



Data Security Strategy: FinSure Bank

Student Name: Mohammad Lakhi

Student ID: 2512430

Subject Code: ACCA7028

Subject Name: Data Security, Governance and Compliance

University of Wales Trinity Saint David

Date: 2nd March 2026

Abstract

This report evaluates the information security, governance, and compliance requirements of FinSure Bank(FSB), a digital-first financial provider that operates almost entirely on cloud-based platforms. The study presents a systematic review of the ISO/IEC 27001 and ITIL 4 frameworks to address the bank's fragmented security posture as well as the risks associated with unmanaged Bring Your Own Device(BYOD). A custom security architecture is created using Zero Trust principles, including Secure Access Service Edge(SASE) and Ensemble Access Control Frameworks(EACF), to provide granular protection for sensitive financial records. Furthermore, the report examines the strategic importance of Continuous Service Improvement(CSI) and dynamic regulatory updates in maintaining resilience in an evolving threat landscape. The proposed governance model ensures that the FSB maintains regulatory compliance while pursuing its goal of rapid, secure digital expansion.

TABLE OF CONTENTS

1	Introduction	1
2	Research on Security Frameworks	4
3	Design of the Bespoke Security and Governance Approach	6
4	Critique and Analysis of Security Regulations and Standards	9
5	Conclusion	14
	REFERENCES	15

Chapter 1

Introduction

The modern financial sector is increasingly characterized by a rapid shift toward digital-first models, in which organizational success is dependent on the seamless availability of internet-based information. For institutions like FinSure Bank, this paradigm shift makes it a significant reliance on external cloud-based platforms, which host more than 90% of institutional infrastructure. However, the widespread use of digital connectivity exacerbates the threat landscape, exposing high-value information assets to attacks by global criminal entities and sophisticated actors. Establishing a strong security posture is crucial for business continuity, not just a technical requirement [5].

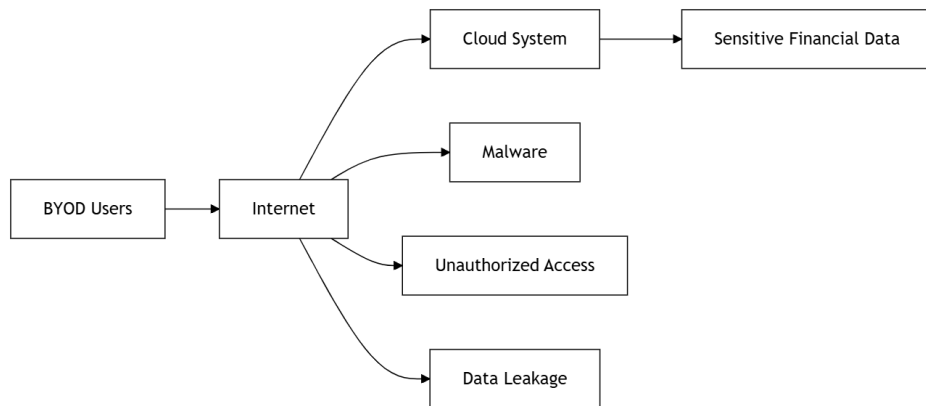


Figure 1.1: FinSure Bank Cloud and BYOD Security Context

FSB’s organizational expansion has created immediate pressures to enable Bring Your Own Device (BYOD) access for employees, contractors, and third-party partners. While such policies improve operational flexibility and collaboration, they also raise serious concerns about data privacy, identity theft, and unauthorized access via unmanaged endpoints. Current research shows that these vulnerabilities are frequently exploited by intruders to facilitate data exfiltration. Addressing the gap between security intention and actual policy compliance is crucial for protecting sensitive financial

records and maintaining a competitive market position [1][2].

Currently, the security infrastructure within the FSB is described as fragmented, with no unified governance model, formal risk management strategies, or structured compliance audits. This deficiency is especially concerning given the sensitivity of the financial and personal information being processed. To mitigate these risks, the organization must implement a "security-in-depth" strategy that includes technological advancements in cloud access as well as strong governance frameworks. This report will evaluate and propose a design that integrates identity management and proactive threat detection to ensure comprehensive regulatory compliance [5][10].

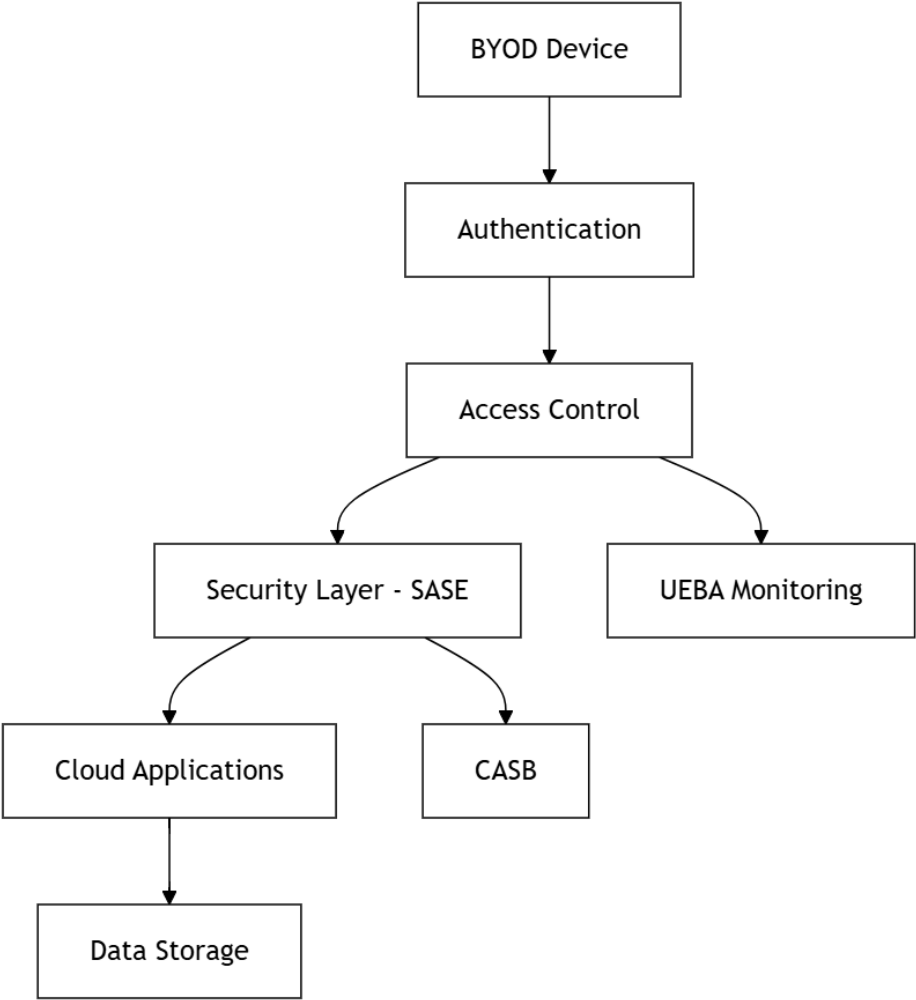


Figure 1.2: Proposed Zero Trust Cloud Security Architecture

Furthermore, the FSB’s lack of comprehensive security policies and compliance controls

demonstrates a critical gap in organizational governance. To protect financial records and intellectual property, effective security management must incorporate formal risk management strategies and structured auditing procedures. High-level security governance must include the implementation of Internal Controls and Audit (ICA) functions, which may include selective encryption and hierarchical key management to protect data in the cloud. This report will research established frameworks to design a bespoke security and compliance approach that mitigates insider threats while aligning with regulatory requirements such as GDPR [8][9].

Threat	Description
Malware	Malicious software that can compromise devices and data integrity.
Data Leakage	Exposure or unauthorized transmission of sensitive organizational data.
Unauthorized Access	Access to systems or data without proper authentication or authorization.
Device Loss	Loss or theft of personal devices leading to potential data breaches.
Untrusted Network	Use of insecure public networks increasing vulnerability to attacks.

Table 1.1: BYOD Security Threats

Chapter 2

Research on Security Frameworks

The establishment of an Information Security Management System (ISMS) based on the ISO/IEC 27001 standard is a critical requirement for securing FinSure Bank's (FSB) decentralised assets. According to research, an ISMS designed specifically for data center environments offers a systematic approach to identifying and managing risks such as information theft and unauthorized access. Implementing the "people, process, and technology" concept allows the bank to protect the confidentiality, integrity, and availability of its sensitive financial records. This framework, using the 21 controls of the ISO 27001 Annex A standard, provides a stronger defense than generalized governance models used in other sectors [11].

Furthermore, this ISMS framework provides a critical baseline for conducting structured security audits and determining the maturity level of technical implementations. For a digital-first organization like FSB, the ability to protect both physical and logical assets is critical to maintaining stakeholder trust and business continuity. Integration of these controls enables management to proactively mitigate threats while also providing a verifiable standard for regulatory compliance. Adopting a specialized ISO 27001-based model addresses the current lack of formal risk management and fragmented policy enforcement within the bank's external cloud infrastructure [11].

The Information Technology Infrastructure Library (ITIL) complements the ISMS's technical controls by providing a common framework for IT Service Management (ITSM) that aligns business requirements with IT delivery. Implementing ITIL at the service operation and Continual Service Improvement (CSI) stages enables the FSB to maintain high quality standards while scaling its digital services. This approach entails developing formal incident and problem management workflows, which are required to manage system events and maintain operational stability. Research shows a direct

link between system quality and user satisfaction, making this framework crucial for competitive digital banking [12].

The use of CSI within the ITIL framework ensures that security and service quality are not static, but rather constantly improved through data collection and analysis. For the FSB, this provides a structured approach to addressing vulnerabilities and adapting to growing concerns about identity theft and online fraud. By focusing on service quality and user experience, the bank can create a security culture that will allow it to expand rapidly across multiple countries. This dual framework approach combines the strict requirements of ISO 27001 with the service excellence of ITIL to establish the comprehensive governance and compliance structure required for high-risk financial environments [12].

Strategic Justification: ISO 27001/ITIL vs Alternatives

For several strategic reasons, the combination of ISO 27001 and ITIL 4 was preferred over alternatives such as NIST CSF or COBIT.

- **Global Certification vs Voluntary Guidelines:** Unlike the NIST Cyber security Framework, which is primarily a voluntary US-centric program development guide, ISO 27001 is a globally recognized, certifiable standard. A bank's ability to provide a ISO 27001 Certified badge is essential for gaining international stakeholder trust [11].
- **Operational Detail vs High Level Governance:** While COBIT is an excellent high-level enterprise governance tool, it lacks the granular how to service delivery focus of ITIL 4. The combination of ISO and ITIL ensures the FSB has a complete security lifecycle from risk assessment to daily service improvement [12].
- **UK Market Alignment:** In the UK and EU financial sectors, ISO 27001 is the gold standard that regulators require. It is possible to map NIST CSF to ISO, but starting with ISO ensures the FSB meets the financial sector's strict compliance requirements from day one [11].

Chapter 3

Design of the Bespoke Security and Governance Approach

The proposed security architecture for FinSure Bank (FSB) follows a "Security by Design" philosophy, which ensures that governance is not an afterthought, but rather integrated into the core of the digital infrastructure. This design, which prioritizes the integration of People, Process, and Technology, provides a scalable roadmap for securing the bank's decentralized assets.

The proposed security architecture for FinSure Bank uses a Zero Trust Multi-Cloud Governance approach to consolidate the bank's current fragmented security posture. This design is based on the assumption that FSB is a fast growing, mid-sized financial institution with the resources to invest in a Secure Access Service Edge model. By switching from a perimeter-based defense to a SASE architecture, the bank can ensure that security policies are dynamically enforced at the edge where users, devices, and applications are located. This transition is crucial for securely facilitating the bank's transition to a Bring Your Own Device (BYOD) policy while protecting internal systems from unauthorized access [4].

Centralized management is achieved by deploying multi-cloud orchestration tools like Azure Arc, which act as a unified control plane for the bank's diverse external infrastructure. This model automates vulnerability scanning, incident response, and policy enforcement across all cloud platforms, ensuring a proactive and consistent approach to risk management. Furthermore, implementing a Cloud Access Security Broker provides the required visibility into the traffic of unmanaged personal devices, allowing for the consistent application of organizational security standards. This unified management strategy addresses the bank's current deficiencies in formal risk oversight and

regulatory compliance [7].

To safeguard the confidentiality of sensitive financial records, the design incorporates an Ensemble Access Control Framework, which provides granular access control for all data stored in the cloud. This technical layer is enhanced by hierarchical selective encryption, which creates a self-protection layer for data and audit reports, ensuring privacy even when data is processed by third party providers. Furthermore, the implementation of User and Entity Behavioral Analytics employs analytical methods to detect anomalous patterns of behavior, providing an important safeguard against identity theft and internal security threats. The FSB's bespoke design prioritizes information security while allowing for rapid digital expansion [8][10].

Technical Implementation Details

- **Micro segmentation and Lateral Movement:** The architecture makes use of micro segmentation in the cloud. By dividing the network into smaller, isolated zones, the bank can prevent an attacker from moving laterally between different financial applications if one account becomes compromised. This is a crucial defense for distributed cloud environments [5].

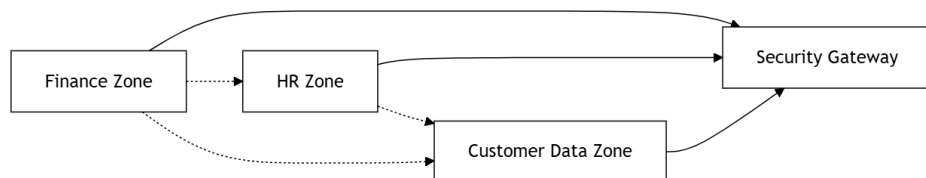


Figure 3.1: Micro Segmentation Security Model

- **Human Centric Security Governance:** Recognizing that the "People" element poses a significant risk in a BYOD environment, the design incorporates an automated Security Awareness and Training program. This ensures that employees and contractors understand their responsibilities under the new governance framework, lowering the risk of accidental data leaks or social engineering successes [1].
- **Resilient Incident Response Lifecycle:** The design incorporates the ITIL 4 Continual Service Improvement model and the bank's incident response protocols.

This ensures that every security incident is analyzed to identify the root cause, and the results are fed back into the governance board to automatically update policies and technical controls [12].

- **Strategic Compliance Mapping:** By aligning the technical controls of the SASE and EACF models with the specific requirements of ISO 27001 Annex A, the bank ensures that it is always "audit-ready". This document provides a clear path for meeting GDPR and other international financial regulations, which is essential for maintaining stakeholder trust during global expansion [11].

Chapter 4

Critique and Analysis of Security Regulations and Standards

The dynamic nature of the global threat landscape necessitates that financial institutions like FinSure Bank (FSB) evolve beyond static security models. As technology advances and new vulnerabilities emerge, particularly in the BYOD context, existing policies can quickly become obsolete, creating loopholes that cyber intruders can exploit to infiltrate sensitive data. As a result, the practice of constantly updating regulations is critical to ensuring that an organization's defensive posture remains resilient to emerging cyber threats. The FSB can maintain a healthy and competitive cloud security posture by staying vigilant to regulatory developments [1][5].

Furthermore, the shift to multicloud environments exposes inherent flaws in traditional computing practices, resulting in the need for more sophisticated security governance. Legacy standards frequently fail to address the unique interoperability and identity management challenges of shared infrastructure, making the adoption of cloud-native regulations a strategic imperative. These updates enable organizations to bridge the gap between security intentions and actual behavior, thereby providing a structured foundation for achieving the appropriate level of assurance. For a digital first entity like FSB, this iterative refinement of standards is critical for maintaining the confidentiality and integrity of highly sensitive financial records [9][5].

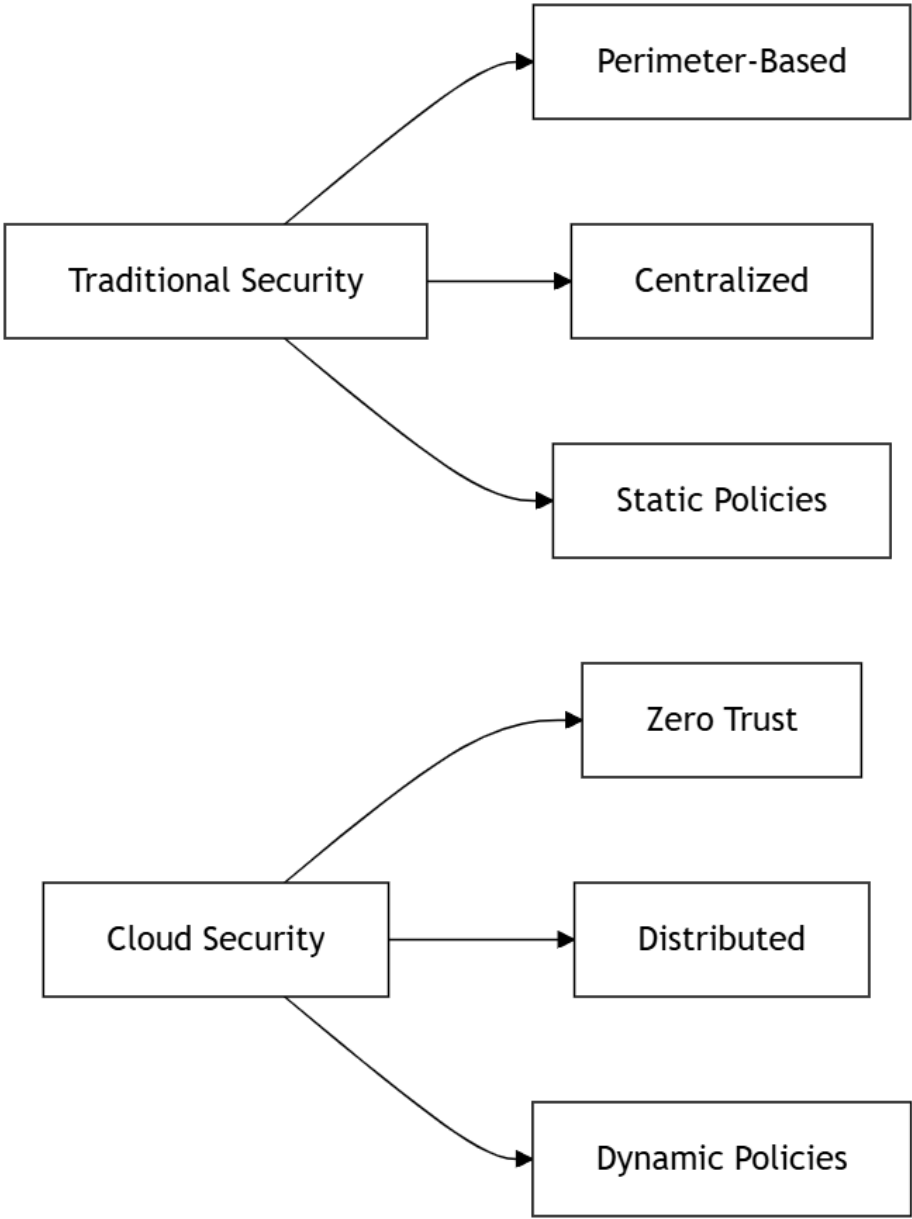


Figure 4.1: Comparison of Traditional and Cloud Security Models

Finally, the introduction of frameworks such as ITIL 4 demonstrates that security governance should be approached as a continuous cycle rather than a one time implementation. Organizations can use Continuous Service Improvement(CSI) to measure and assess their IT services to ensure they meet current quality and security standards. This constant evaluation enables the identification of technological and infrastructure issues that may have an impact on user satisfaction and data security. Commitment

to updated regulations fosters a security aware culture, supporting business continuity and long term institutional growth in a rapidly evolving digital market [12][11].

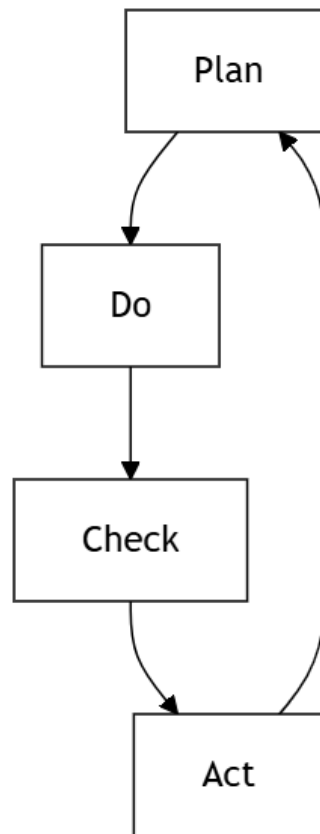


Figure 4.2: Continuous Security Governance Lifecycle

Review of Legacy Standards in Distributed Environments

The primary criticism raised at traditional security standards is their failure to account for the shared responsibility model inherent in cloud computing. Legacy frameworks were intended for on-premise data centers in which the organization had complete physical and logical control. For FSB, which is 90% cloud hosted, these static standards create a governance gap.

- **Interoperability Failures:** Traditional regulations frequently lack a level required to manage identity across multiple cloud providers (AWS vs Azure) resulting in fragmented access controls.
- **Shared Multi-Tenant Risk:** Research suggests that the potential for data

breaches increases in shared environments because legacy standards do not mandate the specific security in depth layers required for cloud isolation [5].

- **Audit Deficiencies:** Internal audits continue to focus on hardware rather than the logic-based software defined networks used by the FSB, leading to a false sense of security [8].

The Systematic Necessity for Regulatory Evolution

A careful examination of the ISO 27001 framework reveals that compliance is a process rather than a destination. The Plan Do Check Act(PDCA) methodology necessitates that an ISMS be constantly audited and improved.

- **Reactive vs Proactive Evolution:** Static regulations change only when a breach occurs. Updated standards enable the FSB to detect weak signals of emerging threats, like new identity theft methods, before they are exploited [2][11].
- **Aligning with Customer Expectations:** In the financial industry, customer trust is linked to data privacy. As global standards like GDPR evolve, FSB's internal regulations must adapt to maintain legal compliance and avoid catastrophic fines associated with regulatory non-compliance [3].
- **CSI Feedback Loop:** By implementing ITIL 4's Continuous Service Improvement, FSB can transform security from a technical cost to a business value. By constantly refining standards, the bank ensures that security measures do not hinder operational speed, but rather facilitate safe and rapid expansion [12].

Addressing the 'Human Perimeter' through Policy Adjustment

- **Behavioral Economics in Security:** According to BYOD research, employees frequently find strict, outdated security policies cumbersome, prompting them to bypass controls. Updating regulations to be user centric, while maintaining technical rigor leads to higher compliance rates [1].

- **Mitigate insider threats:** updated standards must include User and Entity Behavioral Analytics(UEBA). To detect compromised accounts in real time, modern regulations must focus on how the user is behaving, rather than just what they are allowed to do [10].
- **Closing the Loophole in BYOD:** The rapid shift to remote work has revealed flaws that were not present three years ago. Continuous updates ensure that new types of devices and third party applications are brought under the bank's governance umbrella immediately [1][9].

Chapter 5

Conclusion

Finally, the secure digital expansion of FinSure Bank(FSB) is dependent on the successful integration of robust governance frameworks and advanced technical architectures. By transitioning from its current fragmented security posture to an ISO 27001 based unified Information Security Management System (ISMS), the bank will be able to manage the risks associated with its cloud centric infrastructure systematically. This study demonstrates that a bespoke approach incorporating the concepts of people, process, and technology is essential for protecting the confidentiality, integrity, and availability of sensitive financial records within multi-tenant data centers [11].

The proposed design uses Zero Trust principles and Secure Access Service Edge (SASE) to enable secure BYOD access for a diverse workforce while reducing the risk of identity theft and unauthorized access. Furthermore, the use of ITIL 4 standards ensures that service quality and security are maintained through a cycle of continuous service improvement (CSI). By adopting these internationally recognized standards and remaining proactive in responding to regulatory updates, the FSB can achieve the maturity required to protect its information assets. Finally, this comprehensive governance and security strategy provides the resilient foundation required for the bank to sustain its rapid global growth and maintain stakeholder trust in the digital-first financial market [4][12].

References

- [1] C. Hai Goh and A. Ping Teoh, “Determining Bring Your Own Device (Byod) Security Policy Compliance Among Malaysian Teleworkers: Perceived Cybersecurity Governance as Moderator,” *IEEE Xplore*, Nov. 01, 2021. 10.1109/ICITISEE53823.2021.9655895
- [2] C. I. Eke and A. Norman Anir, “Bring Your Own Device (BYOD) Security Threats and Mitigation Mechanisms: Systematic Mapping,” *IEEE Xplore*, Nov. 01, 2021. <https://ieeexplore.ieee.org/document/9791907>
- [3] D. Tayouri; S. Hassidim; E. Bremier; A. Smirnov; P. A. Shabtai, ”CyberSecurity Standards for Cloud Access - Version 2,” in *CyberSecurity Standards for Cloud Access* , vol., no., pp.1-18, 22 Feb. 2022.
- [4] D. Tayouri, S. Hassidi,; A. Smirnov, A. Shabtai, ”Cybersecurity in Agile Cloud Computing–Cybersecurity Guidelines for Cloud Access,” in *Cybersecurity in Agile Cloud Computing–Cybersecurity Guidelines for Cloud Access* , vol., no., pp.1-36, 28 Sept. 2022.
- [5] S. Naik, “Cloud-Based Data Governance: Ensuring Security, Compliance, and Privacy,” *The Eastasouth Journal of Information System and Computer Science*, vol. 1, no. 01, pp. 69–87, Aug. 2023, doi: <https://doi.org/10.58812/esiscs.v1i01.452>.
- [6] N. S. Musa, T. Murugan, N. A. N., and N. M. Mirza, “Research study on securing the cloud: utilizing conventional and blockchain-based access control mechanisms,” *Journal of Cloud Computing*, vol. 14, no. 1, Dec. 2025, doi: <https://doi.org/10.1186/s13677-025-00803-3>.
- [7] A. Yeboah-Ofori, A. Jafar, Toluwalaju Abisogun, I. Hilton, W. Oseni, and A. Musa, “Data Security and Governance in Multi-Cloud Computing Environment,” pp. 215–222, Aug. 2024, doi: <https://doi.org/10.1109/ficloud62933.2024.00040>.
- [8] S. De, S. Foresti, Stefano Paraboschi, and Pierangela Samarati, “Enforcing Corporate Governance Controls with Cloud-based Services,” *IEEE Transactions on Services Computing*, vol. 17, no. 6, pp. 3583–3596, Aug. 2024, doi: <https://doi.org/10.1109/tsc.2024.3451179>.
- [9] H. Wittti, C. Ghedira-Guegan, E. Disson, and K. Boukadi, “Security Governance in Multi-cloud Environment: A Systematic Mapping Study,” *IEEE Xplore*, Jun. 01, 2016. <https://ieeexplore.ieee.org/abstract/document/7557398>
- [10] J. B. Madavarapu, R. K. Yalamanchili, and R. C. B. Madavarapu, “Enhancing Access Control Mechanisms for Data Stored in Cloud Computing,” 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), vol. 13, pp. 766–773, Jan. 2024, doi: <https://doi.org/10.1109/icmcsi61536.2024.00119>.

- [11] D. Achmadi, Y. Suryanto, and K. Ramli, “On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center,” IEEE Xplore, May 01, 2018. <https://ieeexplore.ieee.org/document/8471700> (accessed Nov. 10, 2021).
- [12] H. Gunawan, Aloysius Bagas Pradipta Irianto, and J. Galih, “IMPLEMENTATION OF SUSTAINABLE SERVICE IMPROVEMENT IN ORGANIZATIONS USING FRAMEWORK INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL),” *Procedia computer science*, vol. 234, pp. 748–755, Jan. 2024, doi: <https://doi.org/10.1016/j.procs.2024.03.061>.