



Assignment

Data Security, Governance and Compliance Framework Design for FinSure Bank (FSB)

Submitted By

Abdullah Al Noman

Student ID:

2520302

Module

**Data Security, Governance and Compliance
(ACCA7028_LON)**

Department

MSC Cybersecurity and Digital Forensics

Table of Contents

Section	Title	Page No.
—	Abstract	i
1	Introduction	3
2	Review of Security Frameworks and Models	4
2.1	ISO/IEC 27000 Series	4
2.2	Information Technology Infrastructure Library (ITIL)	5
2.3	NIST Frameworks	5
2.4	COBIT	6
2.5	Comparative Overview of Security Frameworks	6
3	Designed Security, Governance and Compliance Framework for FSB	7
3.1	Assumptions	7
3.2	Governance and Strategic Planning	7
3.3	Security Policies	9
3.4	Risk Management	9
3.5	Protection Mechanisms	10
3.6	Contingency Planning	11
3.7	Service Level Agreements (SLAs)	12
4	Importance of Continuous Regulatory and Standards Updates	12
5	Conclusion	14
—	References	14

Data Security, Governance and Compliance Framework Design for FinSure Bank (FSB)

Abstract

Digital-first financial services have made businesses more reliant on cloud platforms, bring-your-own-device (BYOD) policies, and third-party interfaces. These technologies make it possible to scale and change how things work, but they also create big problems with security, governance, and compliance. Financial institutions work in environments that are very tightly controlled. If they don't protect data or manage risks well, they could face fines, damage to their reputation, and loss of trust from stakeholders.

This research looks at FinSure Bank (FSB), a cloud-based bank that doesn't have a single security governance model, a formal risk management strategy, or organized compliance procedures. The research examines ISO/IEC 27000, ITIL, NIST, and COBIT using established security frameworks and ACCA7028 course material. It also suggests an integrated governance, risk, and compliance (GRC) framework that fits FSB's operating context. The paper also looks at how important it is for regulations to be constantly enforced.

1. Introduction

Cloud computing, mobile platforms, digital payments, and data-driven services have changed the financial services industry by making it possible for operations to be scalable and always available. But new technologies have also made it easier for hackers to get into organizations, especially through BYOD access and third-party integrations. Because of this, banks and other financial organizations are more likely to be targeted by cyber threats, face more scrutiny from regulators, and be held to higher ethical standards. Seeing how common threat categories are spread out helps put the security risks that FinSure Bank faces into context.

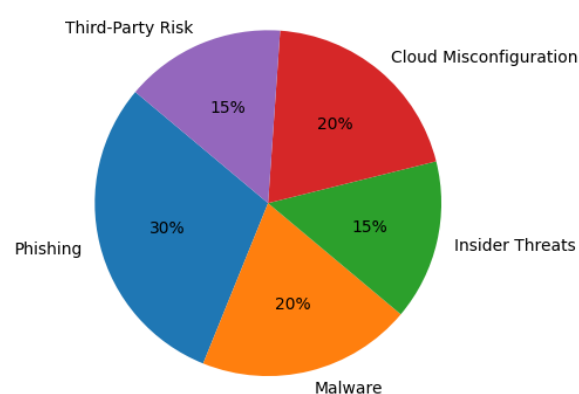


Figure 1. Distribution of common security threats affecting financial institutions

The CIA triad, which stands for Confidentiality, Integrity, and Availability, is often used to explain the basics of information security. The CIA trinity is still important, but most modern security events don't happen because of single technical problems. Instead, breaches often happen because of insufficient governance, uneven risk management, human mistake, or poor policy enforcement. Seeing how

prevalent danger types are spread out and how important CIA principles are in relation to each other helps us understand the threats that FinSure Bank faces. Confidentiality, integrity, and availability are all important security principles, but they are not all equally important in the financial services industry because of how sensitive regulations are and how important transactions are.

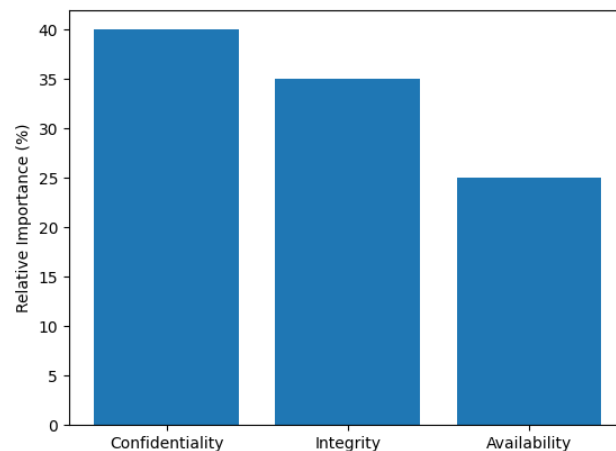


Figure 2. Relative importance of confidentiality, integrity, and availability in financial services.

FSB is a digital-first company that mostly uses cloud technology. It doesn't have security standards that apply to the whole company, a uniform governance framework, or organized compliance auditing. These problems put the organization at risk of data breaches, insider threats, regulatory fines, and loss of customer trust.

2. Review of Security Frameworks and Models

2.1 ISO/IEC 27000 Series

The ISO/IEC 27000 series is a well-known way to handle information security around the world. ISO/IEC 27001 sets the standards for setting up and keeping an Information Security Management System (ISMS) going. ISO/IEC 27002 gives advice on how to put security controls in place in areas like access control, cryptography, incident management, and supplier relationships. This method works especially well for financial institutions like FSB, which need to find a balance between strong security controls and operational flexibility in cloud and mobile settings. ISO/IEC 27001 takes a continuous improvement approach to managing information security, making sure that controls stay effective as risks change.

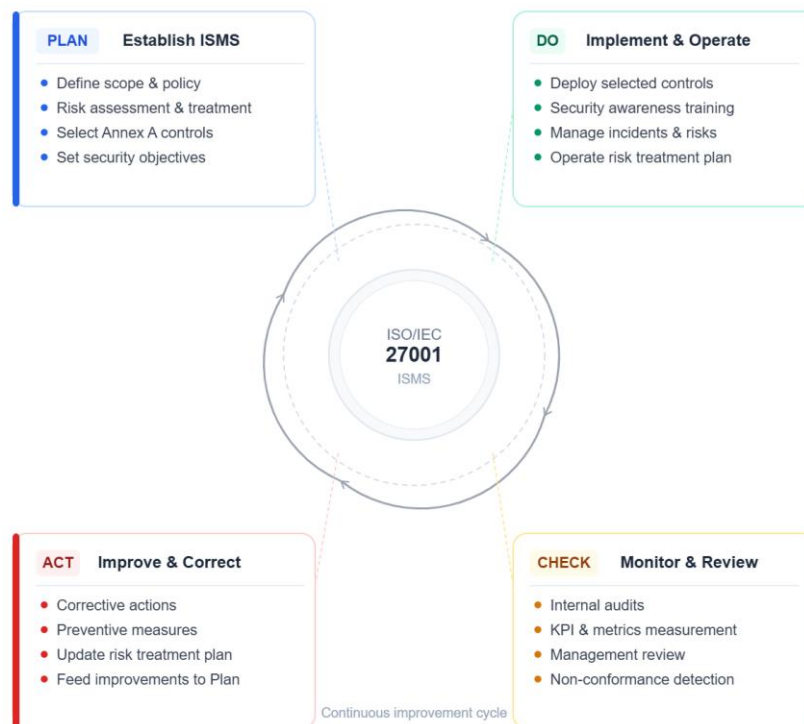


Figure 3. ISO/IEC 27001 ISMS lifecycle based on the Plan–Do–Check–Act model.

One of the best things about ISO/IEC 27001 is that it takes a risk-based approach, which means that organizations have to look at their information assets, risks, and weaknesses before putting in place controls that are appropriate. This flexibility is especially useful for banks and other financial institutions that work in the cloud and on mobile devices. ISO standards only work if executives are committed to them and there is monitoring from the board of directors. If these things aren't in place, ISO adoption could become a compliance-driven exercise instead of a management system that keeps getting better.

2.2 Information Technology Infrastructure Library (ITIL)

ITIL is a set of best practices that helps make sure that IT services are in line with business goals. ITIL doesn't focus on security, but it does make security measures work across the service lifecycle through Service Design, Service Transition, Service Operation, and Continual Service Improvement. ITIL helps FinSure Bank make sure that security needs are included into everyday tasks including designing cloud services, managing controlled change, addressing incidents, and keeping an eye on availability. ITIL works with ISO 27001 to turn high-level security rules into consistent daily practices across cloud services, BYOD environments, and third-party integrations.

2.3 NIST Frameworks

The NIST Cybersecurity Framework (CSF) and the larger NIST SP 800 series give clear and useful advice on how to handle cybersecurity risks, respond to incidents, and make organizations more resilient. The CSF breaks down security tasks into five main categories: Identify, Protect, Detect, Respond, and Recover [5]–[7]. This structure, which is based on the lifecycle, works especially well in environments where threats are always changing and quick detection and response are very important.

NIST's advice helps FinSure Bank be more ready for business in a number of important ways. The Identify function helps with structured asset classification and putting risks in order of importance. Protect and Detect are about putting in place safety measures and monitoring systems. Respond and Recover are about how to deal with incidents, recover from disasters, and keep the business running. These features are necessary to keep services available and follow the rules in case of a security breach.

NIST frameworks add to ISO standards by giving more specific operational guidance, especially in areas like risk assessment (NIST SP 800 30) and incident response planning (NIST SP 800 61). ISO and NIST work well together because they provide both governance structure and operational depth. This makes them a good fit for a full GRC framework.

2.4 COBIT

ISACA created COBIT (Control Objectives for Information and Related Technologies), a complete framework that focuses on making sure that IT governance and corporate governance goals are in line with each other. COBIT is different from ISO 27001 and NIST because it focuses on governance structures, accountability, and value delivery at the organizational level [8].

COBIT is especially important for industries that are regulated, like financial services, where executive oversight, regulatory accountability, and measurable performance are very important. The framework makes it clear what the differences are between governance responsibilities (which are at the board and executive level) and management responsibilities (which are about planning, building, running, and monitoring IT-enabled services). This separation directly addresses a common problem with digital-first companies: security decisions are often left up to technical teams without enough oversight from executives.

COBIT helps FinSure Bank set up:

- Clearly defined roles and duties for overseeing information security
- Board members can see security risks and compliance status
- Using key risk indicators (KRIs) and key performance indicators (KPIs) to measure performance
- Making sure that security investments are in line with the business strategy and risk appetite

COBIT also works with ISO 27001 by making sure that ISMS goals are connected to business goals instead of working on their own. COBIT, on the other hand, only gives limited technical advice. To get good end-to-end security governance, it needs to be used with operational frameworks like ISO 27001 and NIST.

2.5 Comparative Overview of Security Frameworks

The frameworks that were looked at each deal with a different part of information security and governance. ISO 27001 sets up a formal management system for security, NIST adds operational depth for risk and incident management, ITIL makes security a part of service operations, and COBIT makes sure that senior management is in charge and accountable.

Framework	Primary Focus	Key Strengths	Key Limitations
ISO/IEC 27001	Information Security Management	Risk-based, internationally recognised	Requires strong executive commitment
ITIL	Service Management	Operational integration	Limited security specificity
NIST	Risk and Incident Management	Practical, prescriptive guidance	US-centric origins
COBIT	IT and Security Governance	Board-level oversight	Minimal technical detail

FinSure Bank needs more than one framework to work with. Instead, a hybrid approach is needed to deal with governance, operational security, and regulatory compliance all at once.

3. Designed Security, Governance and Compliance Framework for FSB

3.1 Assumptions

The proposed framework is based on the following operational and regulatory assumptions:

- FinSure Bank works in many different places and has to follow both GDPR and national financial rules [9].
- Cloud platforms host core systems and data storage.
- Allowing employees to bring their own devices to work is a long-standing business need.
- Senior management backs efforts to improve governance and follow the rules.

These assumptions reflect the realities of modern digital financial institutions and inform the design of the proposed framework.

3.2 Governance and Strategic Planning

Based on Week 4, the suggested method uses a Governance, Risk, and Compliance (GRC) model that combines the best parts of ISO 27001, NIST, COBIT, and ITIL [3], [5], and [8]. The board of directors is in charge of governance. They set the company's risk appetite, approve security policies, and make sure the company follows all the rules. Senior management is in charge of turning these orders into operational controls and keeping an eye on how well they work. FinSure Bank needs an integrated governance, risk, and compliance architecture to make sure that executive oversight and operational security controls are in sync.

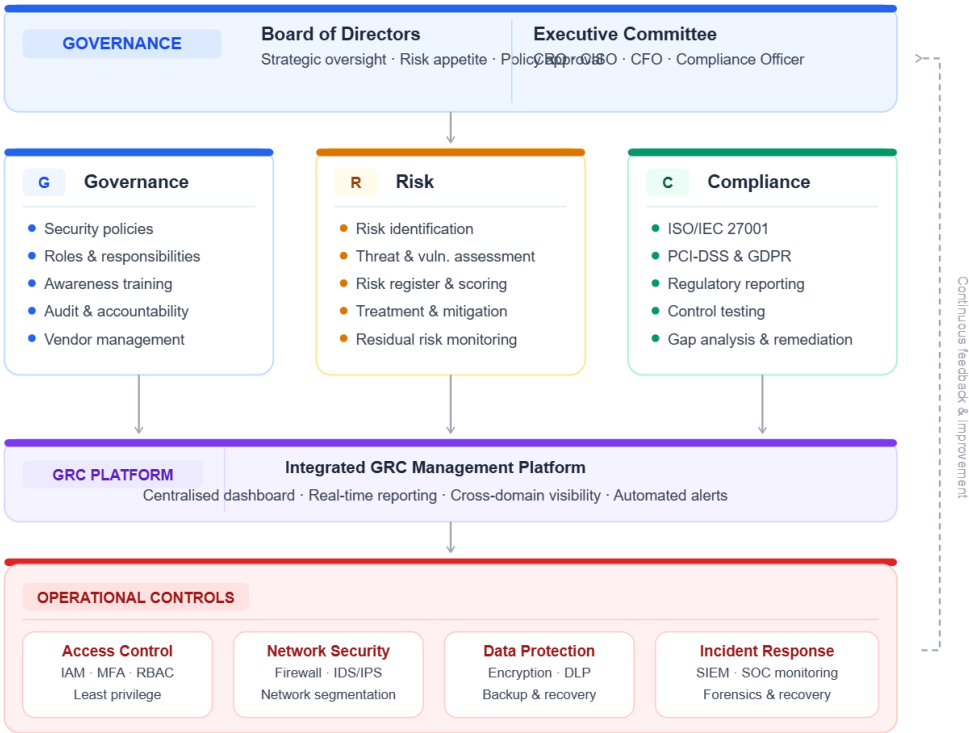


Figure 4. Integrated governance, risk, and compliance framework for FinSure Bank.

For security governance to work, there needs to be a clear division of duties between the board, executive management, and technical security teams.

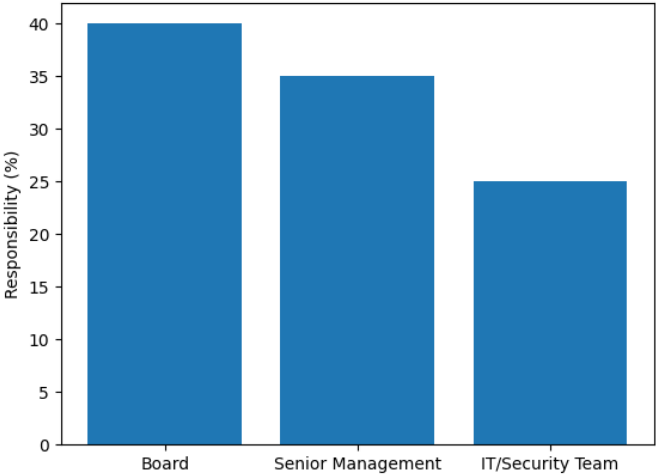


Figure 5. Distribution of security governance responsibilities within FinSure Bank.

This way of running things makes sure that security is seen as a business function that is important to the company's strategy, not just a technical issue. It also makes it easy to report security incidents, compliance breaches, and new risks, making sure that top management is still responsible for the results of information security.

3.3 Security Policies

Consistent with the policy hierarchy discussed in Weeks 3 and 4, FinSure Bank should implement a structured policy framework comprising:

1. **Enterprise Information Security Policy (EISP)** – defining overarching security objectives, responsibilities, and governance principles.
2. **Issue-Specific Security Policies (ISSP)** – addressing specific risk areas such as BYOD usage, cloud access, data classification, and third-party connectivity.
3. **System-Specific Policies (SysSP)** – defining technical requirements for individual systems and platforms.

To make sure that policies are always followed and can be defended in court, they need to be backed up by standards, procedures, and guidelines. Policy documentation is also very important evidence during audits and regulatory investigations in regulated environments [1], [2].

3.4 Risk Management

Based on Week 7 and NIST SP 800-30, FinSure Bank should implement a formal risk management lifecycle encompassing:

- Asset identification and classification
- Threat and vulnerability assessment
- Likelihood and impact analysis
- Risk treatment strategies, including mitigation, transfer, acceptance, and avoidance

You can see the results of a risk assessment by mapping the chance of something happening against the possible effects. This helps you keep your risk priorities straight.

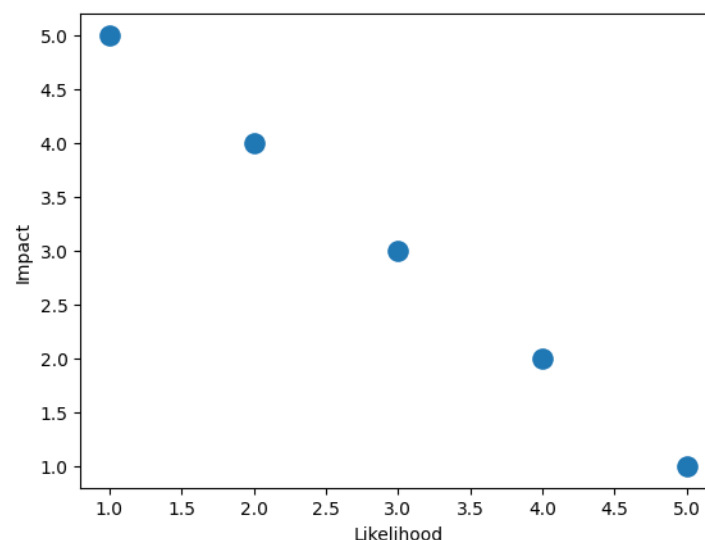


Figure 6. Risk assessment matrix based on likelihood and impact.

Different ways to deal with risk may be used depending on how much risk the organization is willing to take and the rules that are in place.

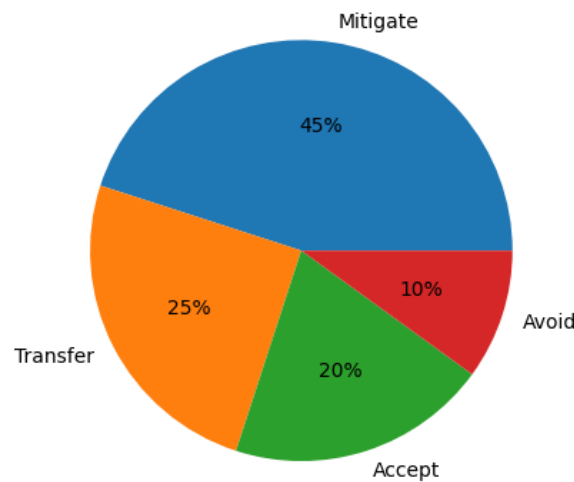


Figure 7. Distribution of risk treatment strategies within the proposed framework.

This structured method makes sure that risks are ranked by how they affect the business, not by how serious they seem to be technically. For instance, risks that could affect customer financial data or the integrity of transactions should be given more weight than risks that could affect non-critical systems. The organization can respond to new threats and changing regulatory expectations by doing risk reviews on a regular basis [6], [7].

3.5 Protection Mechanisms

Based on Weeks 8 and 9, the suggested framework includes multiple layers of protection to keep information assets safe. These are network security measures like firewalls and intrusion detection/prevention systems, secure remote access through VPNs, and strong cryptographic controls to keep data safe when it is not being used, when it is being sent, and when it is being used. Encryption must be used at all stages of data processing and storage in order to fully protect it. Security measures in banks and other financial institutions should work together as layers of protection instead of separate systems. Seeing how control coverage works across different areas shows how important it is to have multiple layers of defense to protect sensitive financial data.

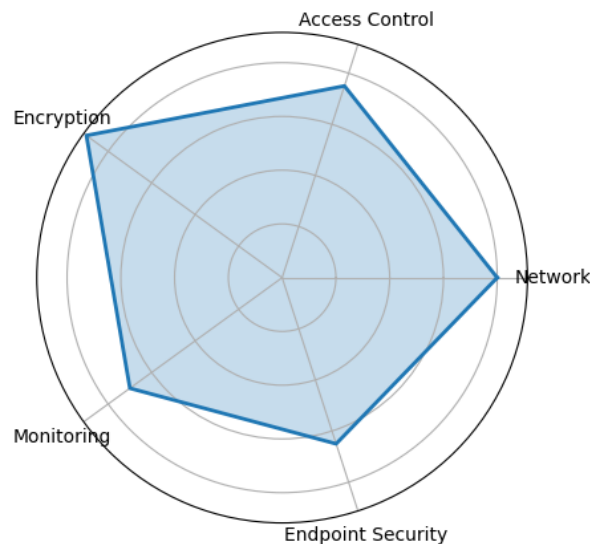


Figure 8. Layered security control coverage across key protection domains.

Access control mechanisms must implement the principles of least privilege and role-based access control (RBAC) to mitigate the risks of insider threats and unauthorized data exposure. These controls are especially important in cloud and BYOD settings to stop credential compromise and lateral movement within systems [1], [5].

3.6 Contingency Planning

As we talked about in Week 6, FinSure Bank needs to have full backup plans, like an Incident Response Plan (IRP), a Disaster Recovery Plan (DRP), and a Business Continuity Plan (BCP). These plans spell out who is responsible for what, how to talk to each other, and what to do first in case of security breaches or system failures. Incident response follows a set process that makes it easier to quickly find, contain, and recover from security events.

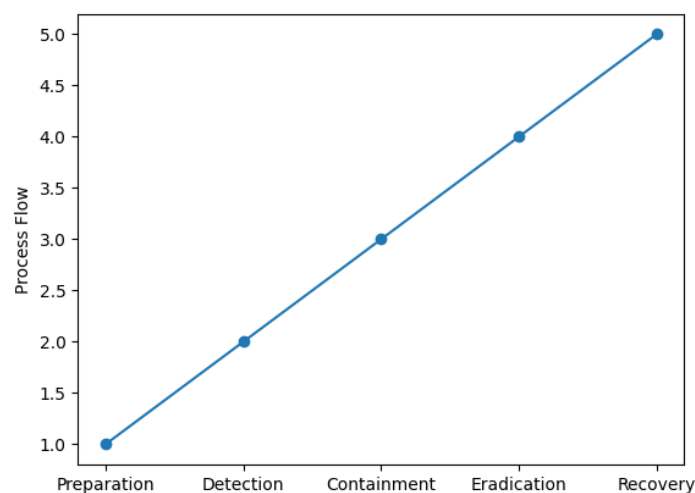


Figure 9. Incident response lifecycle stages.

To make sure that plans stay useful and in line with changes in the organization, they need to be tested regularly through tabletop exercises and simulations. Regulatory frameworks are increasingly necessitating evidence of such testing, especially within the financial sector [7].

3.7 Service Level Agreements (SLAs)

Because FSB depends on cloud providers and third-party service vendors, Service Level Agreements (SLAs) need to be very clear about security responsibilities, availability requirements, incident notification timelines, and compliance obligations. SLAs should also say who has the right to audit and what the penalties are for not following the rules, making sure that everyone in the extended enterprise ecosystem is responsible [5], [8].

4. Importance of Continuous Regulatory and Standards Updates

Information security works in a risk environment that is always changing because of new technologies, new threat actors, and changing social norms. As cloud computing, artificial intelligence, mobile platforms, and cross-border data flows bring in new risks that old rules don't cover, static regulatory frameworks quickly stop working.

To fix problems with governance, supply chain risk, insider misuse, and ethical issues relating to data ownership and algorithmic decision-making, financial institutions like FinSure Bank need to keep updating its rules and regulations. Seeing regulatory forces, the growth of complexity, and the concentration of ethical risk shows why adaptive governance frameworks are needed to keep compliance, resilience, and stakeholder confidence.

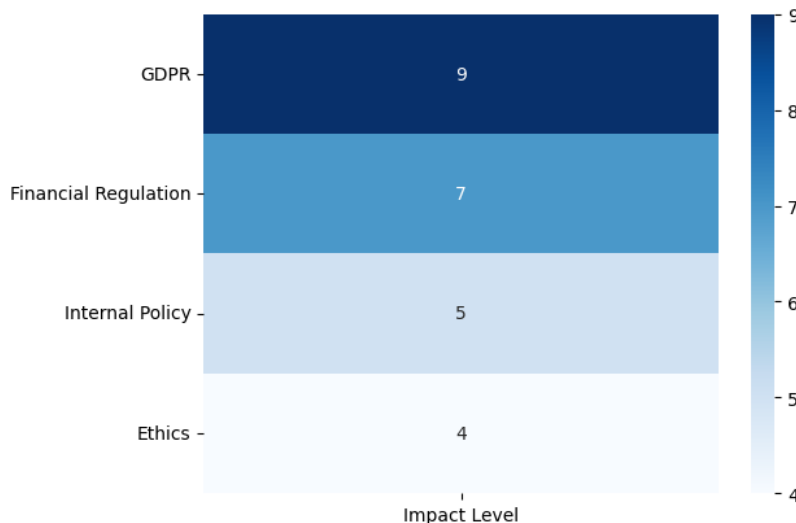


Figure 10. Relative influence of key compliance drivers in financial institutions.

For instance, traditional data protection laws were based on infrastructure that was on-site and well-defined organizational boundaries. On the other hand, modern cloud environments have shared responsibility models, changing data locations, and complicated dependencies on third parties, all of which make it harder to be accountable and follow the rules [9]. Regulatory requirements do not progress in a continuous linear fashion; rather, they frequently escalate in distinct phases subsequent to significant technological, legislative, or ethical advancements.

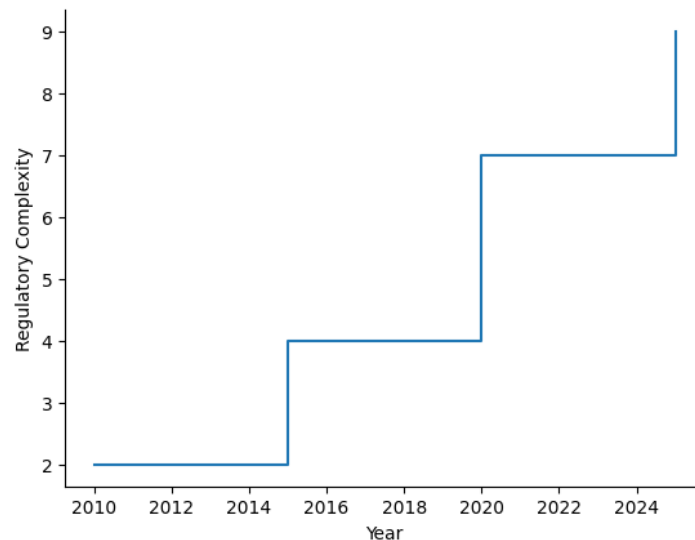


Figure 11. Evolution of regulatory complexity over time.

Ethical factors make the need for regulatory change even stronger. As discussed in Weeks 3 and 9, modern information systems bring up moral issues about who owns data, who watches it, how algorithms make decisions, and how to make money off of personal information. More and more, banks and other financial institutions use automated decision systems and data-driven analytics. If these systems aren't properly managed, they can introduce bias, make things less clear, and hurt customer trust. New rules and standards are very important for setting ethical limits and ways to hold people accountable for these kinds of technologies. Visualising the concentration of these risks helps identify areas requiring stronger governance oversight.

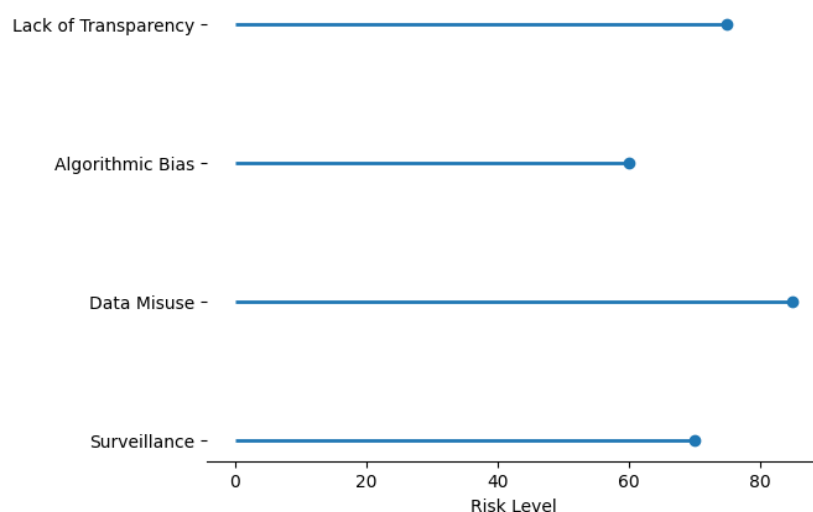


Figure 12. Concentration of ethical risks in data-driven financial systems.

If organizations don't change their regulatory and standards frameworks, they could face serious consequences. If security practices are out of date, they could lead to fines from regulators, damage

to the company's reputation, loss of customer trust, and systemic risk to the financial sector. For FinSure Bank, staying in line with changing rules and standards is not just a matter of following the rules; it is also a strategic necessity for staying competitive, building trust, and keeping operations stable in a digital world that is changing quickly.

5. Conclusion

This report has demonstrated that the security challenges faced by FinSure Bank stem not from not just technology, but also broken governance structures, poor risk management practices, and poor integration of compliance mechanisms. In a world where cloud computing, BYOD access, and many third-party dependencies are common, traditional security methods that only focus on technical controls are no longer enough.

The report has shown that each of the established security frameworks and models, such as ISO/IEC 27001, ITIL, NIST, and COBIT, deals with different but related parts of information security. ISO 27001 gives you a structured way to manage security governance, NIST gives you useful tips on how to handle risk and incidents, ITIL makes sure that security is part of service operations, and COBIT makes sure that executives are in charge and responsible. When put together into a single GRC model, these frameworks offer a complete solution for the complicated operational and regulatory environment of a digital-first bank.

The proposed security, governance, and compliance framework for FinSure Bank stresses accountability at the board level, structured policy hierarchies, formal risk management lifecycles, layered technical controls, and strong planning for unexpected events. The framework helps both operational resilience and regulatory compliance by making sure that security goals are in line with business strategy and legal requirements. It also understands how important service level agreements and third-party governance are for managing risk in an extended enterprise.

Finally, the report has shown that modern information security practice needs to have rules and standards that change all the time. New technologies, smart criminals, and moral dilemmas all require flexible regulatory frameworks that can deal with new risks as they come up. For banks like FinSure Bank, security is a strategic governance function that brings together people, processes, and technology to protect information assets, follow the rules, and keep the trust of stakeholders.

References

- [1] M. E. Whitman and H. J. Mattord, *Principles of Information Security*. Cengage Learning.
- [2] M. E. Whitman and H. J. Mattord, *Management of Information Security*. Cengage Learning.
- [3] ISO/IEC 27001:2022, *Information Security Management Systems*.
- [4] ISO/IEC 27002:2022, *Code of Practice for Information Security Controls*.
- [5] NIST, *Cybersecurity Framework*.
- [6] NIST SP 800-30, *Guide for Conducting Risk Assessments*.
- [7] NIST SP 800-61, *Computer Security Incident Handling Guide*.
- [8] ISACA, *COBIT 2019 Framework*.
- [9] EU GDPR Regulation (EU) 2016/679; UK Data Protection Act 2018.
- [10] ACCA7028 Lecture Materials (Weeks 1–9).