

MSc Cybersecurity and Digital Forensics
ACCA7028, Data Security, Governance and Compliance

Data Security, Governance and Compliance

Applied Framework Design for FinSure Bank (FSB):
**An Integrated ISO 27001 · NIST CSF 2.0 · COBIT 2019 · ITIL 4 Security
Architecture**

Lecturer: Dr. Ayman Al Hajjar



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

TABLE OF CONTENTS

Abstract	3
1. Introduction.....	3
2. Review of Security Frameworks and Models	3
2.1 ISO/IEC 27001:2022 , Information Security Management System (ISMS).....	3
2.2 NIST Cybersecurity Framework 2.0 (2024).....	4
2.3 COBIT 2019 , IT Governance and Management	4
2.4 ITIL 4 , IT Service Management.....	4
2.5 Why an Integrated Approach is Required	5
3. Proposed Integrated Security Governance Architecture for FSB.....	5
3.1 Governance Layer , COBIT 2019	5
3.2 Policy and Compliance Layer , ISO 27001:2022.....	5
3.3 Risk Management Layer , NIST CSF 2.0	6
3.4 Technical Controls Layer	6
3.5 Service Delivery Layer , ITIL 4.....	6
3.6 Assumptions	7
4. Risk Management Strategy	7
5. Critical Analysis: Why Evolving Regulations and Standards Are Essential	8
5.1 The Threat Landscape Evolves Faster Than Static Standards.....	8
5.2 Regulatory Updates Reflect Demonstrated Harm	8
5.3 The Limits of Compliance: Standards as Floors, Not Ceilings	8
6. Conclusion.....	9
References	10

Abstract

This report uses the concepts and practices of data security, governance, and regulatory compliance to the case of FinSure Bank (FSB), a fast expanding digital-first financial services firm that uses nearly all of the cloud infrastructure in various jurisdictions. There is no coherent governance model, formal risk management approach, and systematic compliance controls at FSB at the moment, and it is under acute exposure to regulatory, operational, and reputational risk. Based on ISO/IEC 27001:2022, NIST Cybersecurity Framework 2.0 (2024), COBIT 2019, ITIL 4, PCI DSS v4.0, and the General Data Protection Regulation (GDPR), this report suggests an integrated, multi-layered security governance architecture based on the digital-first, multi-country, BYOD-enabled environment. The report argues that compliance is not a static destination but a continuous, risk-aware discipline.

1. Introduction

The financial services industry worldwide has been radically digitalized in the last decade, and cloud computing, mobile banking, and open APIs have become the cornerstones of service provision. Yet this change has exceeded governance maturity at most organisations, and has resulted in structural security gaps which adversaries, and regulators alike, have been taking advantage of with the global average cost of a data breach increasing to record highs of 4.88 million, up 10 percent year on year (IBM Cost of a Data Breach Report 2024).[\[11\]\[16\]](#)

This is the case with FinSure Bank (FSB). Since it operates in many countries, more than 90% of its infrastructure is hosted on the cloud, has a growing BYOD workforce, and lacks a single security governance framework, FSB is facing a combination of regulatory compliance (GDPR, FCA SYSC rules, PCI DSS), operational risk (insider threats, ransomware, mobile app fraud) and strategic risk (reputational damage, loss of banking licence). These risks cannot be identified, controlled, or reported to regulators systematically without a structured governance architecture in place.[\[15\]](#)

2. Review of Security Frameworks and Models

A security framework is a structured collection of policies, guidelines, and controls in which organisations manage information security risk.[\[9\]](#) In the case of FSB, four complementary frameworks are evaluated: ISO / IEC 27001: 2022 (information security management), NIST CSF 2.0 (cyber resilience based on risk), COBIT 2019 (IT governance), and ITIL 4 (A comparative summary is given in figure 1).

Framework	Type	Scope	Certifiable?	Key Strength for FSB	Standard/Body
ISO/IEC 27001:2022	Standard	Information Security Management (ISMS)	Yes (third-party audit)	Comprehensive 93-control Annex A; GDPR alignment	ISO/IEC
NIST CSF 2.0 (2024)	Framework	Risk-based cyber resilience	No (voluntary guidance)	6 Functions incl. Govern; cloud & supply chain	NIST (US Gov)
COBIT 2019	Framework	IT Governance & Management (EGIT)	Yes (ISACA CISA audit)	Aligns IT goals to business strategy	ISACA
ITIL 4	Framework	IT Service Management (ITSM)	Yes (training certs)	SLA management; service continuity	Axelos / PeopleCert
PCI DSS v4.0	Standard	Payment Card Data Security	Yes (QSA audit)	Mandatory for card payment processing	PCI SSC

Figure 1: Security framework comparison, ISO 27001:2022, NIST CSF 2.0, COBIT 2019, ITIL 4, and PCI DSS v4.0 evaluated for FSB.

2.1 ISO/IEC 27001:2022, Information Security Management System (IMS)

The ISO 27001:2022 is a global standard of setting up, executing, sustaining, and consistently enhancing an Information Security Management System (ISMS). In 2022, ISO 27001 has 11 new controls and reorganised the contents in the Annex A into four themes (Organisational, People, Physical, Technological) containing 93 controls in total, containing 93 controls in total.^{[1][9]} The ISO 27001 has however faced criticism of putting organisations at risk of playing compliance theatre, whereby they seek certification by documentation without actually minimising risk (Siponen and Willison, 2009). In the case of FSB this is a real issue: certification in 18 months would be a strong incentive to a checklist mindset rather than meaningful change in governance.

In the case of FSB, the ISO 27001 certification is directly beneficial in terms of regulation: the controls contained in its Annex A align well with GDPR Article 32 (appropriate technical and organisational measures) and FCA SYSC 13 (operational risk systems and controls). In particular, the controls A.6.7 (remote working), A.5.23 (information security of cloud services), and A.8.16 (monitoring activities) directly deal with BYOD and cloud risks of FSB.^{[1][6]}

2.2 NIST Cybersecurity Framework 2.0 (2024)

NIST CSF 2.0, released in February 2024, represents the most significant update to the framework since its inception. Its most notable addition is a sixth core function, GOVERN, which elevates cybersecurity risk management to a board-level, enterprise risk management responsibility alongside financial and reputational risks.^{[2][17]}

NIST CSF 2.0 is particularly appropriate for FSB because it is explicitly designed for cloud-dependent, multi-jurisdiction organisations and includes new guidance on supply chain security, third-party risk management, and BYOD scenarios.^[2] Approximately 81% of US-based financial institutions reported NIST CSF adoption in 2024, demonstrating its sector applicability.^[12] Nevertheless, voluntary and non-certifiable character of NIST CSF is a constraint to FSB in particular: FCA SYSC regulations require regulators to find demonstrable and auditable controls (which NIST alone cannot offer). That is why it is employed herein as an operational layer as opposed to the main compliance vehicle of FSB. Critically, NIST CSF 2.0 aligns with ISO/IEC 27001:2022 through a published crosswalk, enabling FSB to pursue ISO certification while using the NIST framework operationally.^[18]

2.3 COBIT 2019, IT Governance and Management

COBIT 2019 (Control Objectives for Information and Related Technologies) is developed by ISACA and provides a comprehensive framework for enterprise governance of information and technology (EGIT). Unlike ISO 27001 or NIST, which focus on security controls and risk management respectively, COBIT addresses governance at a strategic level: defining who makes IT decisions, how IT objectives align with business goals, and how performance is measured.^{[3][7]}

COBIT 2019 organises governance and management into five domains, EDM, APO, BAI, DSS, and MEA, containing over 40 governance objectives.^{[3][19]} For FSB, COBIT 2019 is essential for establishing board-level accountability for cybersecurity, defining IT risk appetite, managing third-party (vendor) risk through APO10, and aligning the security investment programme with business outcomes.^[7]

COBIT is widely described as a 'framework of frameworks'. With that being said, the scope of COBIT is also a practical constraint. It has more than 40 governance objectives, which cannot be realised without resources, and is not realistic in the current governance maturity of an organisation at FSB. Instead of wholesale adoption, a targeted one with EDM, APO10, and APO12 should be adopted.

2.4 ITIL 4, IT Service Management

ITIL 4 provides detailed best practices for delivering IT services efficiently and reliably. For FSB, ITIL 4 governs incident management (responding to security events and service outages), change management (controlling configuration changes that could introduce vulnerabilities), service level agreements (SLAs with cloud providers), and service continuity management (business continuity planning). [\[4\]](#) One of the most striking weaknesses is that ITIL 4 focuses on cybersecurity risk without a strategic perspective, i.e. unless COBIT and NIST are above it, ITIL may deliver operationally efficient but strategically vulnerable service delivery.

2.5 Why an Integrated Approach is Required

While each framework reviewed carries individual merit, each also carries inherent limitations that make sole reliance strategically inadequate for FSB's risk profile. The integrated architecture proposed in Section 3 maps each framework to its appropriate layer, creating a unified, defence-in-depth governance stack. [\[17\]](#)

3. Proposed Integrated Security Governance Architecture for FSB

The architecture presented below divides the security governance of FSB into six layers with each layer corresponding to the most suitable framework. This multi-layered model is based on the principles of defence in depth, so that failure at one layer will not affect the rest of the security posture.

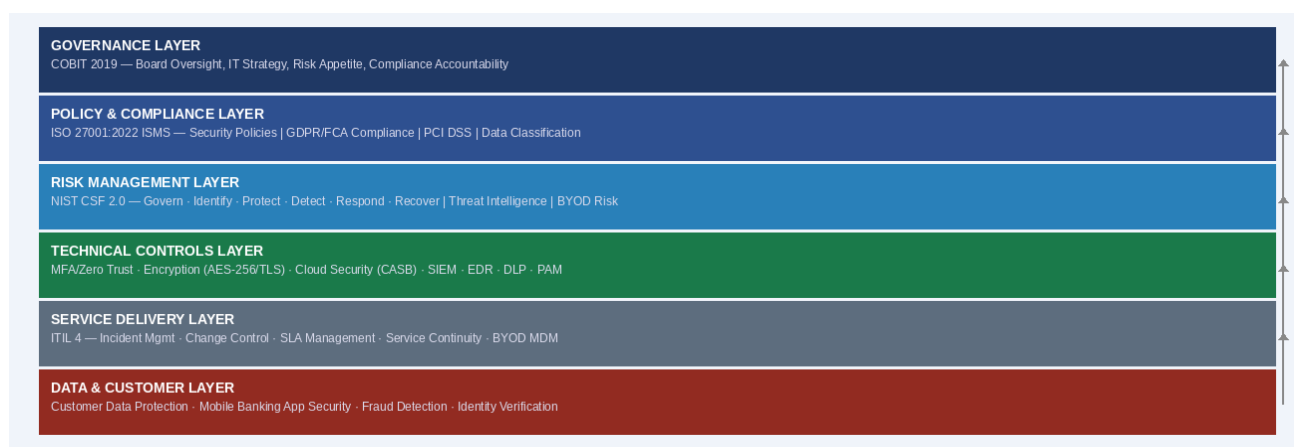


Figure 2: Proposed FSB integrated security governance architecture, six-layer defence-in-depth model.

3.1 Governance Layer, COBIT 2019

COBIT 2019 at its top defines the governance structure of FSB. The accountability of cybersecurity risk is assumed by the Board and CEO as part of enterprise risk management, with guidance on COBIT EDM domain (Evaluate, Direct and Monitor) [\[3\]](#) (a) establishing a Cybersecurity Steering Committee at board level; (b) defining the IT risk appetite and tolerance thresholds of FSB; (c) appointing a Chief Information Security Officer (CISO) with direct access to the board; (d) requiring quarterly. [\[7\]](#)

3.2 Policy and Compliance Layer, ISO 27001:2022

The second layer defines the formal security policy environment of FSB based on ISO/IEC 27001:2022. There are three policies that are significant to the operating model of FSB. First, a BYOD (Bring Your own Device) Security Policy, which aligns to ISO A.5.23 (information security to use cloud services), where contractual security requirements with all cloud providers are mandatory, CASB (Cloud Access Security Broker)

implementation, and annual cloud security audits are mandatory.^[1] Third, Data Classification and Handling Policy based on GDPR Article 5 (purpose limitation, data minimisation, storage limitation), which classifies FSB data by four levels Public, Internal, Confidential, and Highly Restricted.^[6]

The regulatory compliance is supported by ISO 27001 certification: the controls directly correspond to GDPR Article 32 (technical and organisational measures), PCI DSS v4.0 Requirements 3 and 8, and FCA SYSC 13 (operational risk).^{[9][13][15]}

3.3 Risk Management Layer, NIST CSF 2.0

The third layer operationalises FSB's risk management using NIST CSF 2.0's six core functions. Figure 3 maps each function to FSB-specific actions.^[2]

The GOVERN function, introduced in CSF 2.0, mandates that FSB have in place cybersecurity roles, risk tolerance, and enterprise-wide cybersecurity policies connected to the governance layer below, which is a foundational requirement of successful risk management, and FSB does not have it.^{[2][12]}

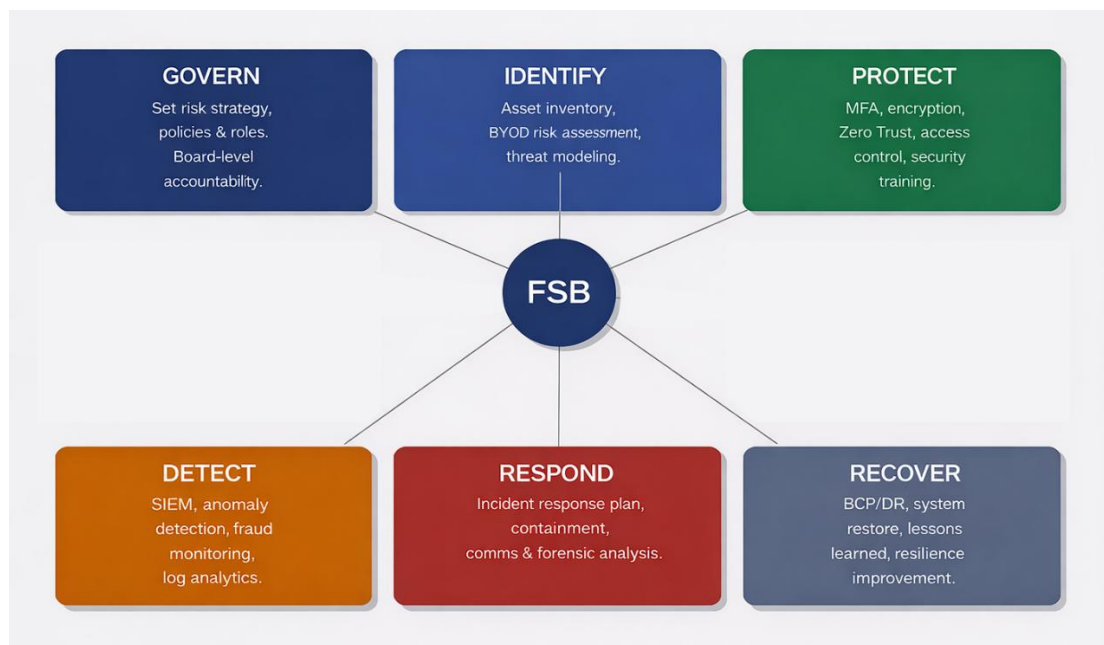


Figure 3: NIST CSF 2.0 six core functions applied to FSB, each function mapped to specific controls and responsibilities.

3.4 Technical Controls Layer

The FSB's technical controls layer has eight priority controls that build on the NIST PROTECT and DETECT functions. (1) for all employee, contractor, and customer accounts to protect against social engineering attacks.^{[2][1]} (2) through Microsoft Intune or a similar service, which makes sure that all BYOD devices follow the rules for compliance.^[1] (3) gives you control over and visibility into all cloud service use, even shadow IT.^[1] (4) preventing exfiltration of classified data via email, cloud storage, or removable media.^[1] (5) Privileged Access Management (PAM) for all admin accounts, with session recording and Just-In-Time access.^[2] (6) to detect anomalies in FSB's mobile banking application and open banking APIs.^[2] (7) monthly scans with authentication, critical patching within 72 hours, and annual penetration testing.^{[1][5]}

3.5 Service Delivery Layer, ITIL 4

The fifth layer regulates the operational delivery of security services with the help of ITIL 4. FSB should introduce: (a) Incident Management, documented security incident response plan (IRP) and defined escalation paths, recovery time objectives (RTO), and communication protocols; (b) Change Management, all

infrastructure changes should pass through a security review gate based on ITIL Change Advisory Board (CAB) process, and include evidence of ISO 27001 certification.[\[4\]\[6\]](#)

3.6 Assumptions

The proposed architecture is based on the following assumptions. (1) FSB can use at least 12-18 months to implement phased governance before it targets ISO 27001 certification. (2) FSB has or can hire a CISO who has direct access to the board (3) FSB processes payment card data and is therefore subject to PCI DSS regardless of card scheme.

4. Risk Management Strategy

The risk management process at FSB should be formalised based on an organised procedure in accordance with COBIT APO12, ISO 27001 Clause 6.1 (risk assessment), and NIST CSF 2.0 IDENTIFY.RA.[\[1\]\[2\]\[3\]](#) Figure 4 risk register identifies the seven highest-priority risks at FSB, such as likelihood, impact, key controls, and framework mapping.[\[16\]](#)

Risk	Likelihood	Impact	Key Control	Framework Mapping
BYOD Data Leakage	Very High	Critical	MDM, DLP, Zero Trust NAC	ISO 27001 A.6.7 / NIST PR.AC
Ransomware / Malware	High	Critical	EDR, SIEM, offline backups, BCP	NIST DE/RS / ISO A.12
Insider Threat	High	High	PAM, UEBA, least privilege, DLP	COBIT APO12 / ISO A.7
GDPR Non-Compliance	Medium	Critical	DPIA, DPO appointment, audit trails	GDPR Arts 5,25,32,37
Cloud Provider Failure	Medium	High	Multi-cloud BCP, SLA clauses, DR	ITIL4 SCMG / ISO A.17
3rd Party / Supply Chain	High	High	Vendor risk mgmt, contractual SLAs	ISO A.15 / COBIT APO10
Mobile App Fraud	High	Critical	MFA, biometric auth, fraud analytics	PCI DSS / NIST ID.RA

Figure 4: FSB top risk register, likelihood/impact assessment with control mapping and framework references.

BYOD data leakage is the most serious risk to FSB. The absence of MDM enforcement, and a BYOD policy, means that personal devices accessing corporate systems are an uncontrolled channel of data egress into the personal cloud storage (e.g., Google drive, iCloud) without any governance controls in place at FSB.[\[1\]\[2\]](#)

The second risk of importance is ransomware and malware. and ransomware attacks can do so completely, IBM's 2024 report confirms financial sector breaches carry disproportionate costs, and FSB currently lacks the SIEM, EDR, or tested incident response capability to contain one.[\[16\]](#) as FSB lacks the SIEM, EDR, or tested ability to react to intrusions. The controls, EDR, SIEM, offline backups, and verified Business Continuity Plan (BCP), are aligned to the NIST DETECT, RESPOND, and RECOVER functions.[\[2\]](#)

The non-compliance of GDPR is an existential regulatory risk to FSB due to its multi-country customer base. GDPR fines in 2024 totaled over €2.1 billion globally.[\[13\]](#) Under GDPR Article 37 (financial sector processors are generally obliged to have one), FSB must have one Data Protection Officer (DPO), make Data Protection Impact Assessments (DPIAs) on all processing operations that have high risk, and have retention and deletion policies.[\[6\]](#)

Supply chain and third-party risk is especially severe to FSB due to its over 90% reliance on clouds. COBIT APO10 (Manage Vendors and Service Providers) and ISO 27001 Annex A.5.19-A.5.22 (supplier relationships)

set the rules for vendor risk management. They say that security due diligence, contractual obligations, and constant monitoring of important third parties are all necessary.[\[1\]\[3\]](#)

5. Critical Analysis: Why Evolving Regulations and Standards Are Essential

The recurrent update of standards and regulations is a contentious issue in information security governance, and is not only essential but also insufficient on its own,[\[10\]](#) and organizations that have compliance as their goal and not an ongoing discipline are systematically vulnerable.[\[8\]](#)

5.1 The Threat Landscape Evolves Faster Than Static Standards

The risk landscape that financial institutions will encounter in 2025 is not much similar to the one in 2015. The appearance of generative AI-enabled phishing, ransomware-as-a-service (RaaS) ecosystems (as seen in the 2025 M&S/Co-op attacks), API-first architecture, and threat to current cryptographic standards all are threat vectors that were not present, or not operationally important, when earlier versions of the framework were published.[\[11\]\[17\]](#)

The 11 new controls of ISO 27001:2022 (including A.5.23 cloud services, A.5.7 threat intelligence and A.8.12 data leakage prevention) are indicative of the same dynamism: the 2013 version had no formally required cloud security controls, which is significant at a time when cloud usage is in its infancy.[\[9\]](#)

5.2 Regulatory Updates Reflect Demonstrated Harm

Regulatory evolution does not occur randomly, it is normally triggered by proven harms. In response to a twenty-year history of evidence that inadequate data protection harmed individuals, the GDPR supplanted the Data Protection Directive of 1995 with multi-factor authentication requirements on all access to cardholder data environments,[\[6\]](#) PCI DSS v4.0 (2022) established multi-factor authentication mandates for all access to cardholder data environments, subsequent to years of card-present fraud that 'compliant' organizations under PCI DSS v3.x continued to experience, highlighting the inadequacy of the previous standard.[\[5\]](#)

In the case of FSB, this has a direct implication in that compliance with the existing version of a standard is a floor, not a ceiling. FSB has to observe regulatory changes in every jurisdiction in which it conducts its business, such as DORA in the context of EU business, FCA operational resilience requirements in the UK, and the development of national cybersecurity laws, and should consider compliance gap analysis as an ongoing, quarterly process rather than an annual certification exercise.[\[15\]\[13\]](#)

5.3 The Limits of Compliance: Standards as Floors, Not Ceilings

Research on the management of information security standards has continuously provided that the risk of compliance theatre exists where organisations become certified to a specific standard without actually making any substantive effort to reduce the risk of information security.[\[10\]](#) Siponen and Willison (2009) contended that standards such as ISO 27001 may devolve into bureaucratic checklists if organizations prioritize documentation over authentic risk mitigation.[\[10\]](#)

Such criticism does not nullify standards, it strengthens the necessity of standards to develop and organisations to go beyond them. The controls required by the ISO 27001, NIST CSF 2.0, COBIT 2019, and ITIL 4 are not required by certification, but are necessary based on the risk register in Section 4 and should be implemented by FSB now, not when they become mandatory.[\[8\]\[17\]](#) A growing governance program at FSB should aim to

fill not only current compliance gaps but also those that are expected to arise in the future. It should do this by using operational resilience practices that are in line with DORA now, instead of waiting for them to become required.[\[14\]](#)

This is the very distinction that von Solms and Van Niekerk (2013) made between information security (defending data assets) and cyber security (defending cyberspace and the individuals within it), claiming that the evolution of controls is not the sole factor that will help the controls work.[\[11\]](#) but rather the evolution of culture and governance.

6. Conclusion

The case of FinSure Bank is a textbook example of why thorough security governance is urgent in the digital-first financial services. Its cloud-related dependency, BYOD proliferation, multi-jurisdiction customer data, and a lack of a single governance model make it vulnerable to risk with a risk profile that cannot be sufficiently mitigated by a single security control measure.

The integrated architecture suggested in the current report, The integrated five-layer architecture proposed in this report, offers FSB a coherent, defence-in-depth architecture which is auditable, certifiable, and operationally deployable.

The critical analysis in Section 5 shows that changing rules and standards are not a burden on businesses; they are responses based on evidence to failures that have been shown to happen. FSB must not view ISO 27001 certification or GDPR compliance as final accomplishments; it must institutionalize continuous improvement, quarterly risk assessments, and proactive regulatory oversight as essential governance practices.

The fact that COBIT 2019, ISO 27001:2022, NIST CSF 2.0, and ITIL 4 converge into a single architecture provides FSB with the governance vocabulary, risk management discipline, technical control rigour, and service delivery maturity to defend its customers, meet its regulators, and establish the digital trust on which its competitive position ultimately relies upon.

References

- [1] ISO/IEC, *ISO/IEC 27001:2022, Information Security Management Systems, Requirements*. [Online]. Available: <https://www.iso.org/standard/27001>
- [2] NIST, *NIST Cybersecurity Framework 2.0, National Institute of Standards and Technology, Feb. 2024*. [Online]. Available: <https://www.nist.gov/cyberframework>
- [3] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*. ISACA, 2019. [Online]. Available: <https://www.isaca.org/resources/cobit>
- [4] Axelos, *ITIL 4: Create Deliver and Support. The Stationery Office, 2020*. [Online]. Available: <https://www.axelos.com/certifications/itil-service-management>
- [5] PCI SSC, *PCI DSS v4.0, Payment Card Industry Data Security Standard*. PCI Security Standards Council, 2022. [Online]. Available: https://www.pcisecuritystandards.org/document_library/
- [6] European Parliament, *Regulation (EU) 2016/679 (GDPR). Official Journal of the European Union, 2016*. [Online]. Available: <https://gdpr-info.eu/>
- [7] Anoruo C., *Employing COBIT 2019 for Enterprise Governance Strategy*. *ISACA Journal*, 2019. [Online]. Available: <https://www.isaca.org/resources/news-and-trends/industry-news/2019/employing-cobit-2019-for-enterprise-governance-strategy>
- [8] Shackelford S.J. et al., *Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework*. *Texas International Law Journal*, 50(2), 2015. [Online]. Available: <https://doi.org/10.2139/ssrn.2446900>
- [9] Disterer G., *ISO/IEC 27000, 27001 and 27002 for Information Security Management*. *Journal of Information Security*, 4(2), pp.92-100, 2013. [Online]. Available: <https://doi.org/10.4236/jis.2013.42011>
- [10] Siponen M. & Willison R., *Information security management standards: Problems and solutions*. *Information & Management*, 46(5), pp.267-270, 2009. [Online]. Available: <https://doi.org/10.1016/j.im.2008.12.007>
- [11] Von Solms R. & Van Niekerk J., *From information security to cyber security*. *Computers & Security*, 38, pp.97-102, 2013. [Online]. Available: <https://doi.org/10.1016/j.cose.2013.04.004>
- [12] ACSMI, *NIST Cybersecurity Framework Adoption Report 2025*. ACSMI, Jul. 2025. [Online]. Available: <https://acsmi.org/blogs/nist-cybersecurity-framework-adoption-original-data-amp-industry-analysis-2025>
- [13] CyberDefenceInfo, *Cybersecurity Compliance in 2025: GDPR, ISO 27001, and NIST Standards*. *CyberDefenceInfo*, Nov. 2025. [Online]. Available: <https://cyberdefenceinfo.com/cybersecurity-compliance-in-2025-a-complete-guide-to-gdpr-iso-27001-and-nist-standards-for-businesses/>
- [14] Invensis, *Top 6 Cybersecurity Standards Every Business Needs*. Invensis, 2025. [Online]. Available: <https://www.invensis.net/blog/key-cybersecurity-standards>
- [15] FCA, *FCA Handbook, Systems and Controls (SYSC)*. Financial Conduct Authority, UK, 2024. [Online]. Available: <https://www.handbook.fca.org.uk/handbook/SYSC/>
- [16] IBM, *Cost of a Data Breach Report 2024*. IBM Security, 2024. [Online]. Available: <https://www.ibm.com/reports/data-breach>
- [17] Bitsight, *7 Cybersecurity Frameworks to Reduce Cyber Risk in 2025*. Bitsight, Mar. 2025. [Online]. Available: <https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk>
- [18] GRC Solutions, *ISO 27001 and the NIST CSF (Cybersecurity Framework)*. *GRC Solutions / IT Governance*, Nov. 2025. [Online]. Available: <https://www.itgovernanceusa.com/iso27001-and-nist>
- [19] ISACA, *COBIT 2019 Key Principles*. *ManageEngine / ISACA*, 2023. [Online]. Available: <https://www.manageengine.com/products/service-desk/itsm/what-is-cobit-2019.html>
- [20] Darmaningrat E. et al., *Risks Assessment of Information Technology Processes Based on COBIT 5 Framework*. *Procedia Computer Science*, 124, pp.569-576, 2017. [Online]. Available: <https://doi.org/10.1016/j.procs.2017.12.191>