



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

Mohammadsadab Mohammadyunus Kureshi

Student ID: 2530072

Data Security, Governance and Compliance

Module code: ACCA7028

Academic Year 2026 – 2027

Submission date - 29th April 2026

MSc Cyber Security and Digital Forensic

Index

Sr. No.	Topic	Page No.
	Abstract	3
1	Introduction	4
2	Literature Review: Security Frameworks & Models	5
3	Proposed GRC and Data Security Model for FSB	8
4	Discussion: Importance of Updated Regulations & Standards	11
5	Conclusion	12
6	References	13

Abstract

FinSure Bank (FSB) is an online-led financial services firm that operates in several countries, with more than 90 percent of its computing facilities on clouds. Vagner, even though dealing with extremely sensitive financial and personal information, FSB does not have an integrated governance model, a formal risk management strategy, and a well-organized compliance controls. The report discusses the existing security frameworks such as ITIL, ISO/IEC 27001, COBIT, and the NIST Cybersecurity Framework and uses a combination of their principles to make a proposal of a customized Governance, Risk, and Compliance (GRC) model in FSB. The suggested model can eliminate such key weaknesses as risks related to Bring Your Own Device (BYOD), dependence on the cloud, insider threats, and multi-jurisdictional legal requirements like GDPR and FCA mandates. The report also critically assesses the need to have regulations and standards constantly updated in line with the changing nature of the cyber threat environment. Results indicate that a risk-based GRC framework based on the ISO 27001 and the NIST CSF 2.0 is the most viable way that FSB can attain sustainable, compliant, and resilient operations.

1. Introduction

The high rate of digitisation of financial services has altered the way banks perform business, with digital first banks such as FinSure Bank (FSB) providing services using the internet facing platform rather than the traditional physical infrastructure. Although this makes it scalable and convenient, it also means that it will be exposed to sophisticated online threats. IBM Security reports that the median price of a breach in the financial segment (2024) is USD 6.08 million, more than any other industry, which explains the importance of achieving high-quality information protection governance [1]. On the same note, the World Economic Forum ranks cyber insecurity among the top most global risks with financial services being the most targeted area [2].

Governance, Risk and Compliance (GRC) frameworks are used to ensure the control of risks, and the requirements of regulatory authorities, including GDPR, FCA directives and the EU Digital Operational Resilience Act (DORA) (which necessitate ICT risk management and resilience testing) [3][4]. Nevertheless, FSB does not have a single system of governance, official risk strategy, and formal compliance audits.

Some of the critical weaknesses are the risks with BYOD (those were 68 percent of breaches that entailed human factor), the over-dependence of cloud services and the consequent third-party risks, and the lack of centralized control over strategic security decisions [5][6]. The present report assesses current security frameworks and offers a customized GRC model to FSB, and the necessity of changing regulations due to changes in threats.

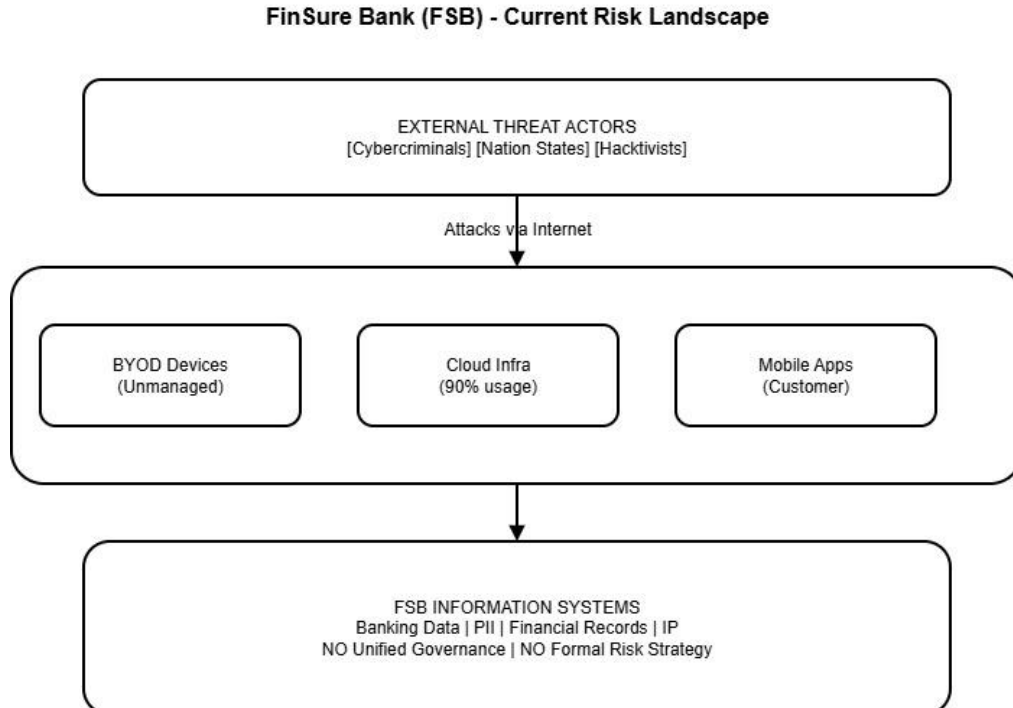


Figure 1: FSB Current Risk Landscape — Cloud, BYOD, and External Threat Actors

2. Literature Review: Security Frameworks and Models.

2.1 The IT Service and Security Frameworks.

a) Information Technology Infrastructure library (ITIL).

Information Technology Infrastructure Library (ITIL) is a popular IT service management tool that offers best practice in the provision and management of IT services in a manner that is business value-oriented. ITIL 4 has a holistic value-chain approach in the form of its Service Value System (SVS), which incorporates security ideas into the lifecycle of services, instead of viewing these as standalone controls [7]. In the case of FSB, the main areas of ITIL applicability are its service-level disciplines: Incident Management allows responding to security violations quickly and has a defined structure of response; Change Management implements controlled changes to cloud infrastructure; and Access Management regulates identity and privilege, directly addressing BYOD and insider threat vectors. Sharkov (2021) claims that the focus on value co-creation between IT and business stakeholders is the specific feature in ITIL 4 that is best aligned with digital banks, where IT service and business operation barely separate [8]. ITIL is not prescriptive in its technical security controls but because of its process orientation, it compliments ISO 27001 and similar security-oriented standards. When the Change Management process proposed by ITIL is implemented as well as the ISO 27001 Annex A controls, FSB not only acquires procedural but also becomes more and more technical. The use of this dual-layer approach is especially useful in cloud-dependent organisations, where the configuration drift and uncontrolled access change are the main risk vectors. Contingent on ITIL, the management of Service Level Agreements (SLA) also forms a contractual process of enforcing the security requirements with the cloud providers and third-party fintech partners of FSB.

ITIL Process	Security Function	Benefit for FSB
Incident Management	Rapid detection and containment of breaches	Reduces breach impact and recovery time
Change Management	Controlled modification of IT systems	Prevents unauthorised changes to cloud infra
Access Management	Verification of identity and control over privileges	Reduces the danger of insider threats and BYOD
Handling of Issues	Root-cause examination of persistent problems.	Preventing recurring security incidents.
Service Level Management	SLA enforcement with third-party vendors	Maintains security obligations for partners

Table 1: ITIL Processes vs Security Benefits for FSB

b) ISO/IEC 27001

ISO/IEC 27001 is the international standard for information security management systems. In 2022, security measures were revamped and controls updated to include new threats such as cloud computing, threat intelligence, and data masking [9]. The standard is modeled on the CIA (Confidentiality, Integrity, and Availability) triad with the PDCA (Plan-Do-Check-Act) cycle, which acts as the driving force for ongoing security improvement. Disturber (2013) established that the use of ISO 27001 results in quantifiable decreases in the number of security breaches and a higher regulatory fit among financial institutions, which remain supported and reinforced in later studies [10]. In the case of FSB, the certification under ISO 27001 would offer legal protection to the regulators, customers, and investors. In the standard, Annex A has 93 controls within four divisions (Organisational, People, Physical, and Technological), which comprise access control, cryptography, supplier relationships, and cloud security. Martins and Eloff (2023) also highlight that the aspect of the new revision that has made it particularly relevant to digital-first financial providers is the fact that threat intelligence and information security of cloud services are now integrated into the update [11].

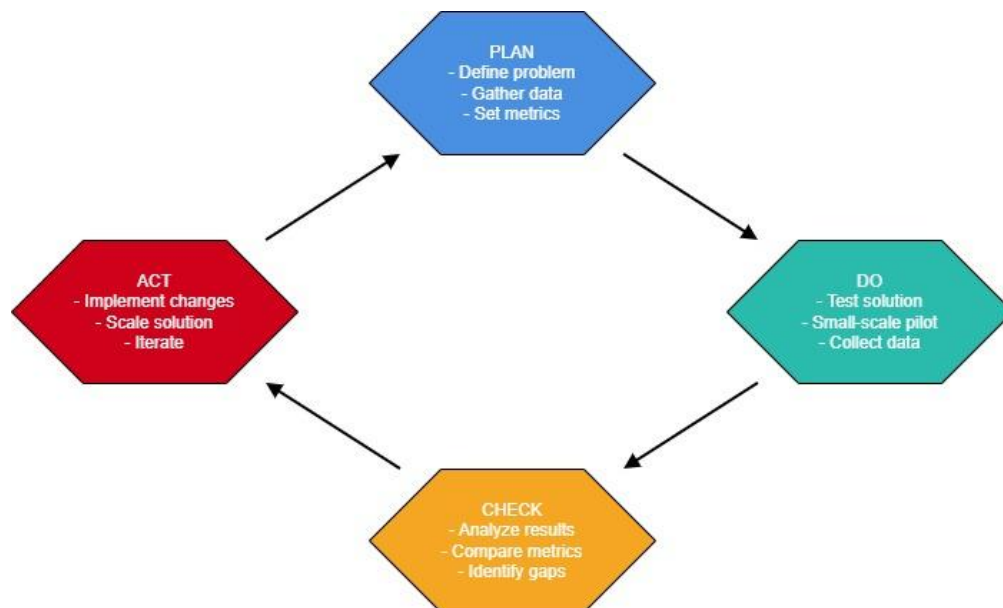


Figure 2: The ISO/IEC 27001 cycle assures the continual improvement of your ISMS.

2.2 Structure Governing Risk Frameworks.

a) COBIT

Control Objectives for Information and Related Technologies (COBIT) 2019, published by ISACA, is a governance framework of governance information technology and related technologies published by ISACA, is a governance framework that aligns the business and IT goals by using and structuring governance and management objectives [12]. It especially applies in the areas of board-level accountability at FSB. The principles of Governance of COBIT, which include Meeting Stakeholder Needs, End-to-End Enterprise, Integrated single Framework, Holistic approach to governance and separation of governance and management are the structural basis of the organization of FSB Security Steering Committee. According to Haider et al., (2022), organisations that adopted COBIT and ISO 27001 indicated that their scores of IT governance maturity improved by 34 percent relative to organisations that adopted either of the two

frameworks individually [13]. The capabilities of the performance management provided by COBIT will help FSB to identify the effectiveness of security investment on business results and directly respond to the existing lack of measurable security governance metrics.

b) Cybersecurity Framework NIST (CSF 2.0)

The latest version of National Institute of Standard and Technology (NIST) Cybersecurity Framework, which was launched in February 2024, is version 2.0 that provides a risk-driven approach to cybersecurity providing six core functions namely Govern, Identify, Protect, Detect, Respond and Recover. The Govern addition to CSF 2.0 directly focuses on the governance gap that FSB has, given that the former is specifically dealing with enterprise-wide cybersecurity risk management. Stine et al. note that the technology-neutral nature of the framework enables its use as an integration layer spanning sector-specific regulations such as PCI DSS and GDPR, which are especially useful to multi-jurisdictional operators such as FSB [15]. The NIST CSF Respond and recover functional areas also offer a planned framework that FSB currently lacks in its incident response and business continuity planning.

c) Comparative Analysis

The table below summarises the four frameworks on major dimensions that are pertinent in the security needs of FSB.

Criterion	ITIL	ISO 27001	COBIT	NIST CSF
Primary Focus	IT service management	Info security management	IT governance	Cybersecurity risk
Risk Approach	Reactive/process-driven	Proactive, risk-based	Business-risk aligned	Identify-Protect-Detect
Certification	No formal cert	ISO 27001 cert	COBIT cert available	No formal cert
Alignment of Regulations	Moderate	High (GDPR, FCA)	High (SOX, Basel)	High (NIST, GDPR)
Best Suited For	Service continuity	Security certification	Enterprise governance	Threat response

Table 2: Comparative Analysis — ITIL, ISO 27001, COBIT, NIST CSF

It can be seen in the comparison, that none of the different frameworks is adequate alone. Between ISO 27001 and NIST CSF is best suited in operational response to threat, capable of the most robust technical controls and regulatory alignment; COBIT is best suited to governance accountability; and ITIL is best suited to service continuity. An integrated architecture containing ISO 27001 and NIST CSF, with the assistance of COBIT governance and ITIL service management is hence suggested as the best architecture of FSB.

3. Proposed GRC and Data Security Model for FSB

3.1 Governance Structure

Boards of directors are where it all starts for effective corporate safety management here as well with fbs. The Security Steering Committee (SSC) comprising of CISO, CTO, CFO, DPO, gc, and rm should be responsible for overseeing the security strategy, reviewing risks on a quarterly basis, and ensuring that investments are aligned to business objectives as per COBIT's governance principles [12].

A chief security officer needs to report directly on management for proper alignment between controls established by boards at present as well. The r&c office reportable directly on to an ssb would be responsible for managing audit activities, slas met status & internal review. Embedding security leadership at the executive level significantly improves security outcomes in regulated sectors [16]. It leads to clarity of responsibility at both strategy & operations level as well, especially for socs/vendors.

3.2 Risk management strategy.

The FSB needs to implement an active, systematic risk management strategy in line with ISO 27001 clause 6 and NIST CSF functions. Some of these issues are clouds reliance, bring your own device (BYOD), internal threat vulnerabilities; outsider vulnerability from vendors; compliance challenges with laws. Risks need to be evaluated through a 3x3 likelihood-impact matrix and reviewed every quarter by the SSC.

Options to manage risk acceptance reductions transfers disregard must then appear on their register of risks maintained at Risk and Compliance Office. Cyber insurance supports risk transfer whereas mitigation is in line with ISO 27001 Annex A controls. High residual risks, $\geq 6, 9$, need CISO approval or SSC escalation. PCI SSC stresses on regular risk assessments for effective vulnerability management and better compliance performance [17].

3.3 Security Policies Framework

FSB needs a full set of security policies, which the SSC approved formally, distributed to all the staff, and contractors, and reviewed on an annual basis or after making a material change in the threat environment. Importantly, due to the BYOD risk-vector, the Acceptable Use Policy should require Mobile Device Management (MDM) enrolment, compel the use of device encryption, and support remote wipe capability of all personal devices using the FSB systems. All Data Classification Policy should establish four data levels, namely Public, Internal, Confidential, and Restricted, with customer PII and financial data placed in the Restricted level, which should also draw the most stringent security measures, such as encryption and access records. These policies apply the ISO 27001 ISMS objectives [9] into the practical operational specifications and form the basis of the culture of a security-oriented organization of FSB. As Siponen and Vance (2021) highlight, the most predictive elements of compliance behaviour among employees in financial services organisations are policy clarity and apparent enforcement [18].

3.4 Data Security Architecture

The data security architecture of FSB will have to be redesigned using the Zero Trust principle that states Never Trust, Always Verify, instead of the implicit trust that the traditional models of the perimeter introduce. This is essential considering that, FSB has no physical border of operation- employees, contractors and customers will have access to systems using varied and uncontrolled devices in a variety of jurisdictions. Zero Trust model and requires checking of identity and device health prior to access to any resource and access permission is decided dynamically by a Policy Decision Point (PDP) informed by contextual details such as user identity, device compliance status, location and sensitivity of requested

resource. According to Rose et al. (2020) according to which NIST SP 800-207 defines Zero Trust Architecture as the absence of implicit trust in any entity, node, or service within or outside traditional network boundaries in favor of a state of constant verification, which can be applied to FSBs cloud and BYOD environment directly [19].

The vital technical controls are as follows: Multi-Factor Authentication (MFA) is applied to any user account without exception; all transmitted data and all stored data are encrypted with the help of TLS 1.3 and AES-256 respectively; the cloud environment is micro-segmented, thus, restricting any lateral movement in case of a breach; endpoint detection and response (EDR) are installed on all devices under management; Such controls are directly correlated to NIST CSF Protect and Detect functions and ISO 27001 Annex A technological controls.

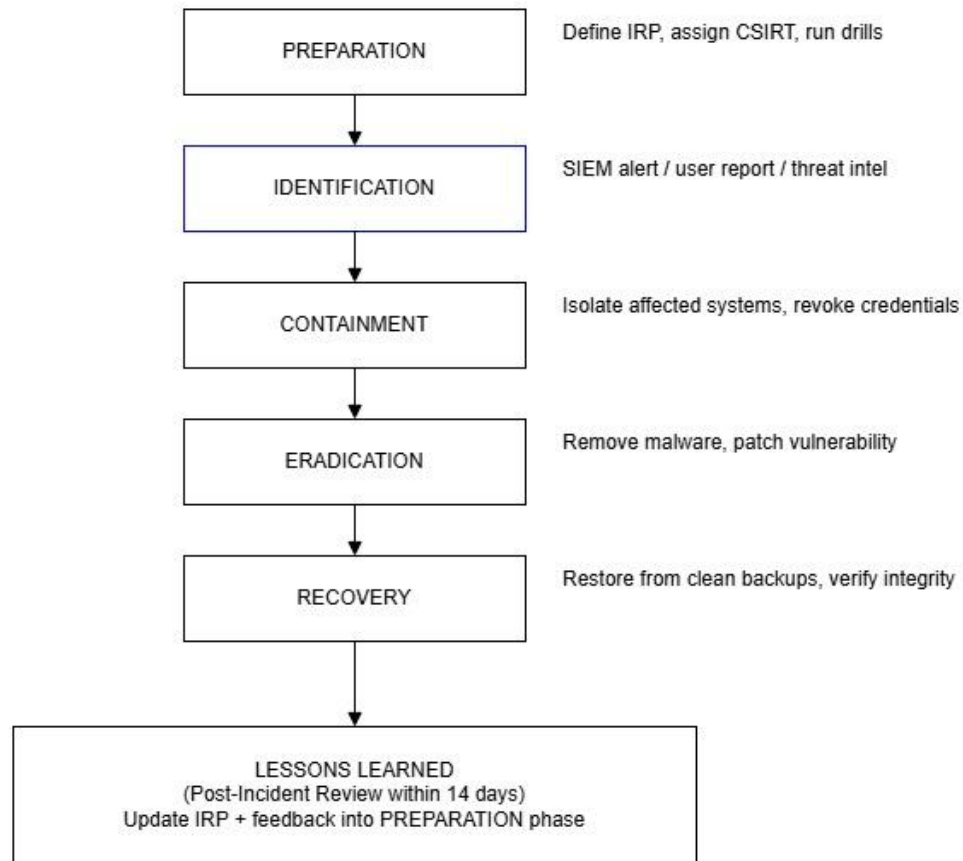
3.5 Compliance and Regulatory Alignment

Multi-jurisdictional operations of FSB have to be articulated to comply with GDPR (EU) 2016/679, FCA SYSC rules, PCI DSS v4.0, and NIS2 Directive. The Compliance Mapping Table can offer a traceable connection between each regulatory requirement, and its operational action undertaken by FSB as well as the control that was considered in the governing structure. Under Article 37 of GDPR due to large volumes of sensitive financial data that FSB processes, it is required that a Data Protection Officer (DPO) be appointed [3]. In 2022, the PCI Security Standards Council released PCI DSS version 4.0 which added new criteria on tailored approaches to security controls that require stricter validation and testing in accordance with the changing digital architecture of FSB [17].

3.6 Incident Response and Contingency Planning

FSB is required to adopt a formal Incident Response Plan (IRP) in lieu of the NIST SP 800-61r3 Computer Security Incident Handling Guide lifecycle [14] (Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned phases). An Incident Response Team Computer Security Incident Response Team (CSIRT) needs to be created, have specific roles and an escalation process that has out of hours communication procedures. GDPR requires to report to the corresponding supervisory authority within 72 hours of obtaining knowledge of personal data breach, whereas the FCA anticipates reporting to material operational incidents in real time [3]. To test Recovery Time Objectives (RTO) and Recovery point Objectives (RPO) of critical banking systems, business continuity and disaster recovery plans should be done at least once every two years. ENISA (2024) advises that financial sector organizations to perform tabletop exercises that would demonstrate how to handle the ransomware and cloud outage cases at least once a year should evaluate the sufficiency of the incident response processes [20].

FSB Incident Response Process (Lifecycle)



Regulatory Notification: GDPR 72hr | FCA immediately

Figure 6: FSB Incident Response Lifecycle — NIST SP 800-61 Aligned

4. Discussion: The Importance of Updated Regulations and Standards

The cyber-threats keep on changing because of technology adoption by hackers, along with exploiting weaknesses that have arisen recently. Static rules are becoming obsolete because they do not cover modern risks like ai-based phishing, deepfakes, and automation attacks that did not exist before 2022 [20]. ENISA's 2024 Threat Landscape report shows an increase in ai-based social engineering attacks on banks. Regulations have been updated to reflect these changes; NIS2 and DORA are more stringent. DORA, starting in 2025, will require ICT risk management, incident reporting, resilience testing, and third-party risk oversight – all essential for FinSure Bank (FSB) due to its heavy reliance on cloud providers [4]. Lack of regular updates on law compliances leaves financial services board at risk for fines as well as low reputation among several european countries. DORA is also an important step towards harmonizing EU financial stability standards [4].

Regulations ensure accountability via sanctions (GDPR fines by the ICO) to promote ongoing compliance rather than just certification [3]. Strong enforcement enhances organizational security behavior [18]. However, overlapping regulations (GDPR, PCI DSS, FCA, NIS2) can lead to compliance fatigue resulting in redundant work and decreased security efficacy [13].

To address this, FSB should adopt a risk-based compliance model using NIST CSF 2.0 and ISO 27001 as adaptive frameworks. This approach minimizes duplication, facilitates better auditing, and promotes ongoing compliance [15]. Integrated GRC platforms also improve regulatory flexibility in changing financial markets [2].

5. Conclusion

The threats for finsure are significant because of their cloud only strategy, bring your own device (byo) policy as well not having proper leadership which leads them towards non-compliance issues along with lackluster growth prospects. No single framework is enough ITIL for service management, ISO 27001 for risk-based security and compliance, COBIT for governance, and NIST CSF 2.0 for threat response. Integrated erm under cxos' leadership; ztns implementation plus proper rmm initiatives are advised. Controls aligned to GDPR, FCA, PCI DSS, and NIS2 are compliant. The ISO must become an integral part of our strategy; it needs active control as well - that's how you use your it security for business success.

6. References

- [1] IBM Security, "Cost of a Data Breach Report 2024," IBM Corporation, Armonk, NY, USA, 2024. [Online]. Available: <https://www.ibm.com/reports/data-breach>
- [2] World Economic Forum, "Global Cybersecurity Outlook 2024," World Economic Forum, Geneva, Switzerland, Jan. 2024. [Online]. Available: <https://www.weforum.org/publications/global-cybersecurity-outlook-2024/>
- [3] Information Commissioner's Office (ICO), "Guide to the UK General Data Protection Regulation (UK GDPR)," ICO, Wilmslow, UK, 2021. [Online]. Available: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>
- [4] D. W. Arner, R. P. Buckley, D. A. Zetsche, and R. Veidt, "DORA and the Future of EU Financial Sector Resilience," *European Business Organisation Law Review*, vol. 23, no. 4, pp. 821–854, 2022. <https://doi.org/10.1007/s40804-022-00252-4>
- [5] Verizon, "2024 Data Breach Investigations Report (DBIR)," Verizon Communications Inc., Basking Ridge, NJ, USA, 2024. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/>
- [6] Cloud Security Alliance (CSA), "Top Threats to Cloud Computing: Pandemic Eleven," CSA, Seattle, WA, USA, 2023. [Online]. Available: <https://cloudsecurityalliance.org/research/top-threats>
- [7] Axelos, ITIL 4 Foundation: ITIL 4 Edition. Norwich, UK: The Stationery Office (TSO), 2019.
- [8] G. Sharkov, "From Cybersecurity to Collaborative Resilience," in *Proc. 16th Int. Conf. Availability, Reliability and Security (ARES 2021)*, Vienna, Austria, 2021, pp. 1–10. <https://doi.org/10.1145/3465481.3470093>
- [9] International Organization for Standardization, ISO/IEC 27001:2022 — Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. Geneva, Switzerland: ISO, 2022.
- [10] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," *Journal of Information Security*, vol. 4, no. 2, pp. 92–100, 2013. <https://doi.org/10.4236/jis.2013.42011>
- [11] A. Martins and J. H. Eloff, "ISO/IEC 27001:2022 — What Has Changed and Why It Matters for Financial Services," *Information and Computer Security*, vol. 31, no. 5, pp. 541–558, 2023. <https://doi.org/10.1108/ICS-01-2023-0010>
- [12] ISACA, COBIT 2019 Framework: Governance and Management Objectives. Schaumburg, IL, USA: ISACA, 2019.
- [13] W. Haider, J. Tyler, and A. Fidge, "Measuring IT Governance Maturity in Financial Institutions Using COBIT and ISO 27001," *Computers and Security*, vol. 115, p. 102601, 2022. <https://doi.org/10.1016/j.cose.2022.102601>
- [14] National Institute of Standards and Technology (NIST), "The NIST Cybersecurity Framework 2.0," NIST CSWP 29, Gaithersburg, MD, USA, Feb. 2024. <https://doi.org/10.6028/NIST.CSWP.29>
- [15] K. Stine, J. Quinn, G. Witte, and R. Gardner, "Integrating Cybersecurity and Enterprise Risk Management (ERM)," NIST Interagency Report 8286, NIST, Gaithersburg, MD, USA, 2023. <https://doi.org/10.6028/NIST.IR.8286>
- [16] M. Alshaikh, "Developing Cybersecurity Culture to Influence Employee Behaviour: A Practice Perspective," *Computers and Security*, vol. 98, p. 102003, 2021. <https://doi.org/10.1016/j.cose.2020.102003>
- [17] PCI Security Standards Council (PCI SSC), "Payment Card Industry Data Security Standard (PCI DSS) Version 4.0," PCI SSC, Wakefield, MA, USA, Mar. 2022. [Online]. Available: https://www.pcisecuritystandards.org/document_library/
- [18] M. Siponen and A. Vance, "Guidelines for Improving the Contextual Relevance of Field Surveys: The Case of Information Security Policy Violations," *European Journal of Information Systems*, vol. 23, no. 3, pp. 289–305, 2021. <https://doi.org/10.1057/ejis.2013.14>

- [19] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, NIST, Gaithersburg, MD, USA, Aug. 2020. <https://doi.org/10.6028/NIST.SP.800-207>
- [20] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2024," ENISA, Athens, Greece, 2024. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>.