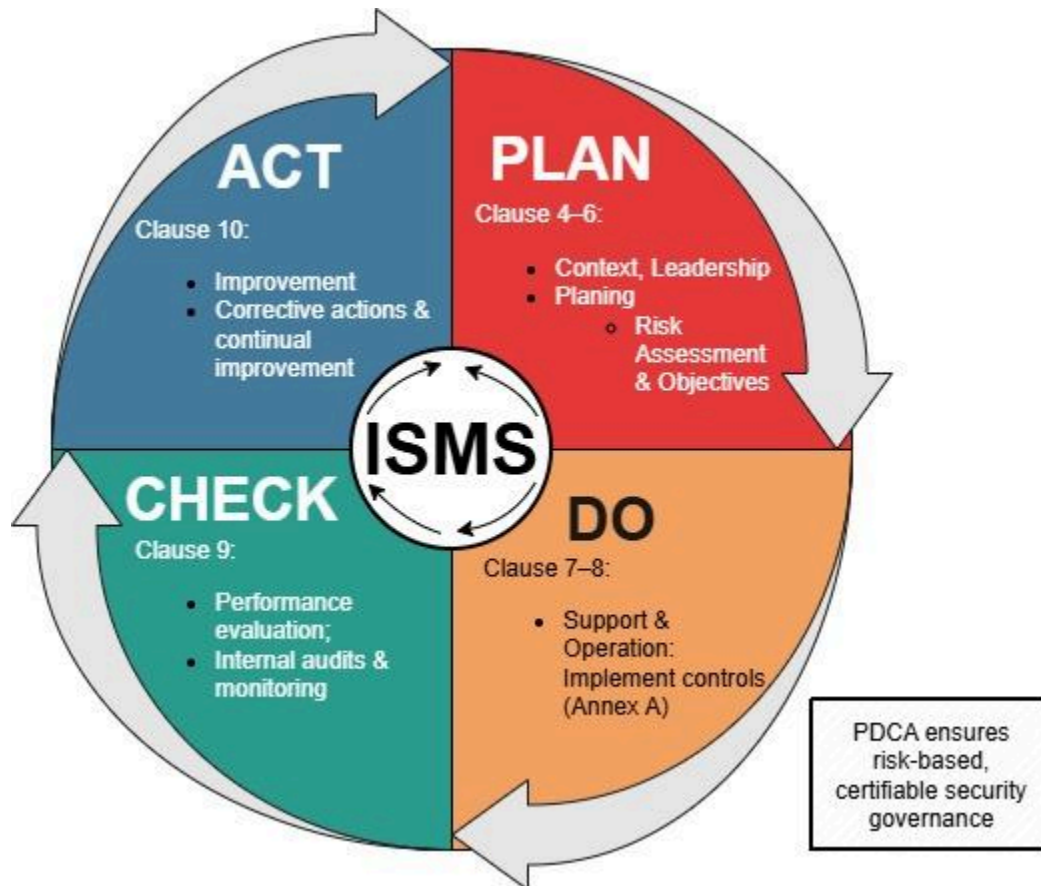


Fig. 1. ISO/IEC 27001 Plan-Do-Check-Act (PDCA) cycle for ISMS, adapted from ISO/IEC 27001:2022 [4].

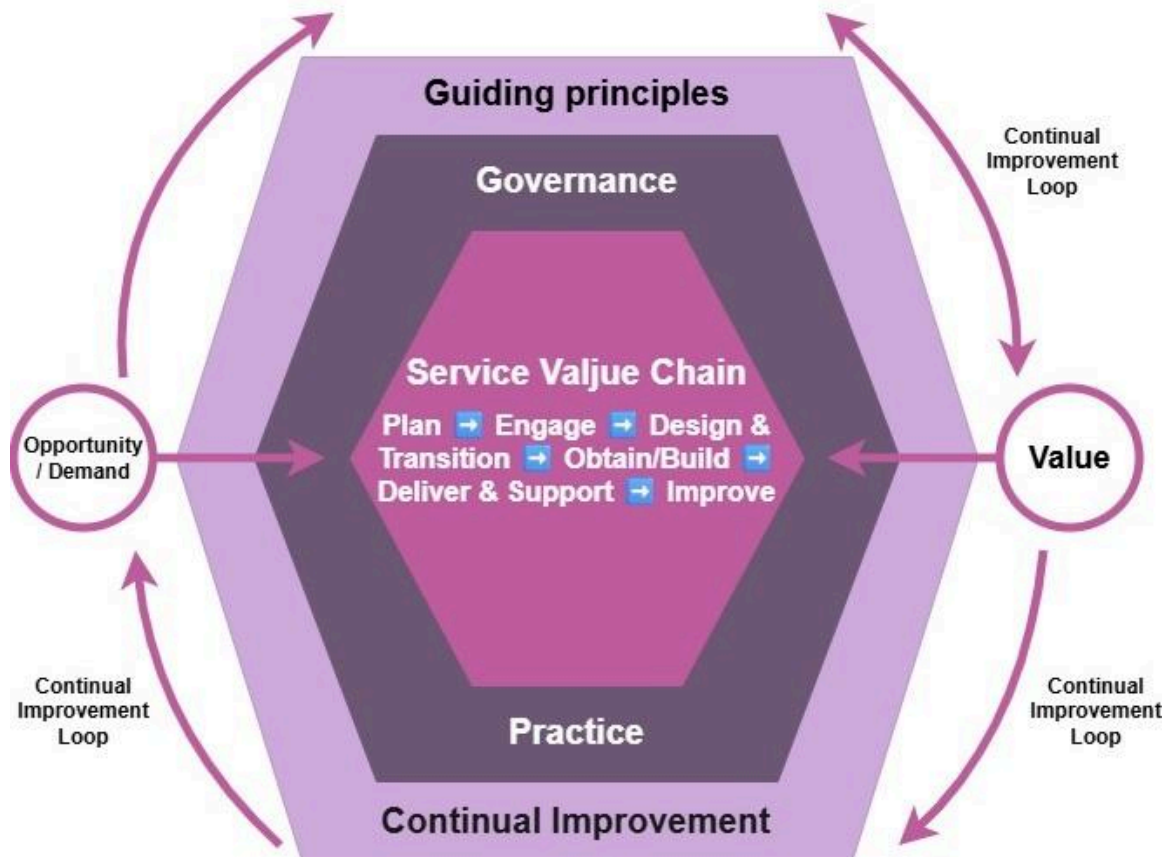


Fig. 2. ITIL 4 Service Value System (SVS) illustrating governance, value streams, and continual improvement [6].

TABLE I

Comparative Analysis of Security Frameworks for Cloud-First Banking Environments

Framework	Risk Management	Compliance Focus	Cloud/BYOD Suitability	Banking Relevance	Key Limitations
ISO 27001	High	GDPR, PCI-DSS	High	High	Limited operational service focus
ITIL 4	Medium	SLA & continuity	High	High	Not inherently security specific
NIST CSF 2.0	High	Govern function	High	Medium High	No formal certification
COBIT 2019	High	Enterprise governance	Medium	High	High complexity for rapid adaption

The selection of appropriate governance and security frameworks is a critical strategic decision for cloud-first banking institutions such as FinSure Bank. Financial organisations operate within highly regulated environments where **risk management, compliance, cloud suitability, and operational resilience** must be addressed simultaneously. This section critically evaluates ISO/IEC 27001, ITIL 4, NIST Cybersecurity Framework (CSF) 2.0, and COBIT 2019, with a focus on their applicability within modern banking systems.

2.1 ISO/IEC 27001: Strong for Rules but Not Flexible

ISO/IEC 27001 is widely recognised as an international standard for information security management, providing a structured and risk-based approach through the implementation of an Information Security Management System (ISMS). It aligns closely with regulatory requirements such as GDPR and PCI-DSS, making it highly relevant for financial institutions [4], [5]. The framework enables organisations to systematically identify, assess, and mitigate risks in a controlled and structured manner. However, despite its strengths, ISO/IEC 27001 presents several limitations. Its documentation-intensive and compliance-driven nature can reduce organisational agility, particularly in dynamic cloud environments where systems are frequently updated. In modern banking systems, where infrastructure and services evolve rapidly, this rigidity can limit responsiveness to emerging threats, including zero-day vulnerabilities and AI-driven cyberattacks. Furthermore, the framework primarily focuses on governance and compliance rather than real-time threat detection and response capabilities. Therefore, while ISO/IEC 27001 provides a strong foundation for governance and regulatory compliance, it must be complemented by more adaptive and operationally focused frameworks to effectively address the challenges of cloud-first banking environments.

2.2 ITIL 4: Effective for Services but Weak for Security

ITIL 4 is a widely adopted framework for IT service management, focusing on service delivery, incident handling, and continuous improvement [6]. The framework is well-suited to cloud and BYOD environments due to its emphasis on flexibility, service integration, and value-driven processes. It supports efficient service delivery and enhances organisational resilience through structured workflows. However, ITIL 4 has notable limitations in the context of cybersecurity. It does not provide comprehensive security controls or detailed mechanisms for threat detection, risk management, and system protection. As a result, organisations relying solely on ITIL may improve operational efficiency but remain exposed to cybersecurity risks [17], [18]. Therefore, ITIL 4 should be used as a complementary framework, supporting service management while being integrated with more security-focused models to ensure comprehensive protection.

2.3 NIST Cybersecurity Framework (CSF 2.0): Flexible but Not Certified

The NIST Cybersecurity Framework (CSF) 2.0 provides a flexible and adaptive model based on five core functions: Identify, Protect, Detect, Respond, and Recover. Its modular design makes it highly suitable for cloud-first banking environments, where security requirements evolve rapidly [9]. NIST CSF excels in operational risk management, offering practical guidance on incident detection and response. It supports continuous monitoring and aligns well with modern security practices such as Zero Trust Architecture. This makes it particularly effective in addressing real-time threats, including phishing attacks, ransomware, and insider risks. However, a key limitation is the absence of formal certification, which reduces its effectiveness in demonstrating compliance to regulators. Financial institutions often require certifiable standards to meet audit and legal requirements, and NIST's voluntary nature can be perceived as insufficient in this context [9]. Consequently, while NIST provides strong operational capabilities, it must be integrated with standards such as ISO 27001 to ensure full compliance and governance.

2.4 COBIT 2019: Strong Governance but Complex

COBIT 2019 focuses on enterprise IT governance, ensuring alignment between IT systems and business objectives. It is particularly valuable in banking environments where strategic oversight and regulatory accountability are critical [10], [1]. COBIT provides comprehensive governance structures, performance metrics, and control objectives, making it highly effective for board-level decision-making and compliance management. It also supports integration with other frameworks, enabling organisations to build a layered security approach. However, COBIT's primary limitation is its complexity and resource-intensive implementation. Its broad scope can make it difficult to adopt quickly, particularly in agile cloud environments. Additionally, COBIT does not provide detailed technical security controls, requiring integration with frameworks such as ISO 27001 and NIST [18].

2.5 Critical Summary and Banking Impact

This analysis highlights that no single framework sufficiently addresses the combined governance, operational, and compliance requirements of cloud-first banking environments. Each framework provides distinct strengths but also introduces specific limitations. ISO/IEC 27001 offers strong governance and compliance assurance but lacks flexibility. NIST CSF provides adaptability and real-time response capabilities but does not offer formal certification. ITIL 4 enhances service management but lacks comprehensive security controls, while COBIT 2019 delivers strategic governance but introduces implementation complexity. In practice, financial institutions require an integrated approach that combines governance, operational efficiency, and adaptive security capabilities. This reinforces the need for a hybrid framework capable of bridging the gap between strategic oversight and technical enforcement. Furthermore, the increasing adoption of cloud systems and BYOD environments introduces additional challenges related to identity management, data protection, and access control. Addressing these challenges requires continuous monitoring, automation, and adaptive security mechanisms [17], [18], [3].

III. Proposed Approach for FinSure Bank

3.1 Design of the FinSure Integrated Adaptive Security Governance Framework (FIASGF)

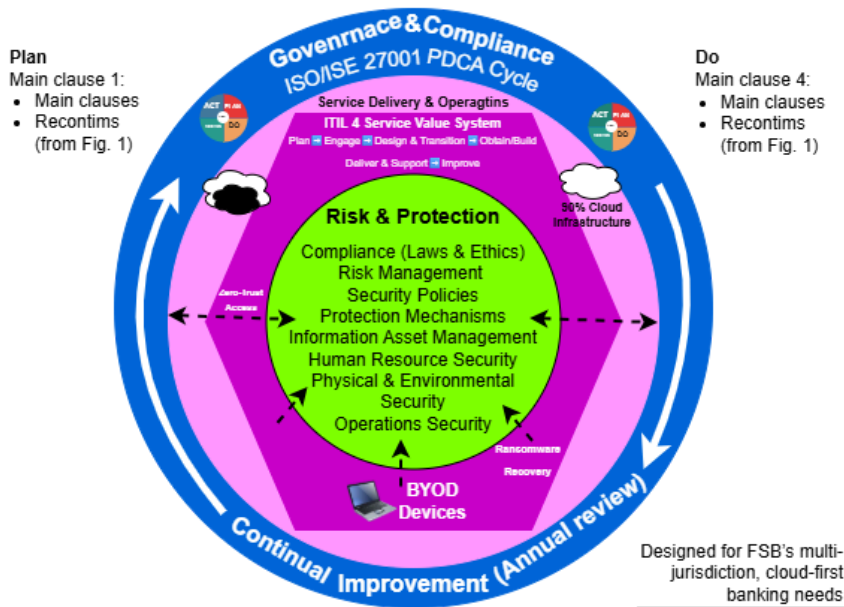


Fig. 3. FinSure Integrated Adaptive Security Governance Framework (FIASGF) layered model integrating ISO 27001 and ITIL 4 for cloud-first banking environments.

TABLE II

3.2 FIASGF Mapping to FSB Requirements and Brief Factors

Factor from Brief	FIASGF Component	FSB-Specific Implementation	Measurable KPI / Expected Benefit
Compliance (Laws & Ethics)	ISO 27001 Clauses 4–6 + legal register	GDPR/PCI-DSS mapping + ethical AI review board	100 % audit pass rate; zero fines
Governance & Strategic Planning	ITIL Governance + ISO Leadership	Board-level Security Committee	Quarterly strategic reviews
Security Policies	ISO Annex A + ITIL policy-as-code	Zero-trust BYOD acceptable-use policy	>95 % policy compliance
Risk Management	ISO risk assessment + ITIL improvement	Monthly quantitative cloud/BYOD risk scoring	Updated enterprise risk register
Security Management Models	Hybrid PDCA + Service Value Chain	Integrated incident response workflow	Mean time to respond < 4 hours
Contingencies Planning	ISO Clause 8 + ITIL continuity	Ransomware recovery playbook + biannual testing	99.9 % uptime during incidents
Protection Mechanisms	ISO technical controls + zero-trust	MDM + encryption at rest/transit for BYOD/cloud	Breach containment < 1 hour
Service Level Agreement	ITIL Service Design + ISO evaluation	MDM + encryption at rest/transit for BYOD/cloud	99.95 % availability

3.3 Design Rationale

The FinSure Integrated Adaptive Security Governance Framework (FIASGF) is designed to address the structural fragmentation identified within FSB. Unlike traditional approaches that apply security frameworks independently, FIASGF integrates governance, risk management, compliance, and operational security into a unified architecture. The framework eliminates siloed decision-making by aligning ISO/IEC 27001 (governance and compliance), NIST CSF (risk management and operational security), COBIT (strategic alignment), and ITIL 4 (service management). This integration ensures that security controls are not only defined at a strategic level but also enforced at an operational level. A key design feature of FIASGF is the implementation of policy-as-code mechanisms, enabling automated enforcement of security policies across cloud and BYOD environments. This approach shifts governance from periodic audits to continuous compliance, ensuring real-time enforcement of security controls.

Furthermore, the framework incorporates zero-trust architecture and continuous risk monitoring, reflecting modern cybersecurity practices that prioritise identity-based access control and adaptive security responses [1], [10], [9].

3.4 Originality (What Makes FIASGF Different)

The originality of FIASGF lies in its KPI-driven governance model. By linking security performance to measurable indicators such as incident response time, compliance rates, and system availability, the framework enables data-driven decision-making and enhances accountability within the organisation.

This integrated and adaptive approach ensures that FSB can respond effectively to evolving threats while maintaining compliance with regulatory requirements [13], [16], [14].

3.5 Implementation Roadmap

The implementation of FIASGF requires a structured and phased approach to ensure effective integration while minimising operational disruption [14].

Phase 1: Governance Assessment and Alignment

This phase evaluates FSB's existing governance structures and identifies key gaps, supported by a centralised governance committee.

Phase 2: Policy Harmonisation and Integration

This stage develops unified policies aligned with ISO/IEC 27001 and zero-trust principles, using policy-as-code for automated enforcement.

Phase 3: Technological Enablement

This phase deploys key technologies such as risk management platforms, cloud dashboards, and automated compliance tools.

Phase 4: KPI Operationalisation and Monitoring

KPIs are embedded into governance processes, supported by real-time dashboards and board-level reviews.

Phase 5: Continuous Improvement and Resilience Testing

The final phase ensures sustainability through continuous monitoring, audits, and resilience testing.

3.6 How FIASGF Solves Problems

FIASGF directly addresses the governance fragmentation and operational inefficiencies identified within FSB by introducing a unified and integrated security model. **Firstly**, the framework establishes a centralised governance structure, ensuring that security, risk, and compliance functions operate under a single coordinated system. This eliminates siloed decision-making and

improves consistency across departments. **Secondly**, FIASGF standardises security controls by aligning them with internationally recognised frameworks. This ensures uniform implementation, simplifies compliance processes, and enhances audit readiness. **Thirdly**, the framework integrates risk management and compliance into a unified workflow supported by shared dashboards and reporting mechanisms. This enables real-time visibility of organisational risk and supports faster, data-driven decision-making. **Additionally**, the use of KPI-driven monitoring enhances transparency and accountability. Senior management can assess performance in real time and respond proactively to emerging threats. **Finally**, FIASGF aligns security practices with business objectives by embedding security controls within service delivery processes. This ensures that security contributes to operational continuity, customer trust, and overall organisational resilience [18], [2].

IV. Critical Evaluation

The FIASGF framework offers several strengths. Its integrated multi-framework approach reduces governance fragmentation and improves coordination across security, risk, and compliance functions. By aligning ISO 27001, ITIL 4, NIST, and COBIT, the framework enhances organisational visibility and eliminates duplication of controls. The incorporation of KPI-driven governance enables measurable performance evaluation, supporting evidence-based decision-making and aligning with regulatory expectations for operational resilience. Additionally, the use of continuous monitoring, automation, and zero-trust principles improves the organisation's ability to detect and respond to advanced cyber threats. However, the framework also presents certain limitations. Its implementation complexity requires significant organisational coordination, technical expertise, and resource investment. Smaller institutions may find it challenging to adopt such an integrated model. Furthermore, the reliance on quantitative KPIs may overlook qualitative factors such as employee behaviour and organisational culture, which play a critical role in cybersecurity. There is also a risk that excessive monitoring and reporting requirements could reduce operational agility.

Overall, while FIASGF provides a comprehensive and adaptive solution, its effectiveness depends on organisational readiness, data accuracy, and the availability of skilled personnel. In practice, the effectiveness of FIASGF will depend on organisational maturity, leadership commitment, and the ability to sustain continuous monitoring and governance processes. This

highlights the importance of aligning technical implementation with organisational capability and governance maturity.

V. Critique, Analysis, and Discussion: Why Constantly Updating Regulations and Standards Is Effective Practice

Adaptive Governance in Response to Emerging Threats and Regulatory Evolution

Cyber threats are increasingly sophisticated, particularly AI-driven attacks and ransomware. Because of this, traditional static security systems are no longer enough. Banks like FSB must move from static governance to adaptive security systems that can change and respond quickly.

FSB faces many risks from AI-based attacks. These include automated phishing, deepfake fraud, and machine learning attacks that can trick or bypass traditional security controls [11], [8]. At the same time, ransomware has become more organised. Attackers now use “Ransomware-as-a-Service” (RaaS), which allows them to carry out large and targeted attacks on banks and important systems [12]. These changes show that checking risks only once in a while is no longer sufficient. Static compliance models cannot keep up with modern threats. This is why continuous monitoring and fast response systems are needed. FIASGF includes these features to handle threats in real time. Technology is also changing fast, which makes governance more complex. Many banks now use cloud systems, open banking APIs, and BYOD devices. These increase the number of ways attackers can enter the system. They also create connections between internal systems and third-party providers. Research shows that more than 60% of financial institutions had security problems related to third parties between 2023 and 2025 [13], [7]. This shows the need for real-time visibility of risks across all systems.

FIASGF addresses these challenges through integrated solutions such as cloud risk dashboards, zero-trust security, and automated policy enforcement. Emerging regulations such as the Digital Operational Resilience Act (DORA), NIS2 Directive, and the EU AI Act require stronger governance, accountability, and continuous compliance mechanisms. These regulations require stronger security, better reporting, and clear accountability at senior levels [15], [16]. These

regulations emphasise continuous compliance, regular testing, and strong governance requirements.

FIASGF supports these requirements by using continuous improvement models from ISO (PDCA) and ITIL (SVS). It also uses monthly KPI dashboards. This ensures that regulatory changes are automatically reflected in risk scores and security controls. By linking rules directly to KPIs, FIASGF ensures that compliance is part of daily operations, not just something checked occasionally [15], [14]. However, there is also a problem called implementation fatigue. Banks often have to deal with too many frameworks and rules at the same time. This can result in staff burnout, increased costs, and reduced effectiveness of security controls. Too many processes and reports can also slow down the organisation and reduce flexibility. FIASGF recognises this issue. Instead of adding more frameworks, it combines them into one system. This reduces duplication and keeps the system simpler and more efficient. Even though adaptive frameworks are flexible, they depend on accurate data, effective automation tools, and skilled personnel. This highlights the need for organisational maturity to effectively implement such frameworks. Overall, FIASGF is designed as an adaptive framework capable of responding to evolving threats, technologies, and regulatory requirements.

By using continuous monitoring, KPI-based management, and integrated frameworks, it enables FSB to stay secure and prepared for both current and future challenges.

VI. Conclusion

The FinSure Integrated Adaptive Security Governance Framework (FIASGF) provides a comprehensive and scalable solution to the security, governance, and compliance challenges faced by FinSure Bank. By integrating multiple established frameworks into a unified and adaptive model, it enhances organisational resilience, improves risk visibility, and aligns security practices with business objectives. This study demonstrates that continuously evolving regulations and standards are not merely compliance requirements but strategic enablers of long-term resilience. In a rapidly changing threat landscape, static governance models are insufficient, highlighting the need for adaptive and integrated approaches.

It is recommended that FSB adopts a phased implementation strategy, beginning with a detailed gap analysis to identify existing weaknesses. Future research should focus on empirical validation of FIASGF through real-world deployment within financial institutions to assess its effectiveness and scalability.

References:

- [1] B. Metin, "Towards an integrated approach based on COBIT and ISO/IEC standards for cybersecurity strategy," *Standards*, vol. 5, no. 4, 2025. Available: <https://www.mdpi.com/journal/standards>
- [2] K. Al-Dosari et al., "Risk-management framework and information-security systems for banks," *Electronics*, vol. 12, no. 17, 2023. Available: <https://www.mdpi.com/journal/electronics>
- [3] M. R. Georgescu, "Data governance as the digital backbone of proactive cybersecurity," *Economies*, vol. 13, no. 9, p. 272, 2025. Available: <https://www.mdpi.com/journal/economies>
- [4] International Organization for Standardization, *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection Information Security Management Systems - Requirements*. Geneva, Switzerland: ISO, 2022. Available: <https://www.iso.org/standard/82875.html>
- [5] M. Suorsa, "ISO/IEC 27001 controls ranked based on GDPR," *Information Security Journal: A Global Perspective*, 2024. Available: <https://www.tandfonline.com/toc/uiss20/current>
- [6] AXELOS, *ITIL 4: Foundation*. London, U.K.: AXELOS, 2019. Available: <https://www.axelos.com/certifications/itil-service-management/itil-4-foundation>
- [7] Huawei, *Data Security Governance Practices*. Shenzhen, China: Huawei, Sep. 2025. Available: <https://www.huawei.com/en/publications>
- [8] A. Ahmed, "Evaluating the effectiveness of data governance frameworks," *PLOS ONE*, 2025. Available: <https://journals.plos.org/plosone/>
- [9] NIST, *Framework for Improving Critical Infrastructure Cybersecurity (CSF) 2.0*. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2023. Available: <https://www.nist.gov/cyberframework>
- [10] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*. Schaumburg, IL, USA: ISACA, 2023. Available: <https://www.isaca.org/resources/cobit>
- [11] ENISA, *Threat Landscape Report 2024*. Heraklion, Greece: European Union Agency for Cybersecurity, 2024. Available: <https://www.enisa.europa.eu/publications>
- [12] World Economic Forum, *Global Cybersecurity Outlook 2024*. Geneva, Switzerland: WEF, 2024. Available: <https://www.weforum.org/reports>
- [13] Deloitte, *Cyber Risk and Resilience in Financial Services*. London, U.K.: Deloitte, 2025. Available: <https://www2.deloitte.com/global/en/insights.html>
- [14] Deloitte, *Continuous Compliance in Financial Services*. London, U.K.: Deloitte, 2025. Available: <https://www2.deloitte.com/global/en/insights.html>
- [15] European Commission, *Digital Operational Resilience Act (DORA)*, 2024. Available: <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>

[16] Basel Committee on Banking Supervision, *Principles for Operational Resilience*. Basel, Switzerland: BIS, 2024. Available: <https://www.bis.org/bcbs/publications.htm>

[17] ENISA, *Threat Landscape Report 2025*. Heraklion, Greece: ENISA, 2025. Available: <https://www.enisa.europa.eu/publications>

[18] D. Puthal et al., “Cybersecurity frameworks and enterprise risk management,” *Journal of Cybersecurity*, 2023. Available: <https://academic.oup.com/cybersecurity>