

Module: Data Security, Governance and Compliance
MSc Cybersecurity and Digital Forensics

**Title : Apply the principles and practices of Data security,
Governance and Compliance based on a given scenario.**

Submitted by-

MD. Mehedi Hasan Mixon

ID: 2436061

Table of Content:

Table of Content:	1
List of Figures:	2
List of Tables:	3
Abstract	4
1. Introduction	5
2. Overview of the Case Scenario	6
3. Research on Models and Frameworks for Security	7
3.1 Introduction to Security Frameworks.....	7
3.2 Information Technology Infrastructure Library (ITIL).....	7
3.3 ISO/IEC 27001	8
3.4 NIST Cybersecurity Framework (CSF)	8
3.5 COBIT Framework	8
3.6 Zero Trust Architecture	9
3.7 Comparative Overview.....	9
3.8 Justification for a Hybrid Approach.....	9
4. Designing a Security Approach for FinSure Bank	10
4.1 Proposed Hybrid Security Model	10
4.2 Security Architecture Diagram	11
4.3 Risk Management Strategy	12
4.4 Security Policies and Governance Controls	14
4.5 Technical Security Controls.....	15
5. Discussion.....	16
6. Conclusion	18
7. References	19

List of Figures:

1. Figure 1: Security architecture for FinSure Bank ----- 12
2. Figure 2: Risk management process ----- 13
3. Figure 3: Lifecycle of security policy development ----- 15

List of Tables:

1. Table –1: Key Functions of the ITIL Framework -----08
2. Table-2: Core Components of ISO/IEC 27001 ISMS -----09
3. Table-3: NIST Cybersecurity Framework Functions -----09
4. Table-4: Principle of Zero Trust Architecture -----10
5. Table-5: Comparative Analysis of Security Frameworks -----10
6. Table-6 Hybrid Security Framework Mapping for FinSure Bank ----- 11

Abstract

The financial industry has undergone tremendous change because of its growing reliance on cloud computing and digital platforms, but it has also brought forth difficult cybersecurity issues. Bring Your Own Device (BYOD) access is supported by FinSure Bank (FSB), a fast growing digital financial institution that predominantly uses cloud-based technology. These technologies improve user accessibility and operational efficiency, but they also make people more vulnerable to cyberthreats such identity theft, insider assaults, data breaches, and noncompliance with regulations. To assess their applicability in resolving FSB's security issues, this research critically analyzes well-known cybersecurity frameworks, such as ISO/IEC 27001, NIST Cybersecurity Framework (CSF), COBIT, ITIL, and Zero Trust Architecture. A hybrid security paradigm that incorporates risk management, governance, and technology measures is suggested based on this investigation. Additionally, the study creates a thorough security strategy that covers incident response planning, policy design, risk assessment, and compliance management. A critical assessment emphasizes how crucial it is to update security frameworks frequently to accommodate changing regulations and growing cyberthreats. The results indicate that in order to guarantee long-term security, compliance, and organizational resilience, FSB needs to take a dynamic, governance-driven, and risk-based strategy.

1. Introduction

The digital transformation of financial services has led to an unprecedented dependence on information systems, cloud platforms, and mobile technologies. While these advancements enable financial institutions to operate more efficiently and reach a global customer base, they also introduce significant cybersecurity risks. Financial organisations have become prime targets for cybercriminals due to the high value of the data they manage, including personal, financial, and transactional information.

FinSure Bank (FSB) is a contemporary financial institution that prioritizes digital technology and uses cloud-based platforms for nearly all of its operations. While clients communicate via mobile banking apps, the company permits workers, contractors, and other partners to access systems via personal devices. This paradigm increases accessibility and flexibility, but it also provides a complicated security environment with many possible ports of entry for attackers. The lack of a structured risk management plan, unified governance structure, and thorough compliance framework is one of the case scenario's main problems. It is challenging to properly manage cybersecurity risks, identify threats, and address incidents with this disjointed approach. Failure to put in place appropriate controls can lead to serious financial penalties, operational interruption, and reputational harm in a highly regulated industry like finance.

This report's objective is to assess current security frameworks and create a methodical strategy suited to the requirements of the FSB. It also critically examines the necessity of regular upgrades to security standards and legislation in contemporary cybersecurity contexts.

2. Overview of the Case Scenario

Offering digital banking, savings, loans, and investment services throughout several locations, FinSure Bank is a quickly expanding financial services company. With more than 90% of its systems hosted externally, the organization's infrastructure is mostly dependent on cloud platforms. This dependence makes data security more difficult and creates dependency on outside companies. Additionally, the company is under pressure to encourage BYOD access, which permits partners and staff to connect via mobile devices and personal laptops. Although this increases output, it also creates security issues like:

- Lack of control over device security
- Increased risk of malware infection
- Data leakage through unsecured endpoints

At the same time, customers are increasingly using mobile banking applications, which raises concerns regarding identity theft, fraud, and unauthorised access. The combination of cloud computing, mobile access, and BYOD significantly expands the organisation's attack surface.

The absence of structured governance and compliance mechanisms creates a critical vulnerability. Without proper policies, risk management processes, and monitoring systems, FSB is exposed to both external cyberattacks and internal threats.

3. Research on Models and Frameworks for Security

Structured approaches for risk management, asset protection, and legal and regulatory compliance are offered by cybersecurity frameworks [1]. The FSB must choose and incorporate suitable frameworks to handle its intricate security environment.

3.1 Introduction to Security Frameworks

Cybersecurity cannot be successfully managed in contemporary organizations with isolated instruments or unofficial procedures. Organizations must use structured frameworks to manage risks, safeguard data, and guarantee regulatory compliance [1]. These frameworks offer a methodical way to specify security policies, delegate tasks, and match security with business goals. This is especially crucial for FinSure Bank (FSB) because of its reliance on mobile banking, cloud infrastructure, and BYOD settings. These elements expand the attack surface and render conventional perimeter-based security inadequate. Because of this, FSB needs to implement a number of frameworks that deal with access control, operational security, and governance. This section evaluates ITIL, ISO/IEC 27001, NIST Cybersecurity Framework, COBIT, and Zero Trust Architecture in terms of their relevance to FSB.

3.2 Information Technology Infrastructure Library (ITIL)

IT service management is the focus of ITIL, which makes sure that IT systems function effectively and serve corporate goals [2]. It presents organized procedures like change management, incident management, and service enhancement.

Table-1

Key Functions of the ITIL Framework

Function	Purpose
Incident Management	Handles security incidents effectively
Change Management	Ensures secure system updates
Service Operation	Maintains daily system performance

ITIL is helpful to FSB in preserving operational stability and guaranteeing that events are handled methodically. It cannot, however, handle cybersecurity issues on its own since it lacks comprehensive security controls.

3.3 ISO/IEC 27001

A well-known standard for information security management is ISO 27001 [3]. It offers a risk-based strategy for guaranteeing compliance and safeguarding private information.

Table- 2

Core Components of ISO/IEC 27001 ISMS

Component	Description
ISMS	Structured security management
Risk Assessment	Identifies threats and vulnerabilities
Controls	Implements protection measures

The PDCA (Plan-Do-Check-Act) cycle, which guarantees ongoing improvement, is its primary strength. For FSB to develop governance, safeguard financial data, and comply with regulations, ISO 27001 is crucial. However, execution necessitates organizational commitment and might be resource-intensive.

3.4 NIST Cybersecurity Framework (CSF)

The NIST framework provides a practical and flexible approach to managing cybersecurity risks [5]. It is built around five key functions:

Table- 3

NIST Cybersecurity Framework Functions

Function	Purpose
Identify	Understand risks and assets
Protect	Apply safeguards
Detect	Monitor threats
Respond	Manage incidents

NIST is extremely helpful to FSB for operational security, particularly in SOC contexts where real-time response and monitoring are essential. Although it needs to be integrated with other frameworks, its adaptability makes it suitable for cloud-based solutions.

3.5 COBIT Framework

COBIT guarantees that IT systems are in line with business goals and concentrates on governance [6]. It establishes accountability, positions, and duties within the company. Because the existing situation demonstrates a lack of governance structure, COBIT is crucial for FSB. The organization can enhance policy enforcement, accountability, and

compliance monitoring by putting COBIT into practice. COBIT, however, can be complicated and might call for more organizational maturity.

3.6 Zero Trust Architecture

A contemporary security approach called "zero trust" is predicated on the idea that no user or device should be trusted by default [7]. Identity, device status, and context must be used to validate each access request.

Table-4

Principles of Zero Trust Architecture

Principle	Description
Identity Verification	Uses MFA and authentication
Least Privilege	Limits access rights
Continuous Monitoring	Tracks all activities

Zero Trust is very important for FSB because of its cloud-based environment and BYOD policy. It lowers the possibility of insider threats and unauthorized access. However, especially with outdated systems, implementation might be difficult.

3.7 Comparative Overview

Table-5

Comparative Analysis of Security Frameworks

Framework	Strength	Limitation	Relevance
ITIL	Improves operations	Limited security focus	Service management
ISO 27001	Strong compliance	Resource-intensive	Data protection
NIST CSF	Flexible & practical	Needs integration	SOC operations
COBIT	Governance structure	Complex	Policy control
Zero Trust	Strong access control	Requires maturity	BYOD security

3.8 Justification for a Hybrid Approach

The difficulties FSB faces cannot be adequately addressed by a single framework. Governance and compliance are provided by ISO 27001, operational security is supported by NIST, organizational alignment is guaranteed by COBIT, and access control is strengthened by Zero Trust. The FSB can create a comprehensive security plan that strikes a balance between technical protection, monitoring, and governance by combining these

principles. The complexity of contemporary cybersecurity situations can be better addressed with this hybrid approach.

4. Designing a Security Approach for FinSure Bank

4.1 Proposed Hybrid Security Model

Instead of depending on isolated controls, a structured and integrated security solution must be designed to handle the security issues seen in the FinSure Bank (FSB) scenario. The organization must combine operational security, technological enforcement, and governance to function in a highly dynamic environment that includes cloud infrastructure, mobile access, and third-party contacts.

A hybrid security model is proposed, combining ISO/IEC 27001, NIST Cybersecurity Framework, and Zero Trust Architecture. Each framework plays a distinct role within the overall system. ISO 27001 provides the foundation for governance and compliance by establishing policies, defining responsibilities, and ensuring alignment with regulatory requirements. NIST CSF supports operational activities such as threat detection, response, and recovery, making it highly suitable for real-time security management. Zero Trust Architecture strengthens access control by ensuring that no user or device is trusted by default, which is particularly important in a BYOD and cloud-based environment.

A hybrid approach is recommended, combining:

Table-6

Hybrid Security Framework Mapping for FinSure Bank

Framework	Role
ISO 27001	Governance & compliance
NIST	Detection & response
Zero Trust	Access control

Security is handled from several angles thanks to this integrated strategy. Technical protections offer security against unauthorized access, operational controls guarantee ongoing monitoring and reaction, and governance guarantees accountability and compliance. When combined, these elements provide a robust and well-balanced security structure that is suited to the requirements of the FSB.

4.2 Security Architecture Diagram

To implement the proposed approach effectively, a layered security architecture is required. This architecture ensures that multiple controls work together to protect systems and data.

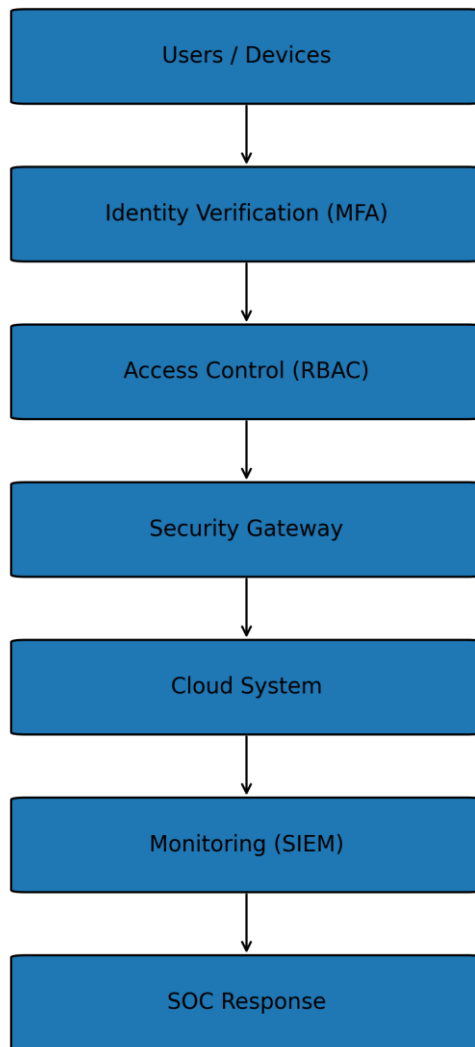


Figure 1: Security architecture for FinSure Bank

Users and devices trying to access the system are where the architecture starts. Identity verification techniques like multi-factor authentication (MFA) make sure that only authorized users are permitted before granting access. Role-based permissions are enforced by access control methods after authentication, guaranteeing that users can only access pertinent resources. Traffic then passes through a secure gateway, which includes firewalls and Zero Trust Network Access (ZTNA) controls. These components inspect and filter traffic, preventing malicious activity from reaching internal systems. The cloud banking system represents the core infrastructure where data and services are hosted. All activities

are continuously monitored through a Security Information and Event Management (SIEM) system, which collects and analyses logs in real time. Any suspicious activity is forwarded to the Security Operations Centre (SOC), where security analysts investigate and respond to incidents.

4.3 Risk Management Strategy

Finding vulnerabilities and implementing the right mitigation techniques require effective risk management. FSB should implement an organized procedure based on the NIST Risk Management Framework and ISO 27005.

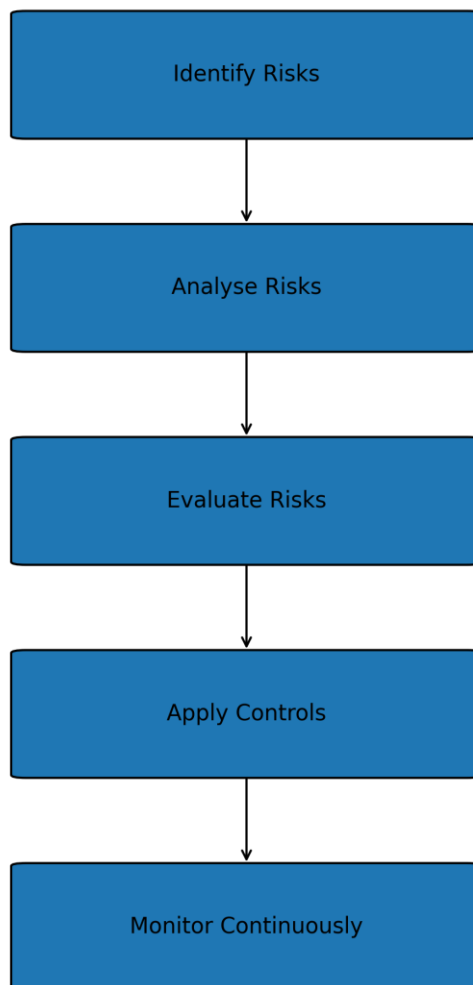


Figure 2: Risk management process

Risk identification is the first step in the process, where possible dangers including phishing, data breaches, and insider assaults are identified. After that, these risks are examined to ascertain their probability and possible effects on the company. Risks are assessed and ranked in order of severity based on this study. Appropriate controls are put in place when risks have been prioritized. These could include organizational policy, user awareness training, or technical solutions like encryption. In order to make sure that controls continue to be effective and adjust to new threats, the last stage entails ongoing monitoring. Instead of responding to issues after they happen, this methodical strategy guarantees that FSB can manage risks proactively.

4.4 Security Policies and Governance Controls

When determining how systems and data should be safeguarded, security policies are essential. Even sophisticated technology safeguards could fail in the absence of well-defined policies due to inconsistent execution or human mistake.

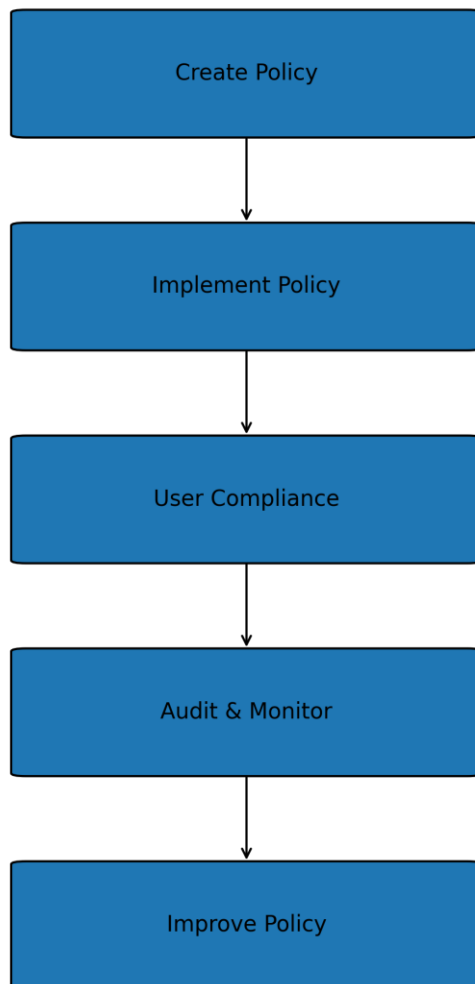


Figure 3: Lifecycle of security policy development

The first stage of the policy lifecycle is policy formulation, during which organizational demands and legal requirements are used to determine security requirements. After that, these rules are applied to all systems and procedures. These policies must be followed by users, which calls for knowledge and instruction. To make sure that policies are effectively implemented, monitoring and auditing are crucial. In order to ensure that security measures continue to be effective over time, any flaws or gaps found during audits are fixed through policy modification.

Key policies for FSB should include:

- BYOD policy (device security and access control)
- Cloud governance policy (data protection and access management)
- Access control policy (least privilege principle)
- Data classification policy (handling sensitive financial data)

4.5 Technical Security Controls

Modern technical controls must be implemented by FSB in order to support the governance framework and policies. These controls provide ongoing defense against cyberthreats and serve as the foundation of operational security. Key controls include:

- Multi-Factor Authentication (MFA) to prevent unauthorised access
- Encryption to protect data in transit and at rest
- Firewalls and intrusion detection systems to monitor network traffic
- SIEM systems for real-time log analysis
- Endpoint protection for BYOD devices

Together, these technologies provide a defense-in-depth strategy, which lowers the probability of a successful attack by using several levels of defense.

5. Discussion

The modern cybersecurity landscape is continuously evolving due to rapid technological advancements, increasing connectivity, and the growing sophistication of cyber threats. For organisations like FinSure Bank (FSB), which operate primarily through cloud-based systems and support Bring Your Own Device (BYOD) environments, these changes significantly increase both operational complexity and security risks. The case scenario clearly highlights that FSB lacks a unified governance model, structured risk management strategy, and formal compliance controls. This absence creates a fragmented security posture, making the organisation more vulnerable to cyber threats. Because of technology developments like cloud computing and artificial intelligence, cybersecurity risks are always changing [9]. Attackers are growing increasingly clever, employing cutting-edge strategies like social engineering and ransomware. Incidents in the real world show how crucial it is to update security procedures. While recent cloud breaches have highlighted the dangers of improperly designed infrastructures, the WannaCry assault revealed how older systems may be exploited [10]. Adoption of BYOD policy is another significant obstacle. Flexibility is increased when partners and workers can access systems on their own devices, but organizational control over endpoint security is greatly diminished. According to studies, unmanaged devices are more likely to have malware or inadequate security settings, which makes them perfect entry points for hackers [12]. In FSB's case, this risk is amplified because both internal users and external customers rely heavily on mobile access. Without implementing strong controls such as Zero Trust and endpoint protection, the organisation risks data leakage and unauthorised system access.

The problem is made more difficult by the increasing sophistication of cyber threats. Perimeter-based security is no longer adequate in traditional security approaches. To get beyond security measures, modern attackers employ sophisticated strategies including social engineering, ransomware, and phishing. For instance, the WannaCry ransomware assault, which affected more than 200,000 systems globally, showed how out-of-date systems and unpatched vulnerabilities may cause significant disruptions. This emphasizes a crucial point: security frameworks and controls must constantly change or they will lose their efficacy. In addition, recent incidents involving cloud service providers have shown that even well-established systems can be compromised if security controls are not regularly updated. The Microsoft Exchange breach in 2023 exposed sensitive data due to weaknesses in authentication mechanisms and key management. This case illustrates that relying solely on existing frameworks without adapting them to new threats can result in serious

consequences. For FSB, which operates in a highly dynamic digital environment, static security practices would leave the organisation exposed to similar risks.

Regulatory compliance is another critical factor that reinforces the need for continuous updates. Laws such as the General Data Protection Regulation (GDPR) impose strict requirements on how organisations collect, process, and store personal data [11]. These regulations are not static; they evolve to address emerging risks and technologies. Failure to comply can result in significant financial penalties, as seen in cases where organisations have been fined millions due to data breaches and poor security practices. For FSB, non-compliance would not only result in legal consequences but also damage customer trust, which is essential in the financial sector. Integrating new technologies like artificial intelligence and the Internet of Things (IoT) is another growing difficulty. Although these technologies have many advantages, they also bring with them new risks. For example, IoT devices can be used as attack entry points because they frequently lack strong security protections. Large-scale distributed denial-of-service (DDoS) attacks can be launched using vulnerable IoT devices, as the Mirai botnet attack showed. FSB must make sure that security considerations are incorporated from the outset rather than being an afterthought as it continues to adopt new technology.

There will probably be a number of repercussions if FSB doesn't upgrade its security frameworks and procedures on a regular basis. These include heightened susceptibility to cyberattacks, monetary losses from fraud or disruption, fines from authorities, and diminished customer trust. Trust is a vital resource in the financial industry, and any security breach may have long-term effects on one's reputation.

6. Conclusion

Considering FinSure Bank's quick digital transition and reliance on cloud-based services, this paper has critically analyzed the cybersecurity issues it faces. Due to the organization's existing lack of a formal compliance framework, organized risk management approach, and unified governance model, there are serious weaknesses that cybercriminals could exploit. It has been shown that no single framework is enough to handle every facet of contemporary cybersecurity through an analysis of well-known frameworks including ISO 27001, the NIST Cybersecurity Framework, COBIT, ITIL, and Zero Trust Architecture. Rather, a hybrid approach is needed to develop a complete security plan that combines operational controls, governance, and technical safeguards. The proposed model integrates ISO 27001 for governance and compliance, NIST for operational security and incident response, and Zero Trust for access control in cloud and BYOD environments. This combination ensures that security is addressed at both strategic and technical levels. The inclusion of structured policies, risk management processes, and monitoring systems further strengthens the organisation's ability to detect and respond to threats. However, the findings of this report also highlight that cybersecurity is not a static discipline. The rapid evolution of cyber threats, technological advancements, and regulatory requirements means that organisations must continuously adapt their security practices. FSB must regularly review and update its policies, invest in new technologies, and ensure that its workforce is equipped with the knowledge and skills required to maintain a secure environment. In addition, the importance of governance cannot be overstated. Effective governance ensures that security measures are aligned with business objectives, responsibilities are clearly defined, and accountability is maintained across the organisation. Without strong governance, even the most advanced technical controls may fail to achieve their intended purpose.

In the end, FinSure Bank's capacity to take a proactive and flexible approach to cybersecurity will determine its long-term success. In an increasingly complicated digital environment, the organization may improve its resilience, safeguard sensitive data, and uphold consumer trust by putting the suggested hybrid structure into practice, bolstering governance, and making a commitment to continuous development.

7. References

- [1] H. I. Kure, S. Islam, and H. Mouratidis, "An integrated cyber security risk management framework for critical infrastructure protection," *Neural Computing and Applications*, vol. 34, no. 18, pp. 15241–15271, 2022.
- [2] H. Gunawan, A. B. P. Irianto, and J. G. P. Negara, "Implementation of ITIL framework for sustainable service improvement in organisations," *Procedia Computer Science*, vol. 234, pp. 748–755, 2024.
- [3] O. A. Fonseca-Herrera, A. E. Rojas, and H. Florez, "A model of an information security management system based on ISO/IEC 27001," *IAENG International Journal of Computer Science*, vol. 48, no. 2, pp. 213–222, 2021.
- [4] E. Koza, "Semantic analysis of ISO/IEC 27000 and NIST cybersecurity framework," *Medicon Engineering Themes*, vol. 2, pp. 26–39, 2022.
- [5] A. Dimakopoulou and K. Rantos, "Comprehensive analysis of cybersecurity using NIST CSF," *Journal of Marine Science and Engineering*, vol. 12, no. 6, p. 919, 2024.
- [6] A. Efe, "A comparison of risk management frameworks: COSO-ERM, NIST RMF, ISO 31000 and COBIT," *Denetim ve Güvence Hizmetleri Dergisi*, vol. 3, no. 2, pp. 185–205, 2023.
- [7] S. Ghasemshirazi, G. Shirvani, and M. A. Alipour, "Zero trust: Applications, challenges, and opportunities," *arXiv preprint arXiv:2309.03582*, 2023.
- [8] A. S. C. Junior and C. H. Arima, "Cyber risk management using ISO 27005: A systematic review," *Revista Foco*, vol. 16, no. 2, pp. 1–15, 2023.
- [9] M. Shafiq, X. Yu, A. A. Laghari, and S. Memon, "IoT security threats and challenges: A review," *IEEE Access*, vol. 10, pp. 123–145, 2022.
- [10] P. Shrivastava and A. Agrawal, "Cloud security challenges and risk mitigation strategies," *Journal of Cloud Computing*, vol. 13, no. 1, pp. 1–15, 2024.
- [11] W. N. Khan and S. Naseeb, "Personal data protection in the era of big data: Navigating privacy laws and consumer rights," *Mayo Communication Journal*, vol. 1, no. 1, pp. 41–51, 2024.
- [12] R. Palanisamy, A. A. Norman, and M. L. Mat Kiah, "BYOD security risks and policy compliance in organisations," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 61–72, 2022.

- [13] O. Ilori, N. T. Nwosu, and H. N. Naiho, "Third-party vendor risks in IT security: A comprehensive audit review," *World Journal of Advanced Research and Reviews*, vol. 22, no. 3, pp. 213–224, 2024.
- [14] C. Harper, "Role-based access control and encryption techniques for database security," *International Journal of Cybersecurity Research*, vol. 5, no. 2, pp. 45–60, 2025.
- [15] P. S. Mrudula et al., "Intrusion detection systems with privacy protection and firewall integration," *IEEE Access*, 2025.