

## **FinSure Bank (FSB): Integrated Security, Governance and Compliance Design**

|                     |                                                                                                          |
|---------------------|----------------------------------------------------------------------------------------------------------|
| <b>Module</b>       | ACCA7028 Data Security, Governance and Compliance                                                        |
| <b>Assessment</b>   | Apply the principles and practices of data security, governance and compliance based on the FSB scenario |
| <b>Referencing</b>  | IEEE                                                                                                     |
| <b>Student name</b> | Zannatul Mawya Priya                                                                                     |
| <b>Student ID</b>   | 2527766                                                                                                  |

## Abstract

FinSure Bank (FSB) has a high-risk digital model: the majority of infrastructure is hosted, a high volume of sensitive financial and personal data is processed at scale, and the business desires employees, contractors and partners to use their own devices. This report contends that FSB should not stick to a single framework. A more robust version is a stratified model whereby COBIT 2019 offers governance responsibility, ISO/IEC 27001:2022 offers the ISMS, NIST CSF 2.0 offers risk management, ITIL 4 offers secure service operations and Zero Trust Architecture offers dynamic access control to BYOD, mobile and cloud environments. The suggested design combines board supervision, identity-based access, posture of the device, classifying data, assuring suppliers, reporting incidents, disaster recovery, and GDPR/DORA processes. New rules and standards are approached as a necessity since threats, cloud dependencies and legal expectations evolve at a higher rate than the fixed control baselines.

**Table Of Contents**

**Abstract..... 2**

**1. Introduction..... 4**

**2. Review of relevant frameworks and models ..... 5**

**3. Integrated design for FSB ..... 7**

**4. Why updated regulations and standards remain good practice ..... 16**

**Conclusion..... 16**

## 1. Introduction

The situation in the FinSure Bank is a common digital-banking security challenge: the growth of the business has been outpaced by security controls. FSB relies primarily on externally hosted, cloud-based services, serves customers with mobile apps and is straining to enable bring-your-own-device (BYOD) to its employees, contractors and third parties. In such an environment, perimeter-based security is ineffective since trust now depends on users, devices, APIs, suppliers and cloud workloads rather than office location. It is aggravated by the fact that there is no single model of governance, formulated risk management strategy and structured process of compliance audit. The current body of information security governance literature has demonstrated that divided responsibility is a failure in control in itself since policies, ownership and oversight of risks become inconsistent [1]. This report initially examines pertinent frameworks and then comes up with an integrated operating model of FSB. It also questions the rationale of why constantly revised regulations and standards continue to be good practice of a digital financial institution.

## 2. Review of relevant frameworks and models

No single framework fully meets FSB's needs. ITIL 4 converts policy into live service practices including incident management, change enablement, service continuity and continual improvement, but is not an entire security baseline itself [13]. The ISO/IEC 27001:2022 is more grounded as it provides FSB with certifiable ISMS that is based on scope, risk treatment, policies, supplier controls, incident handling and continual improvement [11].

NIST CSF 2.0 introduces a more flexible approach to profiling the current maturity, determining the desired state and ranking remediation. The role of its Govern is particularly applicable since FSB is not weak only due to the absence of tools, but the absence of leadership integration, role definition and supply-chain management [12]. COBIT 2019 follows up on this by ensuring that governance is explicit and has accountability regarding oversight, risk appetite, assurance, and performance measurement accountable at board level [10].

The technical model that is most appropriate in the context of cloud-heavy and BYOD-heavy environments in FSB is Zero Trust Architecture. According to NIST, zero trust is the absence of implicit trust, which is determined solely by the network location; identity, device health and policy are continually assessed before access is provided [14]. The subsequent cloud-native guidance provided by NIST demonstrates the potential to use identity-based enforcement of policy and micro-segmentation to assist the multi-cloud and hybrid environments [2]. The best response to FSB is a stratified approach: governance by COBIT, the ISMS by ISO 27001, risk management by NIST CSF 2.0, the operationalisation by ITIL 4 and the technical enforcement by zero trust.

| Framework / model       | Best role                               | Strength                                          | Limitation                                      |
|-------------------------|-----------------------------------------|---------------------------------------------------|-------------------------------------------------|
| ITIL 4                  | Operationalise secure services          | Strong incident, change and continuity discipline | Not a standalone security baseline              |
| ISO/IEC 27001:2022      | ISMS and audit basis                    | Certifiable and evidence-driven                   | Needs business tailoring                        |
| NIST CSF 2.0            | Risk profiling and improvement planning | Govern function and flexible target profiles      | Not certifiable on its own                      |
| COBIT 2019              | Board governance and accountability     | Clear governance/management objectives            | Less detailed on technical controls             |
| Zero Trust Architecture | Dynamic access and segmentation         | Best fit for BYOD and multi-cloud least privilege | Depends on strong IAM, telemetry and automation |

*Table 1. Role of each framework/model in the FSB design.*

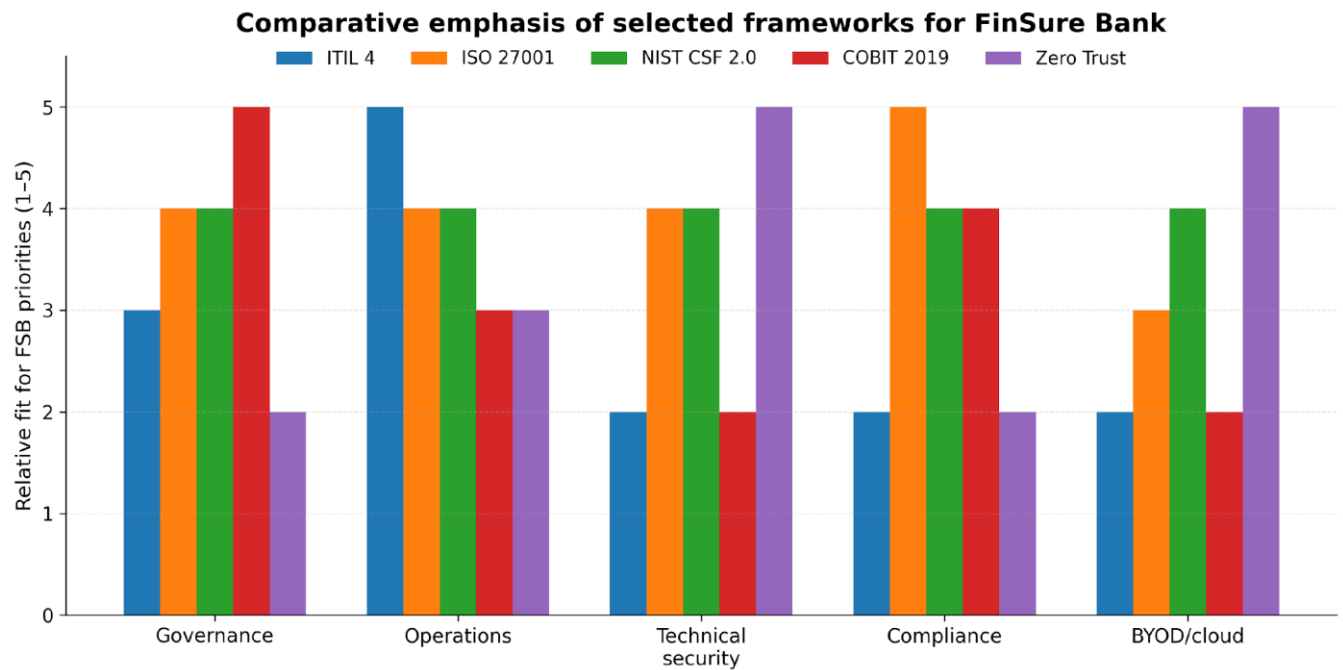


Figure 1. Comparative emphasis of selected frameworks for FSB priorities.

### Assumptions used in this design

1. FSB serves EU/EEA customers, so GDPR applies.
2. DORA is either directly applicable or the most relevant resilience benchmark.
3. External hosting places critical ICT suppliers in scope.
4. BYOD is a business requirement that must be controlled rather than prohibited.
5. FSB currently lacks a mature enterprise data inventory, tested DORA workflow and consolidated access governance model.

### **3. Integrated design for FSB**

FSB should adopt a board-approved security governance model, headed by a Board Risk and Cyber Committee, with the assistance of the CISO, Data Protection Officer, Head of IT Operations and Third-Party Risk Manager. Accountability and review forums should be defined by COBIT, and policies should be structured by ISO 27001, as well as risk treatment and audit evidence and corrective action records [10], [11]. The Board must approve the cyber risk appetite, tolerances of privileged access, cloud concentration limits and incident escalation regulations and review the performance on a quarterly basis.

The areas that the policy stack should focus on include identity and access management, BYOD/mobile security, data classification, encryption, third-party risk, incident response, backup and recovery, logging and data subject rights. BYOD studies reveal that organisations tend to allow personal devices without incurring device-specific controls, training, and user awareness, resulting in unnecessary exposure [16]. FSB should require registration of devices, posture verification, high-quality MFA, phishing-resistant privileged user authentication, encrypted corporate containers, the ability to remotely wipe and contractual terms in access by contractors.

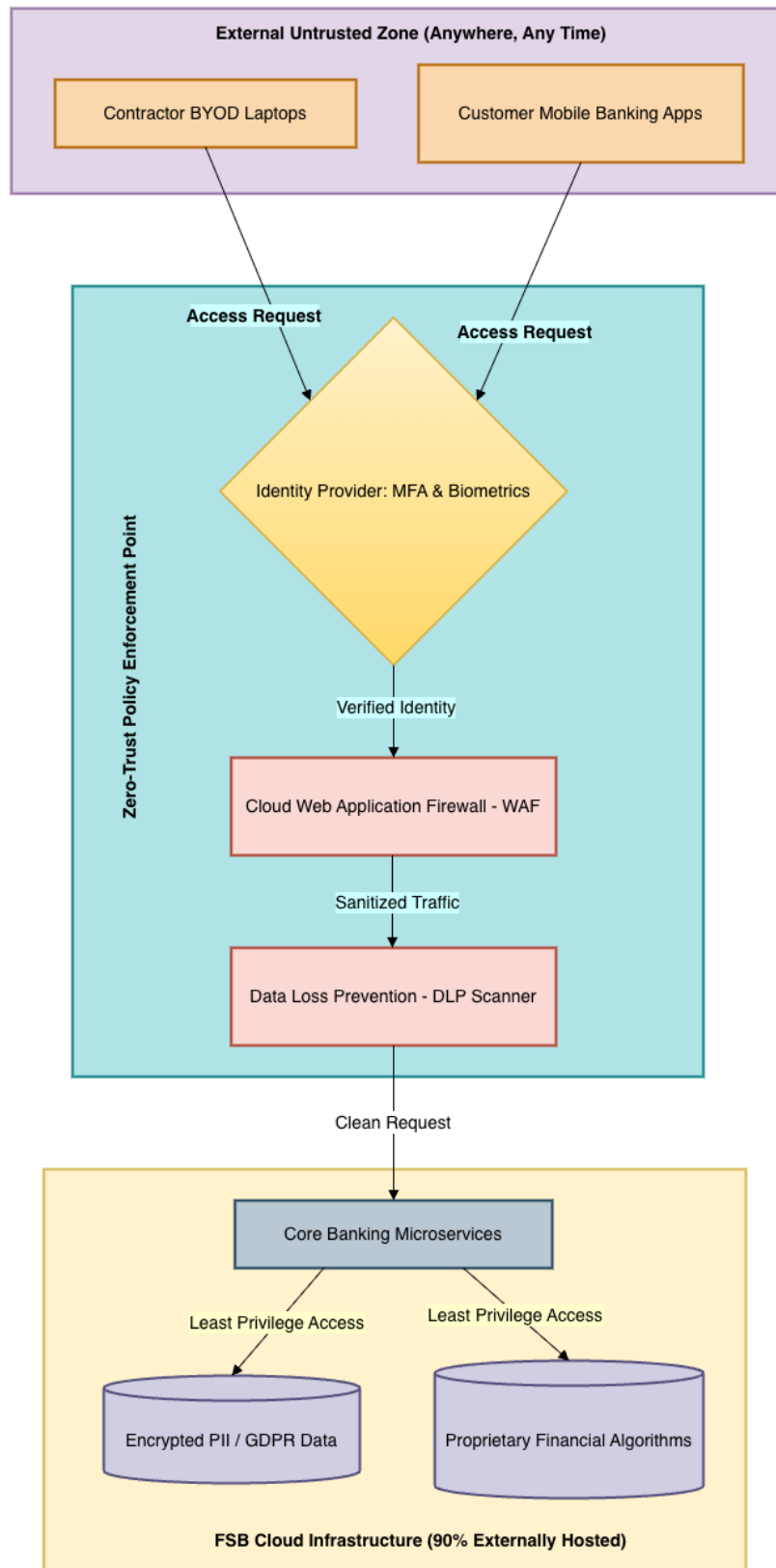


Figure 2. Target zero-trust architecture for FSB.

| Control area                     | Lead owner                     | Priority actions                                         | Illustrative KPI                             |
|----------------------------------|--------------------------------|----------------------------------------------------------|----------------------------------------------|
| Board governance                 | Board Risk and Cyber Committee | Approve risk appetite and review cyber metrics quarterly | Overdue high-risk issues                     |
| Identity and BYOD                | CISO and IAM lead              | MFA, posture checks, PAM and contractor onboarding       | Failed posture checks; privileged exceptions |
| Data governance and privacy      | DPO and data owners            | Classification, data map and DSAR workflow               | Overdue DSARs; data-map coverage             |
| Third-party assurance            | Third-Party Risk Manager       | Critical supplier tiering, audit rights and exit plans   | % critical suppliers assessed                |
| Resilience and incident response | Head of IT Operations and CISO | IR/BCP/DR tests and DORA workflow                        | MTTD; MTTR; exercise completion              |
| Audit and awareness              | Internal Audit and HR/L&D      | Role-based training and annual audits                    | Completion rates; repeat findings            |

*Table 2. Governance and policy ownership model for FSB.*

Technically, zero trust should be the default access model that FSB implements. All access requests from employees, contractors, partners, and mobile application components as well as mobile application fragments must be subjected to a point of policy enforcement that verifies identity strength, posture, behavioural indicators and resource sensitivity prior to providing access under least privilege. The customer channels, core banking service, administrative systems and controlled data stores should be micro-segmented so that a compromise in one zone does not automatically enable lateral movement [2], [14]. The administrative access must be separated to business-user access and just-in-time privilege, with higher level of logging and step-up authentication when performing high risk actions.

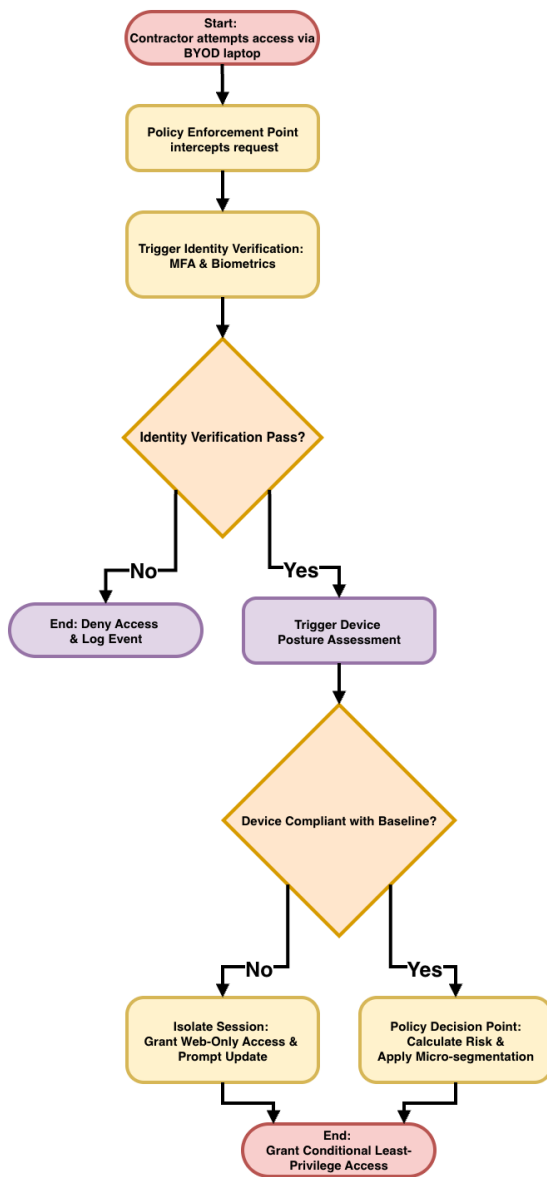


Figure 3. Contractor BYOD access decision flow.

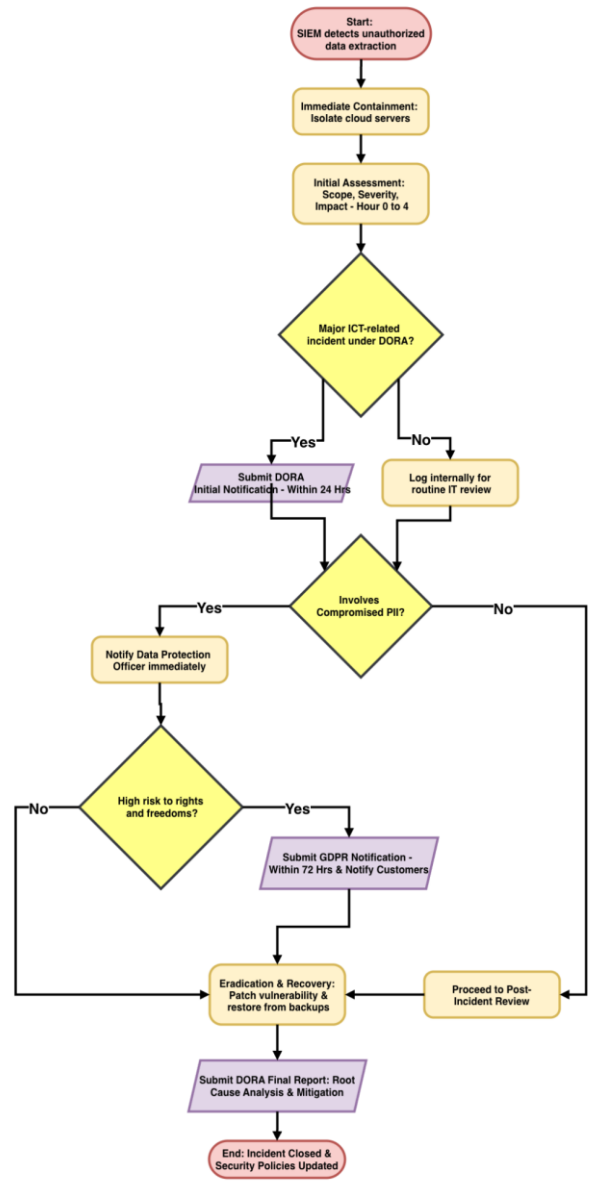


Figure 4. Major ICT incident workflow linking DORA, GDPR, recovery and review.

Access control needs to be accompanied by data governance. Customer PII, payment data, lending history and audit logs and proprietary algorithms are to be categorized and mapped to handling rules. Encryption must be enforced both in transit as well as rest and key management should not be co-located with application administration. There should also be an up-to-date data inventory since it is impossible to satisfy GDPR rights without understanding where the personal data are stored, or who has them in their possession [7], [6].

Risk management should be a continuous process rather than an annual exercise. The current state and the target state can be compared with NIST CSF 2.0 profiles and the key risk indicators are to be reviewed monthly. The heatmap created based on the scenario shows that the third-party compromise, cloud concentration, credential theft, customer account takeover and unmanaged BYOD endpoints are the most significant risks. This priority is supported by new sector reporting: ENISA studied 488

publicly reported European finance incidents between January 2023 and June 2024, with Verizon identifying the involvement of third-party in 30% of breaches, and IBM reporting average costs of USD 6.08 million on breaches in the financial sector in 2024 [3], [9], [15]. FSB should track privileged-access exceptions, unsuccessful posture checks, open critical vulnerabilities, assurance gaps with a supplier, incident response time and overdue cases of DSAR. The management should also map these indicators to a few board level key risk indicators so that these risk trends could be seen early enough to initiate treatment decisions as opposed to explanation after the fact.

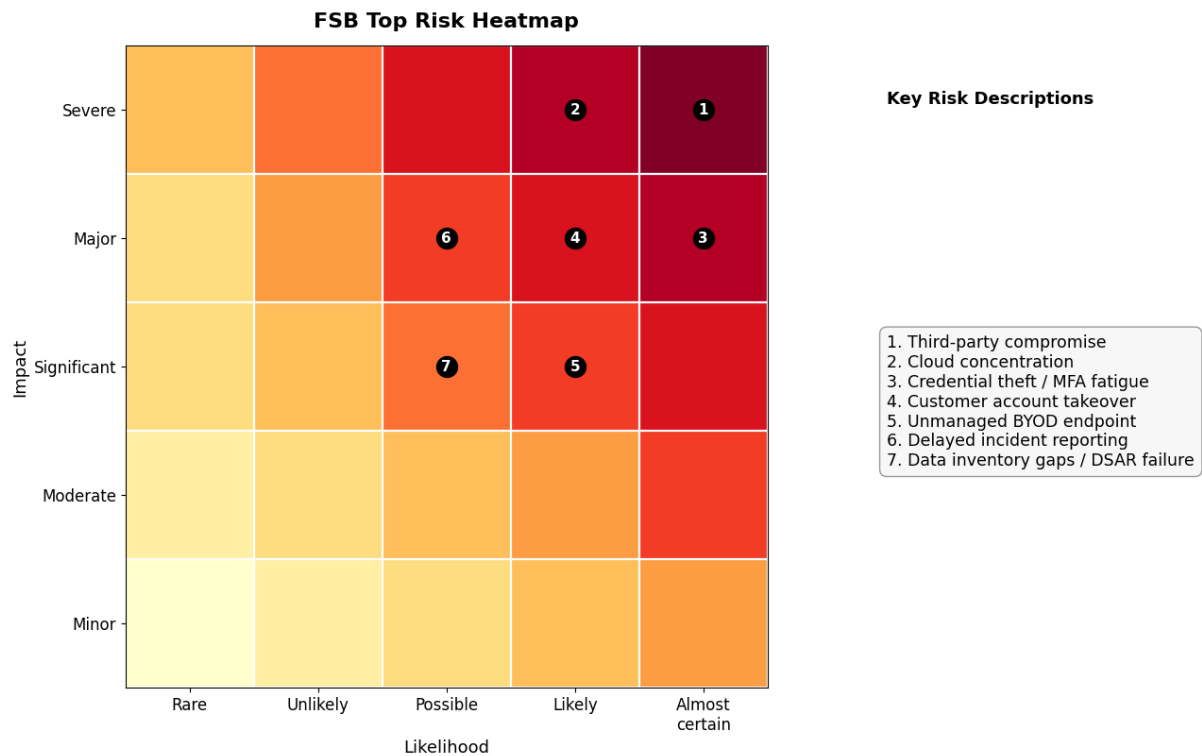


Figure 5. FSB top risk heatmap derived from the scenario and recent finance-sector reporting.

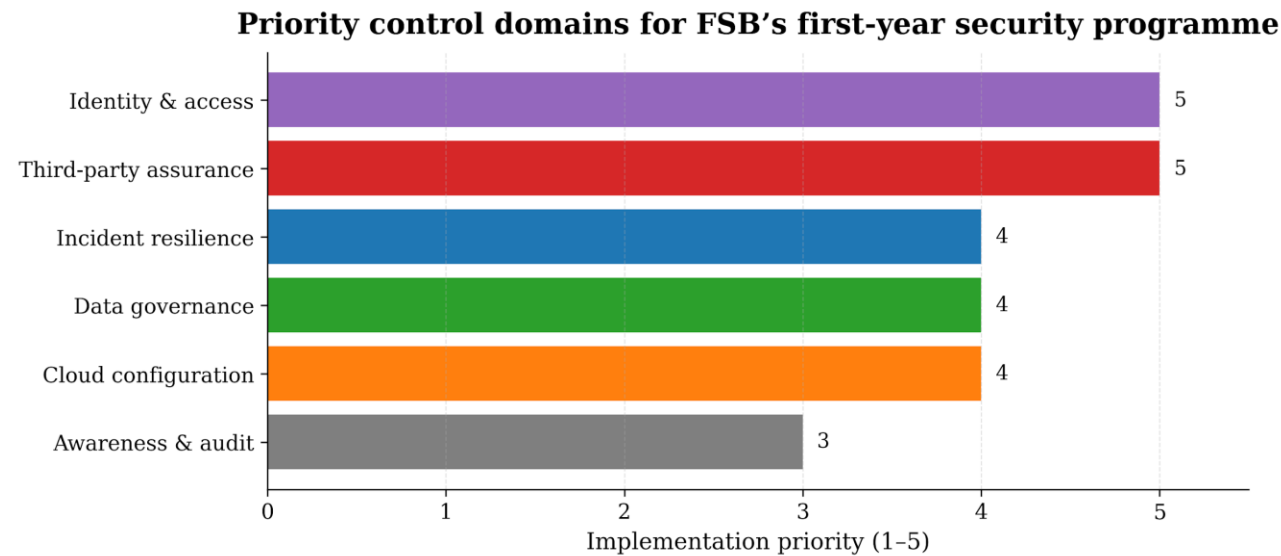


Figure 6. Priority control domains for FSB’s first-year security programme.  
(Author’s synthesis derived from the scenario, risk heatmap and selected frameworks)

Third-party assurance requires special attention because outsourcing does not transfer accountability. Tiering and evaluation should be performed on critical ICT providers in terms of security architecture, breach reporting, audit rights, transparency of subcontractors, backup and exit. Incident notification windows, the retention of logs, recovery targets and patching deadlines should be included in security-specific service levels. This is consistent with the way that ICT third-party risk is handled by DORA and it is aligned with the reliance of FSB on externally hosted infrastructure [8], [4].

FSB also requires an integrated resilience and compliance workflow. Tabletop and technical exercises should be conducted together, and incident response, business continuity and disaster recovery are to be tested together. The notification of a personal data breach that is likely to endanger rights and freedoms should be provided to the supervisory authority, as stipulated by GDPR, within 72 hours, whereas under DORA, time restrictions are now defined in the possible cases of the initial, intermediate and final reporting of major ICT-related incidents [7], [4]. Ideally, FSB must operate on one workflow, which is detect, contain, classify, escalate, notify, recover and review.

It is also important to have a formal process of data subject access request (DSAR). The requests must pass through the identity verification, request triage, data discovery, legal-exemption checking and secure delivery. According to EDPB guidance, the right of access is not merely a legal requirement but is an operating requirement, which requires that it be searchable, controllable and intelligible in terms of its communication [6]. This necessitates FSB to have a central case-management process, which is connected to its data map, so that the responses are comprehensive, timely and auditable. The deletion requests must be verified against legal-retention exemptions and responses to customers should be consistent in wording to ensure that compliance is not only comprehensible but also correct.

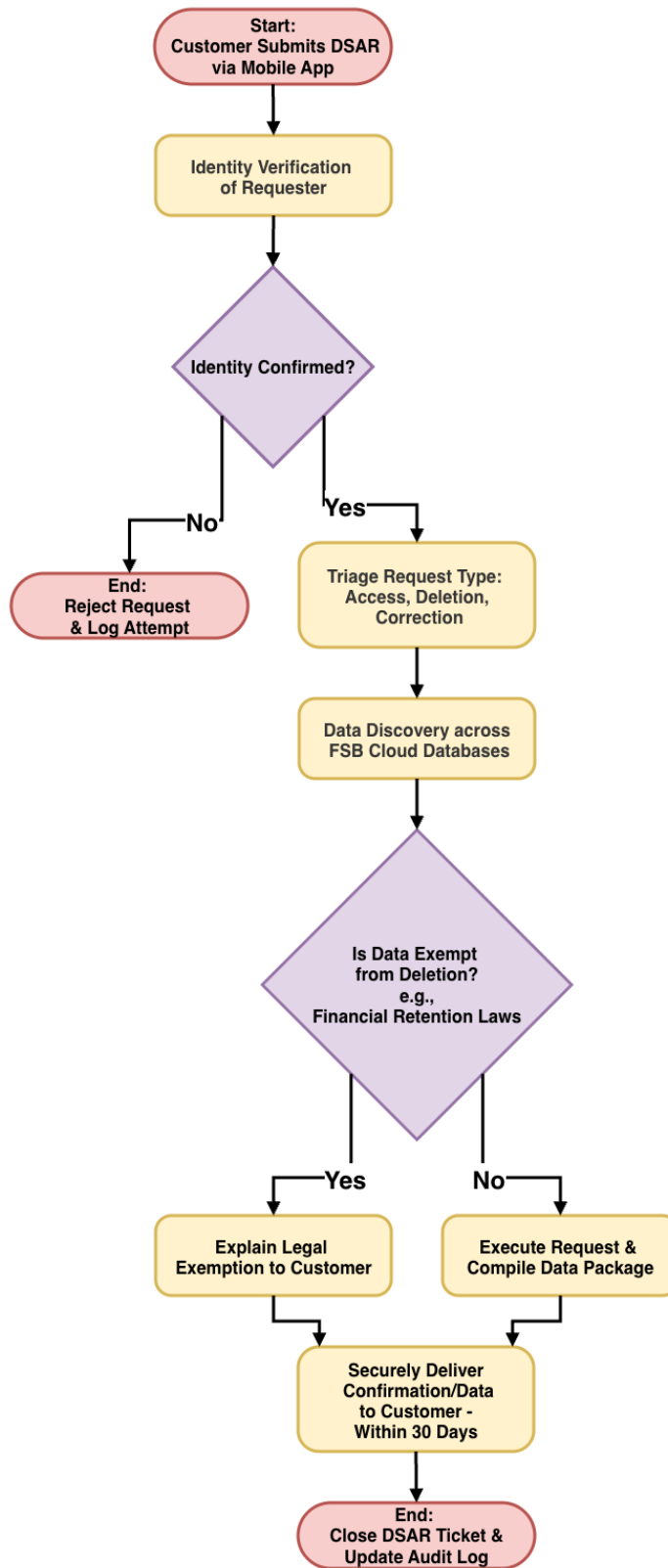


Figure 7. DSAR workflow from identity verification to secure delivery.

| Obligation | Trigger | Time expectation | FSB response |
|------------|---------|------------------|--------------|
|------------|---------|------------------|--------------|

|                                               |                                    |                                                                                                                                                |                                                                                |
|-----------------------------------------------|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Major ICT-related incident (DORA)             | Incident classified as major       | Initial notice within 4 hours of classification and no later than 24 hours after awareness; intermediate within 72 hours; final within 1 month | Classify, notify regulator, preserve evidence and complete root-cause analysis |
| Personal data breach (GDPR Art. 33)           | Likely risk to rights and freedoms | Notify supervisory authority within 72 hours                                                                                                   | Privacy/legal escalation, impact assessment and regulator notification         |
| High-risk personal data breach (GDPR Art. 34) | High risk to individuals           | Without undue delay                                                                                                                            | Notify affected customers with protective guidance                             |
| DSAR right of access                          | Verified request from data subject | Normally within 1 month; limited extension possible where justified                                                                            | Case management, data retrieval and secure delivery                            |

Table 3. Key regulatory triggers and FSB operating responses.

ITIL 4 also adds value since security decisions need to endure daily service provision. The secure change enablement, incident prioritisation, service configuration management and continuity planning are required in the case of FSB to ensure that the governance intent would not fail during the operations [13]. The bank should therefore incorporate security checks in the customer app change approvals, cloud infrastructure and administrative privileged access.

Continuous assurance is necessary. Governance effectiveness and policy compliance and high-risk technical controls should be tested by internal audit whereas independent testing should include cloud configuration, privileged access, phishing resilience and supplier assumptions. Exception review should be done by the management on a monthly basis and time-bound remediation plans must be required.

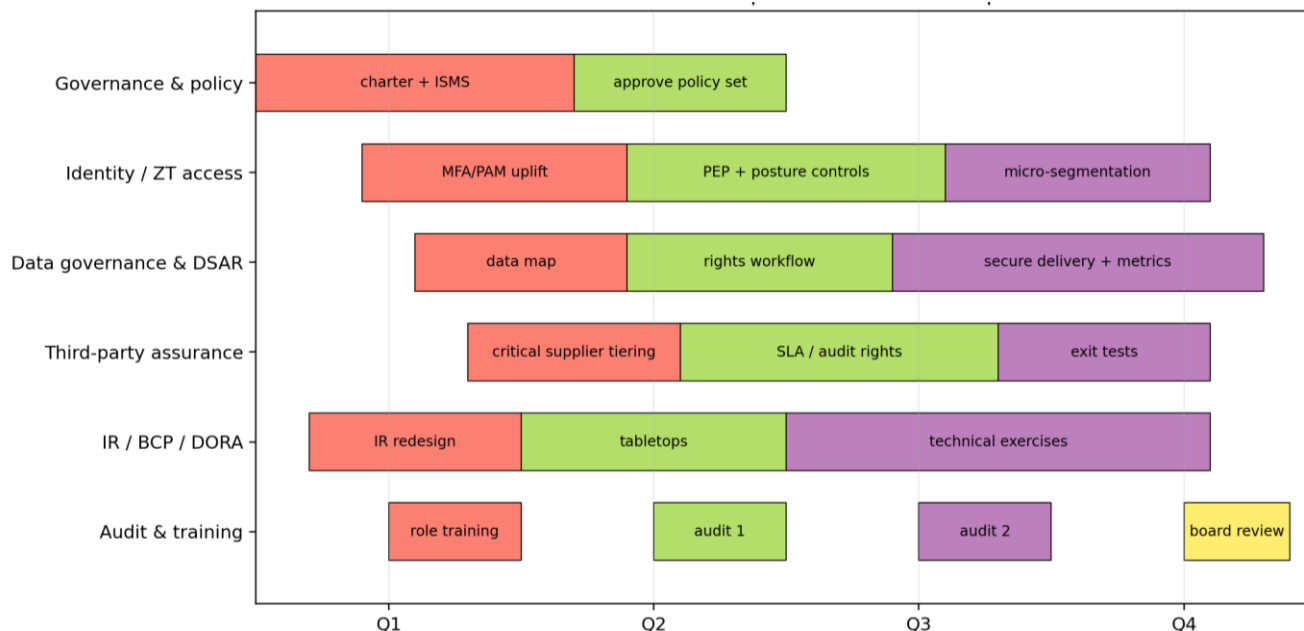


Figure 8. Illustrative 12-month implementation roadmap for FSB.

All cloud platforms, identity systems, endpoints and key applications should have monitoring and logging that is centralised. The security telemetry should be correlated within a single workflow to enable the quick investigation of failed posture checks, anomalous sign-ins, evidence of privileged actions and data-exfiltration. In the case of regulated banking services, time-synchronisation of logs,

retention based on legal and audit requirements and unauthorised change protection should be provided. This would enhance the security operations and quality of evidence towards both DORA, GDPR and internal audit checks.

Mobile applications, API and cloud infrastructure changes, such as code review, secrets management, vulnerability testing and rollback planning should also be incorporated in the secure-by-design development gates of FSB. This helps ensure that governance and compliance controls are embedded in practice rather than remaining paper-based.

## **4. Why updated regulations and standards remain good practice**

Regularly updating regulations and standards is a good practice since the pattern of threats, technologies and business dependencies evolve more rapidly than fixed sets of control. The primary risks of FSB, the concentration of clouds, exposure to mobile banking, supplier dependence, abuse of credentials and cross-border data processing are even more urgent today as compared to the time when many perimeter-centred models were authored. This can be exemplified by the revision of NIST CSF to the version 2.0: the introduction of Govern is indicative of the fact that cyber failure tends to start with poor leadership, absence of accountability and uncontrolled dependencies in the supply-chain, as opposed to being confined to technical misconfiguration only [12]. Similarly, the presence of complex digital ecosystems in which financial companies are now reliant on the fact that they require harmonised resilience and incident-reporting regulations is reflected in DORA and its reporting standards [8], [4].

Updated guidance also reduces ambiguity. Breach notification and access rights guidance by EDPB converts the wide-ranging GDPR requirements into realistic expectations regarding evidence, timeliness and communication, and ensures consistency in compliance across organisations [5], [6]. The right answer is not to fight change, but to develop a governance model that is able to assimilate it with an ongoing control library, explicit ownership and repeatable change management.

A high rate of regulatory change may pose implementation pressure, documentation and compliance fatigue, in particular with legacy systems. The issue is not compliance itself, but weak governance arrangements. FSB is advised to have a mapped control library showing which controls satisfy which laws, standards and internal policies. That strategy makes regulatory change a design undertaking to be handled, not a set of unrelated paperwork actions.

## **Conclusion**

FSB is not required to have another stand-alone security initiative; it should have a combined operating model. A layered design in which COBIT 2019 defines governance, ISO/IEC 27001:2022 establishes the ISMS, NIST CSF 2.0 structures risk management, ITIL 4 supports secure services, and Zero Trust Architecture enforces dynamic access is the strongest approach. This design would minimize the exposure of FSB and enhance regulatory defensibility since it is backed by enhanced supplier assurance, tested incident response, DSAR workflows and frequent audit. New rules and standards must be considered the strategic input to that model since, in a digital bank, security, governance and compliance are variants of the same discipline.

## References

- [1] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: Systematic review," *Comput. Secur.*, vol. 99, Art. no. 102030, Dec. 2020, doi: 10.1016/j.cose.2020.102030.
- [2] R. Chandramouli and Z. Butcher, "A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments," NIST, Gaithersburg, MD, USA, NIST SP 800-207A, 2023, doi: 10.6028/NIST.SP.800-207A.
- [3] ENISA, "ENISA Threat Landscape: Finance Sector," 2025. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector>
- [4] *Commission Delegated Regulation (EU) 2025/301 on time limits and content for reporting major ICT-related incidents under DORA*, European Commission, 2025. [Online]. Available: [https://eur-lex.europa.eu/eli/reg\\_del/2025/301/oj/eng](https://eur-lex.europa.eu/eli/reg_del/2025/301/oj/eng)
- [5] European Data Protection Board, "Guidelines 9/2022 on personal data breach notification under GDPR," 2023. [Online]. Available: [https://www.edpb.europa.eu/our-work-tools/documents/guidelines/guidelines-92022-personal-data-breach-notification-under\\_en](https://www.edpb.europa.eu/our-work-tools/documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en)
- [6] European Data Protection Board, "Guidelines 01/2022 on data subject rights – Right of access," 2023. [Online]. Available: [https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_en)
- [7] *Regulation (EU) 2016/679 (General Data Protection Regulation)*, European Parliament and Council, Apr. 2016. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- [8] *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)*, European Parliament and Council, Dec. 2022. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng>
- [9] IBM, "Cost of a data breach 2024: Financial industry," 2024. [Online]. Available: <https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry>
- [10] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*, Rolling Meadows, IL, USA: ISACA, 2019.
- [11] *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*, ISO/IEC Standard 27001:2022, 2022.
- [12] NIST, "The NIST Cybersecurity Framework (CSF) 2.0," Gaithersburg, MD, USA, NIST CSWP 29, 2024, doi: 10.6028/NIST.CSWP.29.
- [13] PeopleCert, *Reader's Manual: ITIL 4 Practice Guide*, 2023. [Online]. Available: <https://www.axelos.com/resource-hub/practice/readers-manual-til-4-practice-guide>
- [14] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST, Gaithersburg, MD, USA, NIST SP 800-207, 2020, doi: 10.6028/NIST.SP.800-207.
- [15] Verizon, "2025 Data Breach Investigations Report," 2025. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/>

- [16] T. A. Wani, A. Mendoza, K. Gray, and F. Smolenaers, "Status of bring-your-own-device (BYOD) security practices in Australian hospitals – A national survey," *Health Policy Technol.*, vol. 11, no. 3, Art. no. 100627, Sep. 2022, doi: 10.1016/j.hlpt.2022.100627.