

A Unified Security, Governance, and Compliance Framework for FinSure Bank

Student Name: Muhammad Haroon

Data Security, Governance and Compliance

Lecturer: Dr. Vijeyanathan Thayanathan



Table of Contents

Abstract	2
1. Introduction	2
2. Research into Security Frameworks and Models.....	3
2.1. Information Technology Infrastructure Library (ITIL)	3
2.1.1. Key Components Relevant to FSB	3
2.2 ISO/IEC 27000 Series (Focus on ISO/IEC 27001)	4
3. A Designed Approach for FinSure Bank	5
3.1 Pillar 1: Governance and Strategic Planning for Security	5
3.2 Pillar 2: Risk Management and Compliance	6
3.3 Pillar 3: Security Operations (Protection Mechanisms & Policies)	7
3.4 Pillar 4: Resilience and Assurance (Contingencies & Service Level Agreements)	8
4. Critique and Analysis: The Imperative of Evolving Regulations and Standards	9
4.1 Adapting to Technological Innovation and Emergent Threats	9
4.2 Driving a Culture of Continuous Improvement	9
4.3 Enhancing Stakeholder Trust and Market Confidence	10
4.4 Addressing Systemic Risk and Establishing Accountability	10
5. Conclusion	11
6. References	12

Abstract

The present-day digital revolution of the financial service sector, just as seen in the case of the Fin Sure Bank (FSB) has brought a complex plethora of information security problems. Cloud-based infrastructure deployment, BYOD policy, and fragmented security posture place FSB at a significant risk, including failures to meet regulations, breach of information, and insider threat. The report is a critical evaluation of established security frameworks i.e. ITIL and ISO/IEC 27001 to assist in the design of a custom stitched security governance model to be implemented in FSB. The proposed framework will merge the governance, risk management, compliance and security operations in one structure that will be tailored to the digital-first, cloud-native environment of the organisation. Further, the report decries the necessity to come up with regulations and standards based on the premise that they will be useful towards decreasing the emergent threats, culture of unrelenting improvement, and assure the stakeholders of confidence in a constantly changing digital landscape. It concludes with the roadmap of step by step implementation, which may also point to the fact that in the case of FSB, security does not constitute a product, but an evolving, business-facilitating capability.

1. Introduction

Information security has been developed to be a pillar of organisational resiliency in digital economy particularly in the financial services industry. FinSure Bank (FSB) being a digital-first financial institution is in a precarious growth period, as the case scenario shows. Its business model characterized by the cloud-native infrastructure, workforce that is geographically spread through personal devices (BYOD) and an increased number of customers that rely on the usage of mobile applications exposes it to an even more significant threat environment (Dupont, 2019). The inability to implement detailed security policies, the single model of governance, and formalized risk management strategies puts FSB at the risk of regulative fines, financial fraud, reputational losses and operational disruption (Akinsola, 2025).

The urgent requirement in this report involves a systematic approach to the issue of security in FSB. It starts by studying the known security frameworks and models (including the Information Technology Infrastructure Library (ITIL) and the ISO/IEC 27000 family) in order to determine best practices (Merchan-Lima *et al.*, 2021). Using this knowledge, the report then develops an

integrated, personalized security, governance and compliance model in the specific context of FSB. Lastly, it gives a critical review of why the ever-changing nature of regulations and standards is not just a compliance cost but a general best practice to organisational survival and development. The recommendations are based on the analysis that FSB has a moderate-high budgetary allocation to security (in line with its growth stage), desire to embrace formal security culture, and it is primarily working within the European regulatory paradigm, and as such, GDPR is a major compliance factor (Desmoitier, 2023).

2. Research into Security Frameworks and Models

To be able to develop a powerful background of FSB, one must be familiar with the most popular frameworks that dictate IT service management and information security management. Two of the most notable ones are ITIL and ISO/IEC 27000 series.

2.1. Information Technology Infrastructure Library (ITIL)

ITIL is a collection of comprehensive ITSM practices that are aimed at aligning IT services to the business. In the case of FSB, security would not be an add-on to the IT services but should be integrated into the lifecycle.

2.1.1. Key Components Relevant to FSB

- **Service Strategy:** This step would make sure that the security investments made by FSB reflect its business objectives of fast growth and in a digitally-first service provision.
- **Service Design:** This is also crucially important and also encompasses the Security Management process. ITIL promotes security by design, whereby security controls should be integrated into new services (such as a new mobile banking feature) at the time they are created, and not afterwards (Gedela, 2025).
- **Service Operation:** This sector involves the daily operation of services. In the case of FSB, it would mean the adoption of sound Access Management controls to address the complications of BYOD and access by third-party partners, and Event Management to identify and react to security incidents in real-time (Al Harthy, 2022).
- **Continuous Service Improvement (CSI):** The CSI model of ITIL offers an opportunity to continuously assess and enhance security operations to shift FSB to the non-dispersed, reactive position to an optimized, proactive one (Yugay *et al.*, 2025).

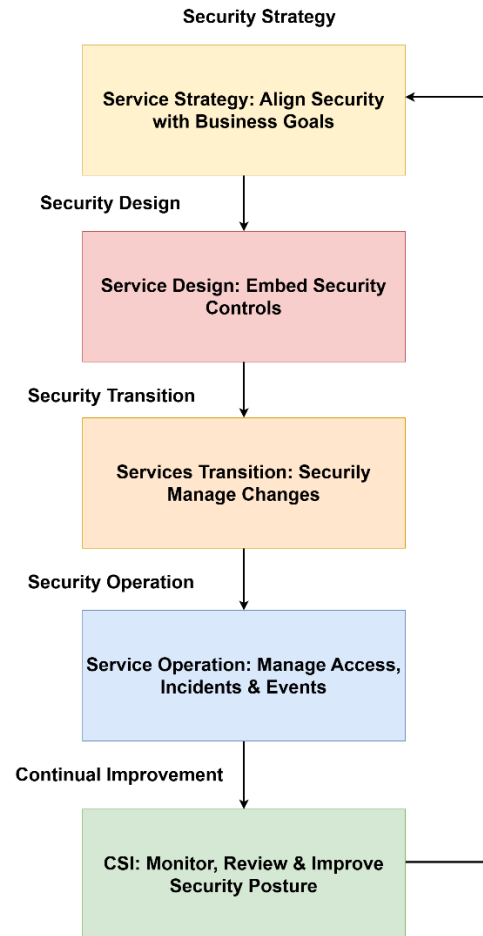


Figure 1: ITIL Service Lifecycle (Adapted for Security Context)

2.2 ISO/IEC 27000 Series (Focus on ISO/IEC 27001)

Whereas ITIL offers a process framework to operate in the management of IT services, the ISO/IEC 27000 family offers the specification of Information Security Management System (ISMS) (Al Faruq *et al.*, 2020). The ISO/IEC 27001 is the globally accepted standard in setting, setting up, sustaining and enhancing of an ISMS. It is premised on a risk management strategy and Plan-Do-Check-Act (PDCA) cycle.

Main elements that were applicable to FSB:

- **Clause 4: Context of the Organisation:** This obliges FSB to be aware of its own inner and outer environment such as needs and expectations of its stakeholders (customers, regulators, partners). This goes straight to the demand of a joint model of governance in the scenario.

- **Clause 5: Leadership:** Requires top management to lead and show its commitment to the ISMS. This is essential to FSB, because its existing disjointed strategy is probably not executive sponsored.
- **Clause 6: Planning:** Focuses on a risk approach. In the case of FSB, this formalises the risk management strategy, which involves it identifying, evaluating and treating risks associated with cloud hosting, BYOD, and insider threats.
- **Annex A:** This is a list of 93 security controls in 14 domains, including access control, cryptography, physical security, and supplier relationships. This can be taken as a checklist by FSB in order to develop its all-encompassing security policies.

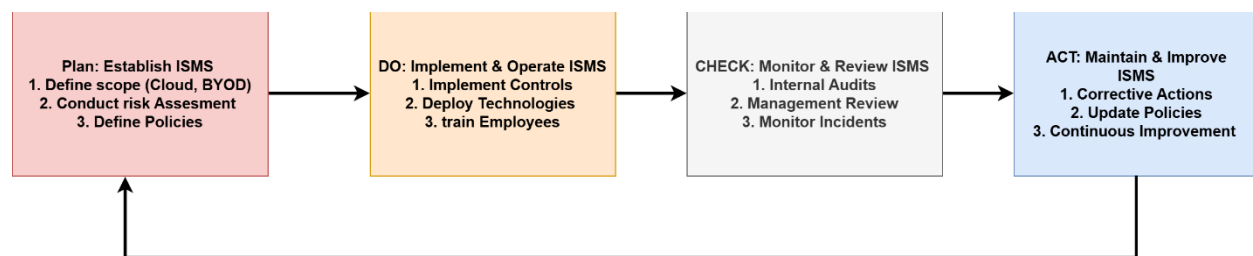


Figure 2: ISO/IEC 27001 Plan-Do-Check-Act (PDCA) Model for FSB

These two models are complementary. ITIL offers the process (manage security as a service), and ISO/IEC 27001 offers the management system (manage and govern, and assure compliance). The best way out of FSB would be to combine all these.

3. A Designed Approach for FinSure Bank

On the basis of the research, a tailored and combined system is suggested to satisfy the needs of FSB. The following framework is referred to as the Integrated Security, Governance and Compliance Framework (ISGC Framework), which is based on four pillars, as shown below.

3.1 Pillar 1: Governance and Strategic Planning for Security

Assumption: The executive leadership of FSB is devoted to the idea of security as the enabler of business.

- **Executive Security Committee:** FSB should form cross functional committee that is led by CISO (Chief Information Security Officer) and with the representatives of Legal, HR,

IT, and Business Units. This committee will have the duty of developing security strategy, passing of budgets, and alignment with business objectives (Kappers and Harrell, 2020).

- **Coherent Security Policies:** The haphazard strategy should be changed into a coherent set of policies. Basing its policies on ISO/IEC 27001 Annex A, FSB will draft policies that involve:
 - **Acceptable Use Policy (AUP):** Specification of the BYOD, personal use of devices, and access to the internet.
 - **Data Classification and Handling Policy:** Requires a policy to be set on the way sensitive financial and personal data should be handled, encrypted and shared.
 - **Access Control Policy:** Legalizing the principle of least privilege and role-based access control (RBAC) among the employees, contractors and partners.

3.2 Pillar 2: Risk Management and Compliance

- **Assumption:** FSB is based in a multi-jurisdictional setting and has GDPR as the main data protection law.
- **Risk Management Framework (RMF):** An official RMF that is grounded on the NIST (National Institute of Standards and Technology) Cybersecurity Framework (CSF) ought to be embraced. This framework has its main functions of Identify, Protect, Detect, Respond, recover that enables a common language of risk. For FSB, this means:
 - Detect: List all the cloud assets, flows of data, and third-party relationships. Risk register will be developed to monitor cloud misconfiguration risks, BYOD data leakage risks, and insider threats (Ademilua, 2021).
 - Protect: Application of safeguards, as provided in Pillar 3.
- **Compliance Automation:** Since the regulatory environment is dynamic, compliance checks cannot be done manually. FSB must invest in Cloud Security Posture Management (CSPM) tools which can automatically scan its cloud environments to be compliant with its benchmarks (such as CIS (Center for Internet Security)) and compliance regulations (e.g., GDPR data residency) (Garg, 2025). This guarantees compliance on a continuous basis as opposed to auditing that is one-time based.

3.3 Pillar 3: Security Operations (Protection Mechanisms & Policies)

- **Assumption:** FSB can afford to invest in newer security systems, specifically the endpoint and cloud security systems.
- **BYOD and Cloud Security:** There is no compromise when it comes to having a strong Unified Endpoint Management (UEM). This will impose security measures to every personal device that is used to access corporate data including:
 - The use of tough passcodes and biometrics.
 - Encryption of data of the corporation on the device (containerization).
 - The capability to remotely delete corporate data without interference with personal data.
 - In cloud security, the deployment of Cloud Access Security Brokers (CASBs) to offer visibility and control of data entering and leaving cloud applications can be used.
- **Identity and Access Management (IAM):** Well-developed IAM is the basis of the security in BYOD and cloud environment. FSB must implement:
 - Multi-Factor Authentication (MFA): This is required on all access to internal systems, as well as those of employees, contractors, and partners (Donald, Bumpus and Zhang, 2021).
 - Zero Trust Network Access (ZTNA): We are replacing traditional VPNs with ZTNA, which is an approach that allows access based on user identity, device posture, and context, and not network location. A cloud-native bank is best suited to this (Zohaib *et al.*, 2024).
- **Threat Intelligence / Security Operations Center (SOC):** SOC is necessary and can either be managed or in-house to offer 24/7 monitoring, detection, and response. This will make use of threat intelligence to hunt proactively on indicators of compromise (IOCs), and in particular those of financial fraud.

3.4 Pillar 4: Resilience and Assurance (Contingencies & Service Level Agreements)

Because the majority of infrastructure at FSB is served in the cloud, vendor operation and resilience cannot be considered secondary, as they need to be developed to the full extent and continuously managed.

- Outages of cloud providers are among the most critical risks as it is viewed through a Business Continuity (BC) and Disaster Recovery (DR) prism. In this regard, a powerful Business Continuity Plan (BCP) and clearly defined Disaster Recovery Plan (DRP) should be put in place by FSB (Balibek, Storkey and Yavuz, 2021).
 - One of the most important elements of this is redundancy. Applications must be created to operate in more than one availability zone (AZ) and where possible even in more than one cloud provider. This will decrease the dependence on any particular environment and will reduce the risk of a total cut of the service.
 - Testing is important too. Plans are never good unless they are seen to work in practice. FSB is advised to conduct regular tabletop exercises and full failover exercising to test the response procedures and to be sure that systems can recover according to what is expected in real life conditions.
- Service Level Agreement (SLA) is also important in a cloud-native banking model. Contracts with cloud providers, managed security service providers (MSSPs) and other third parties should state security expectations (Chitraju, 2024). It incorporates the following specifics: incident response schedules, penetration testing requirements, and explicit procedures of data breach notification.
 - FSB should also adopt an elaborate Third-Party Risk Management (TPRM) program in parallel. This program must also constantly evaluate and observe the security positioning of all their critical vendors, and make sure that their practices are consistent with those of FSB itself and with the requirements of the security regulations (Haritwal, 2025).

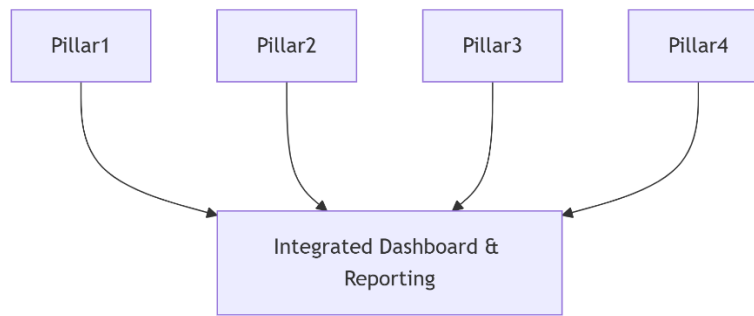


Figure 3: The Integrated Security, Governance, and Compliance (ISGC) Framework

4. Critique and Analysis: The Imperative of Evolving Regulations and Standards

Having regulations and standards updated at all times is also part of best practice. Instead of being perceived as a drain on the budget, this continuous transformation contributes to organisational stability as well as greater resilience in society at large (Bhamra and Brodersohn, 2025). It is this flexibility that is particularly crucial to an organisation such as FSB due to several important reasons.

4.1 Adapting to Technological Innovation and Emergent Threats

In the context of the FSB, it means that in the nearest future, the application of AI in issues like credit assessment or fraud detection is going to be subject to a stricter regulatory control. Unless security structures are adjusted in line with such changes, organisations might be caught relying on the outdated security measures as they face more sophisticated risks (Mallick and Nath, 2024). An ongoing revision of regulations would stimulate organisations to constantly revise and transform their technology settings so that innovation would be consistent with the best security practices and compliance rules (Folorunso, Wada, *et al.*, 2024).

4.2 Driving a Culture of Continuous Improvement

A tick-box compliance culture is very likely to result in a static regulatory environment. In such culture the aim is just to fulfill a set number of requirements. This is exactly the disjointed and complacent strategy that FSB is already experiencing (FSB, 2023).

When regulations and standards are constantly updated, like the different versions of ISO/IEC 27001 organisations must keep improving (Folorunso, Mohammed, *et al.*, 2024). The European Banking Authority for example keeps updating its guidance. Organisations are forced to re-evaluate their Information Security Management System (ISMS). They need to re-evaluate their risk analysis. Update their controls. Through this process, the view on security is altered. It is no longer a fixed cost, but a moving business ability.

It is essential to FSB adopting such a mentality. It should stop being reactive and shift to proactive and predictive security posture (Mwase, 2025). This implies that security is a business capability rather than a cost that FSB should pay attention to. FSB should reconsider its ISMS and revise its controls on a regular basis.

4.3 Enhancing Stakeholder Trust and Market Confidence

The most important thing for institutions is the new rules. These new rules and standards are like a promise that the institution will do what is right by its customers, investors and partners. When the Financial Stability Board wants to get into markets or work with financial technology companies it is helpful to show that it is following the latest standards, like the ones from the International Organization for Standardization that came out in 2022, which pay a lot of attention to cloud and threat intelligence (Pitkar, 2025). This shows that the institution is good at keeping things secure. It is, like having someone else say that the institution is doing a job of keeping things safe. On the hand if the institution does not keep up with the new standards it can hurt its reputation and make people think that it is not careful enough which can make it more likely that something bad will happen and customers will lose faith in the institution (Van Der Cruijssen, De Haan and Roerink, 2023).

4.4 Addressing Systemic Risk and Establishing Accountability

The financial system is all connected, so when one company like FSB has a problem, it can cause a lot of problems too. When something big goes wrong like the crisis in 2008 new rules are made to help prevent it from happening again (Dalio, 2022). For example, the 2008 financial crisis led to Basel III and the NotPetya attack in 2017 showed that companies need to be better prepared for things like that which's why we have rules like the Digital Operational Resilience Act (*Emerging Financial Risks -2025 & Beyond* by Abhishek Nagesh :: SSRN, 2025). DORA. DORA says that

financial companies like FSB have to be very careful with their computer systems and make sure they are safe. They have to test everything and make sure the other companies they work with are safe too. These new rules are not just made up they are because people found some weaknesses in the system. They help make sure that companies are responsible for managing the risks and that someone is in charge of making sure they do it right. In this manner, it is not up to every company to sort all the issues but someone is managing everything to ensure it is done the right way similar to DORA and financial firms, such as FSB (Dalio, 2022).

This way it is not up to each company to deal with all the problems but someone is overseeing everything to make sure it is done correctly like with DORA and financial companies, like FSB (Dalio, 2022).

5. Conclusion

The things of ITIL and the good aspects of ISO/IEC 27001 have been incorporated into the report to form the Integrated Security, Governance and Compliance Framework. This is a plan that is developed in relation to FinSure Bank and it addresses the issues that were identified. It establishes a decision-making process, which consists of a committee of top managers and ensures that all policies are identical. It also makes risk management more formal and not just something that is done when it is needed. The plan protects the bank from risks like people using their own devices and cloud infrastructure by using things like UEM, ZTNA and a security operations center (Fopa Mamene, 2024). It also makes sure the bank can still operate even if something bad happens by having a plan in place and managing third party vendors closely.

This report also says that rules and standards are always changing and that is a thing. For FinSure Bank it is not a problem to keep up with these changes it is something that needs to be done. Following frameworks like DORA and ISO/IEC 27001:2022 helps the bank get better all the time makes stakeholders trust the bank and makes sure the banks security is always getting better to match the threats it faces (Karakasilioti, 2024).

To move forward FinSure Bank should follow a plan that is done in steps:

- Phase 1 which's from the start to six months the bank should set up a governance structure, like a chief information security officer and an executive committee. The bank should also

do a risk assessment using the NIST Cybersecurity Framework and write the main security policies.

- Phase 2 which's from six months to a year the bank should start doing basic security operations like managing user devices and identities with multi factor authentication. The bank should also start looking at what it needs to do to meet the ISO/IEC 27001 standards.
- Phase 3 which's from one year to two years the bank should get certified in ISO/IEC 27001 put in place advanced security controls like zero trust network access and a security operations center that is open all the time. The bank should also make sure it is managing third party risk and automating compliance programs.

6. References

Ademilua, D.A. (2021) “Cloud security in the era of big data and IoT: A review of emerging risks and protective technologies,” *Communication in Physical Sciences*, 7(4), pp. 590–604.

Akinsola, K. (2025) “Regulatory Compliance and the Role of Corporate Governance in Preventing Financial Misstatements,” *Available at SSRN 5126627* [Preprint]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5126627 (Accessed: March 24, 2026).

Al Faruq, B. *et al.* (2020) “Integration of ITIL V3, ISO 20000 & iso 27001: 2013 for it services and security management system,” *International Journal*, 9(3). Available at: <https://www.academia.edu/download/63914423/ijatcse15793202020200714-22443-1agpx5m.pdf> (Accessed: March 24, 2026).

Al Harthy, K. (2022) “A Risk Management Framework for the BYOD Environment.” Available at: https://pureportal.coventry.ac.uk/files/80093962/AlHarthy_2022_PhD.pdf (Accessed: March 24, 2026).

Balibek, M.E., Storkey, I. and Yavuz, H. (2021) *Business continuity planning for government cash and debt management*. International Monetary Fund. Available at: [https://books.google.com/books?hl=en&lr=&id=YB9HEAAQBAJ&oi=fnd&pg=PA5&dq=one+of+the+most+significant+risks.+To+address+this,+FSB+should+establish+a+robust+Business+Continuity+Plan+\(BCP\)+alongside+a+well-defined+Disaster+Recovery+Plan+\(DRP\).&ots=mUXMMI2Ppa&sig=gCwR_Lok3tX3snOSVve5UI_-TvE](https://books.google.com/books?hl=en&lr=&id=YB9HEAAQBAJ&oi=fnd&pg=PA5&dq=one+of+the+most+significant+risks.+To+address+this,+FSB+should+establish+a+robust+Business+Continuity+Plan+(BCP)+alongside+a+well-defined+Disaster+Recovery+Plan+(DRP).&ots=mUXMMI2Ppa&sig=gCwR_Lok3tX3snOSVve5UI_-TvE) (Accessed: March 24, 2026).

Bhamra, R. and Brodersohn, E. (2025) “Understanding organizational dynamism: Fostering creativity and agility for resilience in social security institutions,” *International Social Security Review*, 78(2–3), pp. 37–54. Available at: <https://doi.org/10.1111/issr.70003>.

Chitraju, S. (2024) “Cloud-Native Identity and Access Management for Financial Service Providers,” *Available at SSRN 5653690* [Preprint]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5653690 (Accessed: March 24, 2026).

Dalio, R. (2022) *Principles for navigating big debt crises*. Simon and Schuster. Available at: <https://books.google.com/books?hl=en&lr=&id=2eyaEAAQBAJ&oi=fnd&pg=PA75&dq=it+c+an+cause+a+lot+of+problems+too.+When+something+big+goes+wrong+like+the+crisis+in+2008+new+rules+are+made+to+help+prevent+it+from+happening+again&ots=ucCMZwVHYO&sig=mOD7GUrUI0Rzr838MJzwELv-QMQ> (Accessed: March 24, 2026).

Desmoitier, N. (2023) *Bridging sustainability scales, from global frameworks to operational methods for sub-level actors: focus on climate change mitigation strategies for organizations*. PhD Thesis. École centrale de Nantes. Available at: <https://hal.science/tel-04416882/> (Accessed: March 24, 2026).

Donald, E.C., Bumpus, M.A. and Zhang, X. (2021) “A case study in selection and deployment of a multi-factor authentication solution,” *Issues in Information Systems*, 22(3), pp. 62–72.

Dupont, B. (2019) “The cyber-resilience of financial institutions: significance and applicability,” *Journal of cybersecurity*, 5(1), p. tyz013.

Emerging Financial Risks -2025 & Beyond by Abhishek Nagesh :: SSRN (2025). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5241889 (Accessed: March 24, 2026).

Folorunso, A., Wada, I., *et al.* (2024) “Security compliance and its implication for cybersecurity,” *World Journal of Advanced Research and Reviews*, 24(01), pp. 2105–2121.

Folorunso, A., Mohammed, V., *et al.* (2024) “The impact of ISO security standards on enhancing cybersecurity posture in organizations,” *World Journal of Advanced Research and Reviews*, 24(1), pp. 2582–2595.

Fopa Mamene, M. (2024) *Secure Access Service Edge (SASE): Architecture, Implementation, and Performance Evaluation*. PhD Thesis. Hochschule Rhein-Waal. Available at: https://opus4.kobv.de/opus4-rhein-waal/frontdoor/deliver/index/docId/2070/file/Morelle-Fopa_Complete-Thesis.pdf (Accessed: March 24, 2026).

FSB, F.S.B. (2023) “2023 Bank Failures: Preliminary lessons learnt for resolution.” Available at: <https://elischolar.library.yale.edu/cgi/viewcontent.cgi?article=5294&context=ypfs-documents2> (Accessed: March 24, 2026).

Garg, P. (2025) “Cloud security posture management: Tools and techniques,” *Available at SSRN 5357921* [Preprint]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5357921 (Accessed: March 24, 2026).

Gedela, K.K.K. (2025) “Bridging Traditional ITSM and Modern Engineering: An Ethnographic Study of ITIL & SRE on GCP,” *Digital Repository of Theses* [Preprint]. Available at: <https://repository.learn-portal.org/index.php/rps/article/view/821> (Accessed: March 24, 2026).

Haritwal, S. (2025) “Food Safety Certification: Importance, Standards, and Global Implications,” *Standards, and Global Implications (October 03, 2025)* [Preprint]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5558880 (Accessed: March 24, 2026).

Kappers, W.M. and Harrell, M.N. (2020) “From degree to chief information security officer (CISO): A framework for consideration,” *2020 ASEE Virtual Annual Conference Content Access*. Available at: <https://peer.asee.org/from-degree-to-chief-information-security-officer-ciso-a-framework-for-consideration> (Accessed: March 24, 2026).

Karakasilioti, G.M. (2024) *Supporting the digital operational resilience of the financial sector: The EU's DORA Digital Operational Resilience Act*. Master's Thesis. Πανεπιστήμιο Πειραιώς. Available at: <https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/16273/DORA%20-%20MTE2109%20Karakasilioti.pdf?sequence=1&isAllowed=y> (Accessed: March 24, 2026).

Mallick, M.A.I. and Nath, R. (2024) “Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments,” *World Scientific News*, 190(1), pp. 1–69.

Merchan-Lima, J. *et al.* (2021) “Information security management frameworks and strategies in higher education institutions: a systematic review,” *Annals of Telecommunications*, 76(3–4), pp. 255–270. Available at: <https://doi.org/10.1007/s12243-020-00783-2>.

Mwase, A. (2025) *A Dynamic Security Model for the Fintech Ecosystem*. PhD Thesis. University of South Africa (South Africa). Available at: <https://search.proquest.com/openview/f581623e56f0e3591b8355d9795b7d42/1?pq-origsite=gscholar&cbl=2026366&diss=y> (Accessed: March 24, 2026).

Pitkar, H. (2025) “Cloud security automation through symmetry: Threat detection and response,” *Symmetry*, 17(6), p. 859.

Van Der Crujssen, C., De Haan, J. and Roerink, R. (2023) “Trust in financial institutions: A survey,” *Journal of Economic Surveys*, 37(4), pp. 1214–1254. Available at: <https://doi.org/10.1111/joes.12468>.

Yugay, A. *et al.* (2025) “Role of Well Integrity in Meeting Production Mandates: Prevention of Well Barrier Failures,” *SPE Annual Technical Conference and Exhibition*. SPE, p. D031S034R008. Available at: <https://onepetro.org/SPEATCE/proceedings-abstract/25ATCE/25ATCE/792023> (Accessed: March 24, 2026).

Zohaib, S.M. *et al.* (2024) “Zero trust vpn (zt-vpn): A systematic literature review and cybersecurity framework for hybrid and remote work,” *Information*, 15(11), p. 734.