



LEVEL 7 ASSESSMENT SPECIFICATION

Programme: MSc Cybersecurity and Digital Forensics

Module: Data Security, Governance and Compliance

Module code: ACCA7028

Lecturer: Dr Ayman El Hajjar

Student Name: Yaskumar Jiteshbhai Bhingradiya

Student ID: 2528447

Abstract

The objective of this report is to design an integrated information security governance framework for AeroLink Logistics (ALL) to meet the increasing challenges of cyber security, governance and compliance from Cloud computing, Artificial Intelligence (AI), Internet of Things (IoT) technologies, remote working and outsourcing to third parties. The study ultimately provides a critical evaluation of leading information security frameworks; it will include the NIST Cybersecurity Framework (CSF) 2.0, ISO/IEC 27001, COBIT 2019, ITIL 4, and Zero Trust Architecture against strengths, weaknesses and organisational fit. A new integrated framework for enhancing governance, risk management, regulatory compliance, vendor security, business continuity, incident response capabilities is proposed based on these results. The scheme is expected to enhance cyber resilience, optimize efficiency of operations, enable regulatory compliance, mitigate security risks and enhance confidence of stakeholders by ensuring continuous improvement of security and good governance.

Table of Contents

1. Introduction.....	4
1.1 Background.....	4
1.2 Problem Statement.....	4
1.3 Report Structure.....	5
2. Organisation Background and Case Analysis.....	6
2.1 Company Overview.....	6
2.2 Current Security Challenges.....	6
2.3 Assumptions.....	7
3. Literature Review: Information Security Frameworks and Models.....	8
3.1 Information Security Governance.....	8
3.2 NIST Cybersecurity Framework.....	9
3.3 ISO/IEC 27001 and ISO/IEC 27002.....	10
3.4 COBIT 2019.....	11
3.5 ITIL 4.....	12
3.6 Zero Trust Architecture.....	13
3.7 Shared Responsibility Model (Cloud).....	14
3.7 Critical Comparison of Frameworks.....	14
4. Design of an Integrated Security Governance Framework.....	16
4.1 Framework Design Principles.....	16
4.2 Proposed Integrated Framework.....	17
4.3 Governance Structure.....	18
4.4 Risk Management Framework.....	19
4.5 Security Policies and Access Control.....	20
4.6 Vendor Security Management.....	20
4.7 Business Continuity and Incident Response.....	21
4.8 Data Protection and Compliance Mapping.....	21
5. Critical Discussion: Continuous Updates to Regulations and Standards.....	22
6. Conclusion and recommendations.....	23
References.....	25

1. Introduction

1.1 Background

Utilizing cloud computing for digital transformation, organisations highlight the AI, and Internet of Things (IoT) technology to achieve operational efficiency across innovation [7]. Enhancing technology highlighting the attack surface for cybercriminals has been expanded through the cloud computing system. The risks of ransomware attacks, data breaches, and unauthorised access are increased [34]. With the laws and regulations, effective information security governance helps to protect the enterprise-critical information and digital assets cyber resilience, risk management.

1.2 Problem Statement

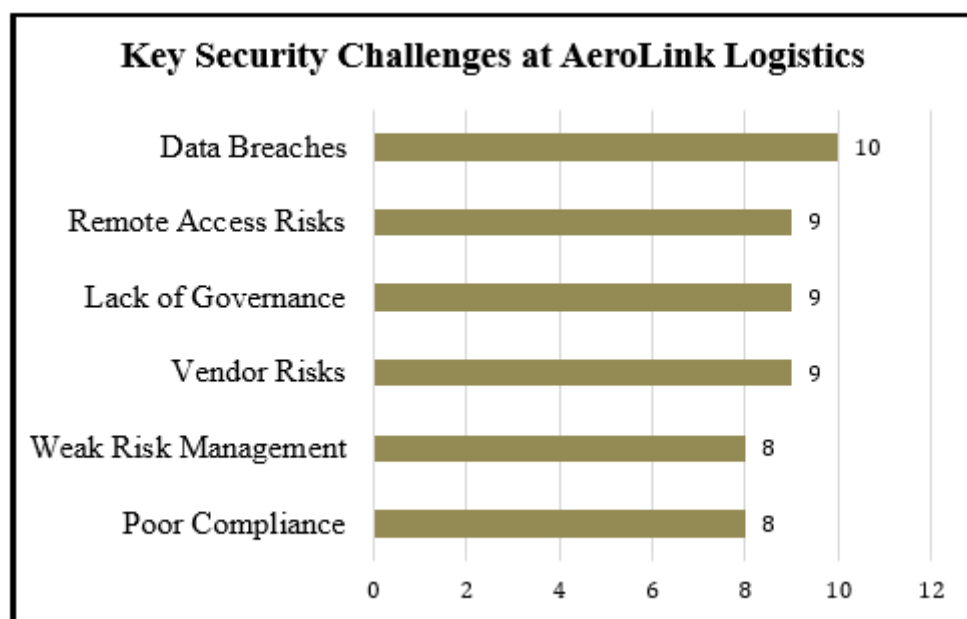


Figure 1: Key Security Challenges at AeroLink Logistics

(Source: Self-developed)

AeroLink Logistics (ALL) is an international logistics company that utilizes cloud computing, machine learning-powered analytics, connected devices for tracking, and third-party IaaS and SaaS providers for operations globally. The organisation faces immense challenges in cybersecurity, which includes repeated breaches of data, vendor security

management and governance weaknesses among others [52]. Similarly, the absence of formal compliance with GDPR, ISO/IEC 27001 and others has caused increased operational and regulatory risks. Thus, there is a need for a robust Integrated Security Governance and Compliance Framework to strengthen resilience, accountability and continuous risk management.

1.3 Report Structure

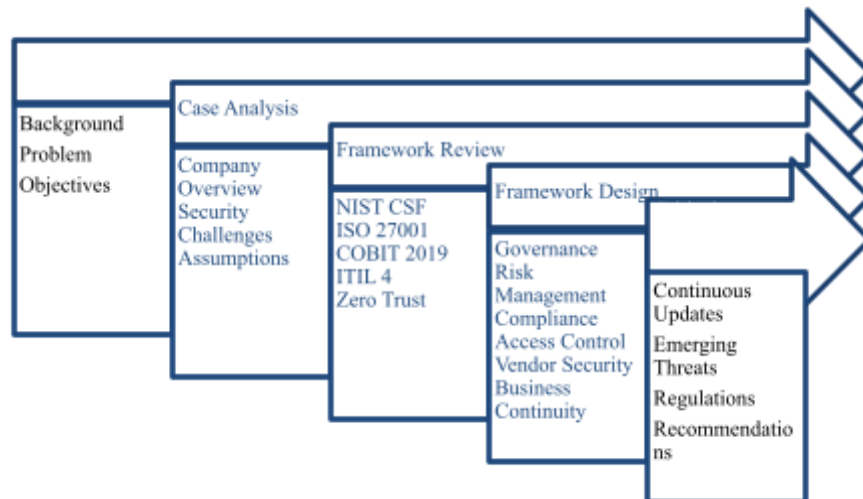


Figure 2: Structure of Report

(Source: Self-developed))

The report first reviews leading information security frameworks NIST CSF, COBIT 2019, ITIL, ISO/IEC 27001, before proposing an integrated security, governance, and compliance framework for AeroLink Logistics (ALL). Therefore, this report critically evaluates the significance of constant updating security standards and regulations to identify the emerging technologies, evolving cyber threats for meeting with the global compliance requirements

2. Organisation Background and Case Analysis

2.1 Company Overview



Figure 3: AeroLink Logistics Digital Operations Overview

(Source: Self-developed)

AeroLink Logistics (ALL) is a multinational supply chain and logistics company that provides real-time tracking, warehousing and distribution services to its global clients. The organization uses cloud computing through IaaS and SaaS to achieve operational efficiency and better customer service [48]. Around 88% of its IT infrastructure is third-party dependent. Monitoring of shipments is supported by IoT sensors lead to highlight the AI analytics has helped in demand forecasting, routing, and operational decisions. Consistent. To securely access business applications, operations help employees, suppliers and logistics partners from different geographic locations [44].

2.2 Current Security Challenges

AeroLink Logistics has some governance and cyber security issues though it has a strong digital structure. Organizations expose themselves in data breaches, service disruptions, and misconfigured cloud environments when organizations are relied heavily on cloud platforms,

[45]. As IoT-enabled tracking devices can be exploited for unauthorized access, devices create additional attack vectors to the network [25]. Contract risk exposures have required heightened oversight which is relying on third-party vendors about supply chain and [21].

2.3 Assumptions

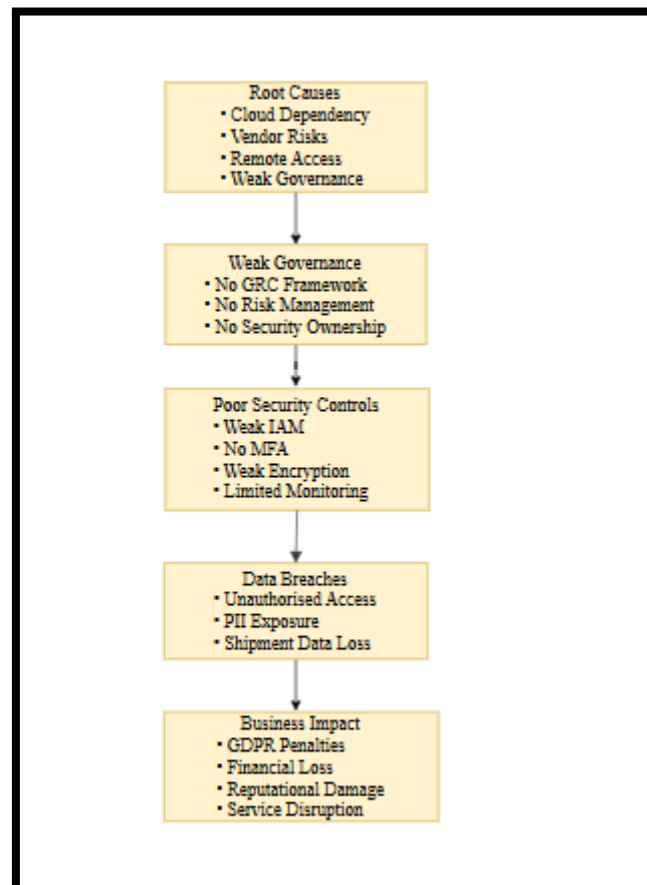


Figure 4: Problem Tree Analysis of AeroLink Logistics Security Challenges

(Source: Self-developed)

Assumptions have been made, which are all based on the information given in the case scenario to support the analysis and proposed security framework *[refer to Appendix-A]*. AeroLink Logistics (ALL) is assumed to be a large multinational organisation headquartered in the UK that has a moderate budget for cybersecurity [12]. It also has a hybrid workforce. The organisation is assumed to use Microsoft Azure cloud services, have a developing security maturity, process personal data that is subject to GDPR and not yet obtain ISO/IEC 27001 certification [10].

3. Literature Review: Information Security Frameworks and Models

3.1 Information Security Governance

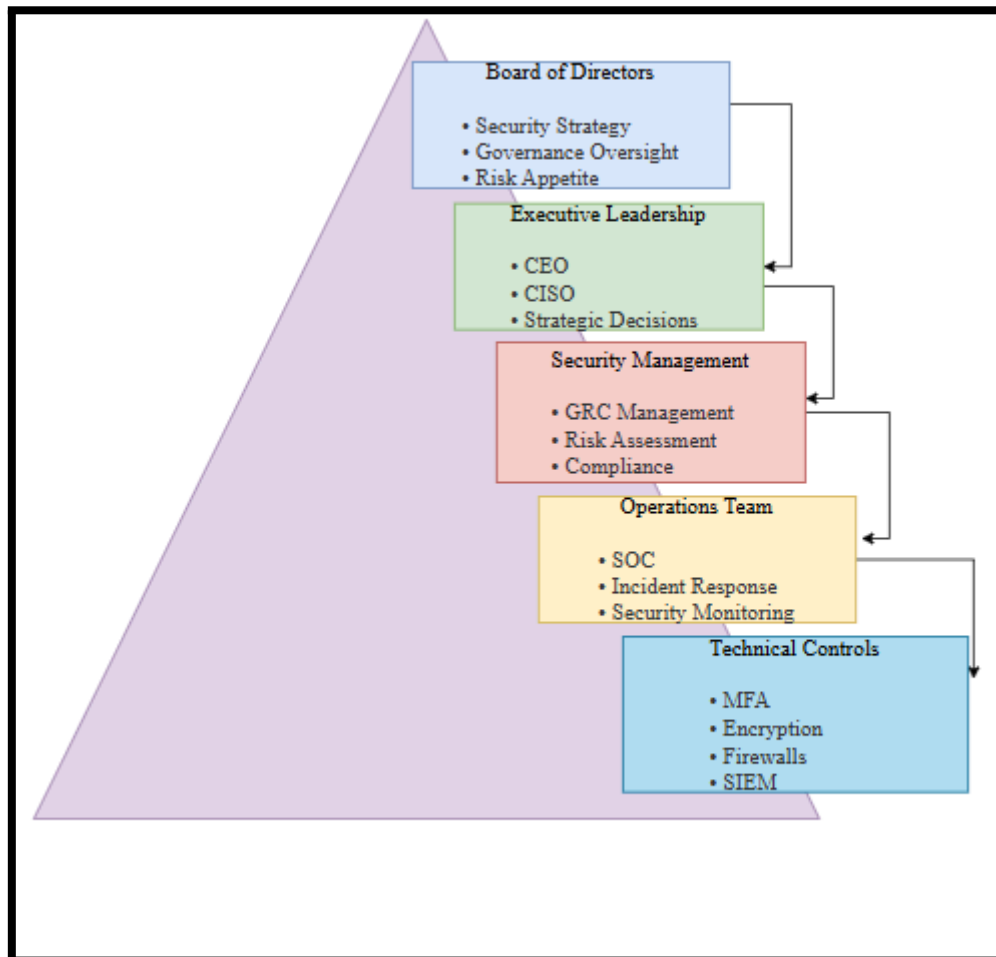


Figure 5: Security Governance Pyramid

(Source: Self-developed)

The governance of information security ensures that the organization's cybersecurity strategies align with its processes, compliance, and risks [31]. Governance, Risk and Compliance (GRC) provides a structured approach to identify, assess and mitigate information security risks, and comply with relevant laws and standards such as the GDPR and ISO/IEC 27001 [24]. Effective governance requires that the Board of Directors actively oversee things to ensure security policy establishment, risk appetite definition, resource allocation, and monitoring organisational performance. As depicted in Figure 5, security responsibilities flow down from strategic leaders to executive managers, operational teams and technical controls, creating accountability and building national cyber resilience.

3.2 NIST Cybersecurity Framework

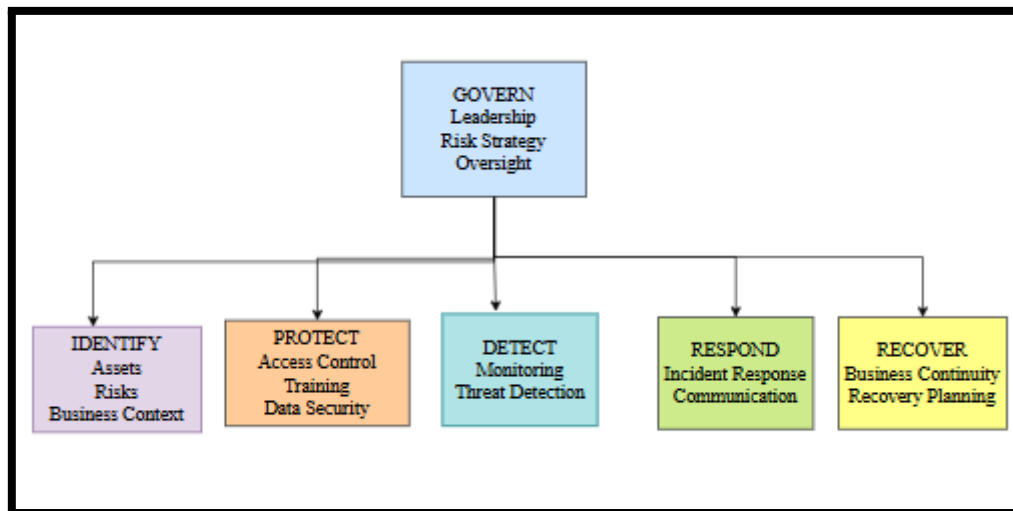


Figure 6: NIST Cybersecurity Framework (CSF) 2.0

(Source: Self-developed)

The NIST Cybersecurity Framework (CSF) 2.0 allows a flexible and risk-based approach to organisations' cybersecurity [51]. The new Govern function mandates leadership oversight and accountability, along with a cybersecurity and risk strategy. The other functions such as Identify, Protect, Detect, Respond and Recover in an organisation guide it through cyber risks during the whole of the security life cycle. A framework's flexibility, scalability and compatibility with other standards such as ISO/IEC 27001 standard) are some of its strengths [41]. However, the fact that the framework is not certifiable, and its implementation by an organization would require in-house expertise, are its weaknesses. After the Colonial Pipeline ransomware attack (2021), several organisations embraced the principles of NIST CSF to enhance their governance, incident response and cyber resilience [14]. The NIST CSF offers a sound basis for setting up a cybersecurity governance framework for AeroLink Logistics.

3.3 ISO/IEC 27001 and ISO/IEC 27002

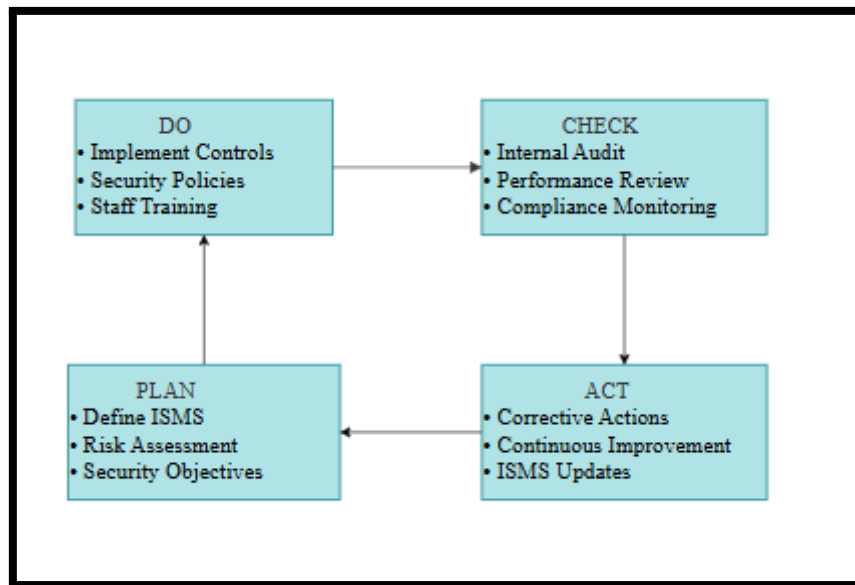


Figure 7: ISO/IEC 27001 PDCA Cycle

(Source: Self-developed)

An Information Security Management System (ISMS) is the establishment of ISO/IEC 27001 which allows the information risk across the organizations in a systematic way [26]. Plan Do Check Act or PDCA cycle supports regular assessments of risks, application of security controls, and ongoing performance evaluation [42]. By covering access control, cryptography, asset management, incident management, the standard ISO/IEC 27002 provides guidance on the implementation of the Annex A security controls [40]. AeroLink Logistics can implement a governance framework with the help of ISO/IEC 27001 which strengthens security and compliance and enhances organizational resilience.

3.4 COBIT 2019

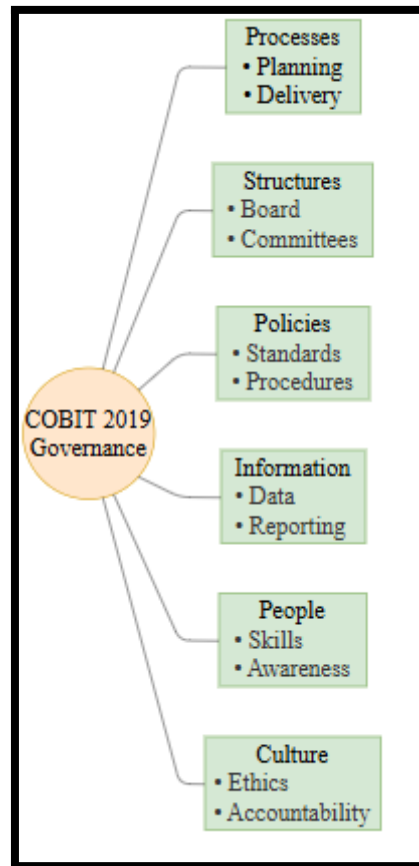


Figure 8: COBIT 2019 Governance System Components

(Source: Self-developed)

COBIT 2019 is a framework for enterprise IT governance, which ensures the information technology is in sync with the goals of the organization through governance and performance management [29]. This will help managers make more strategic decisions about the governance structure, allocation of responsibilities and performance measures. The framework strengthens organizational accountability, enhances IT investments, and mitigates risks [46]. As a foundation for governance the CobiT 2019 serves complements the AeroLink Logistics to enhance strategic management and organisational accountability.

3.5 ITIL 4

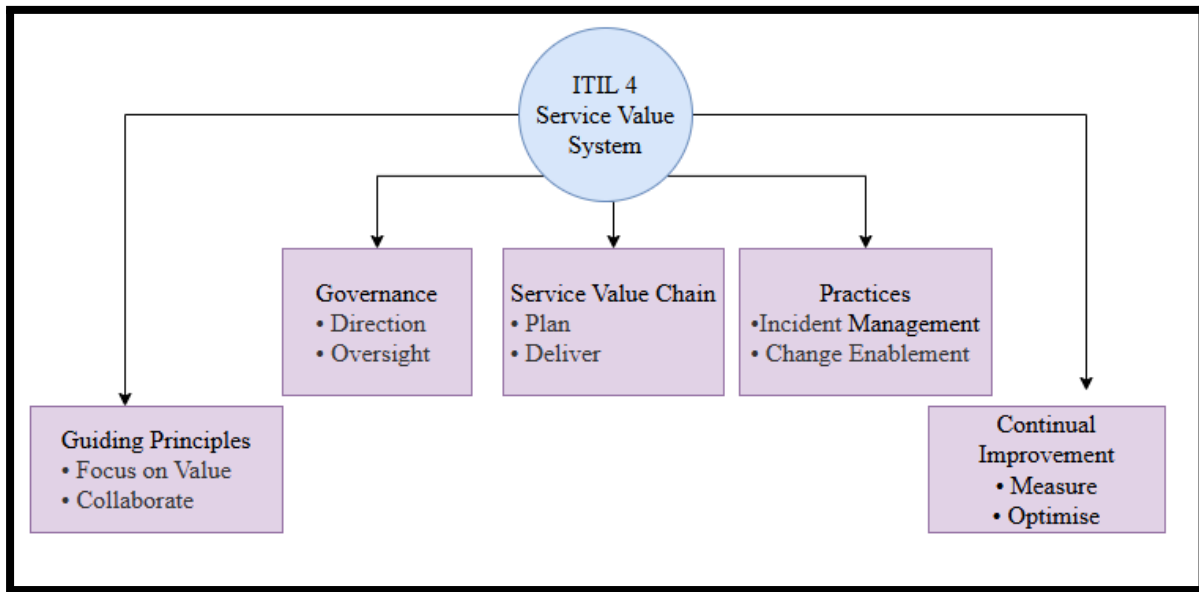


Figure 9: ITIL 4 Service Value System

(Source: Self-developed)

In integrating governance and the complete value of their IT services, ITIL 4 is a service management framework which supports organizations to achieve secure and reliable IT service management [9]. To minimize service disruption and business continuity, the framework helps to gain effective incident management. The service value streams manage operations to help to give service delivery effectiveness and customer satisfaction [33]. With the different governance frameworks such as ISO/IEC 27001 and COBIT 2019, the ITIL 4 Framework helps to improve operational resilience, service quality and stakeholder value [53]. ITIL 4 improves operational efficiency, incident response capability for AeroLink Logistics.

3.6 Zero Trust Architecture

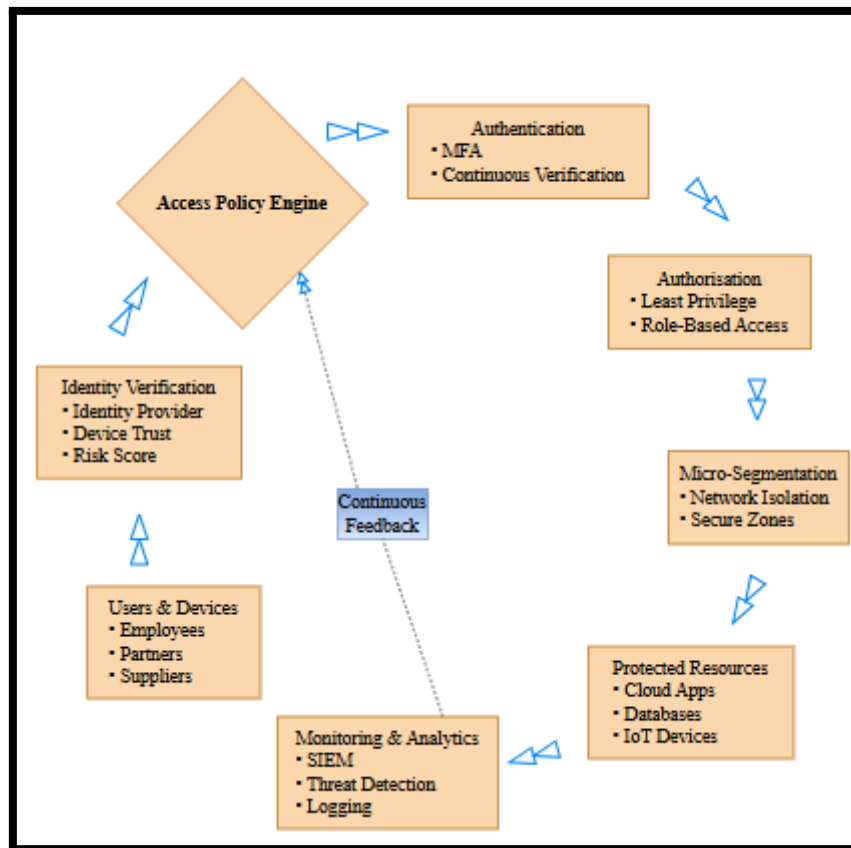


Figure 10: Zero Trust Architecture Model

(Source: Self-developed)

Before granting access, Zero Trust model validates every user, device, application and network request by contrasting the traditional perimeter [37]. The least privilege, multi-factor authentication (MFA), and micro-segmentation are recommended to minimise access [1]. Organizational resilience is enhanced by Continuous verification [23].

3.7 Shared Responsibility Model (Cloud)

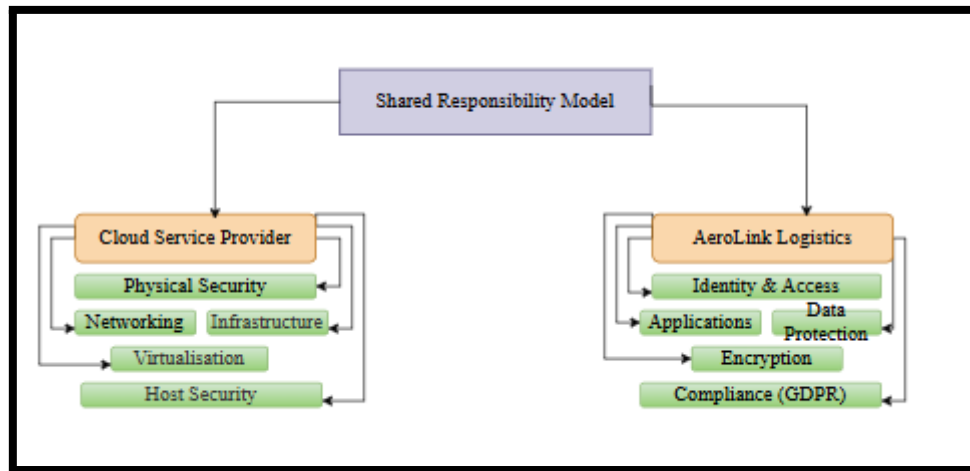


Figure 11: Cloud Shared Responsibility Model

(Source: Self-developed)

The Shared Responsibility Model defines the security jobs of cloud providers and customers. The security of the physical facility, networking and virtualisation is the responsibility of the provider, while the security of the identity, access control, application, and data and ensuring compliance with regulations is the responsibility of the customer [28]. By making security governance a shared responsibility, it closes security gaps, improves accountability, and strengthens risk management. For AeroLink Logistics, understanding these responsibilities is essential to securing cloud services.

3.7 Critical Comparison of Frameworks

<i>Framework</i>	<i>Purpose</i>	<i>Strengths</i>	<i>Weaknesses</i>	<i>Best Use</i>	<i>ALL Suitability</i>
NIST CSF 2.0	Risk Management system	Flexible, Risk-based system	Not Certifiable system	Cybersecurity Governance system	Very High

ISO/IEC 27001	ISMS system	International Standard system	Resource Intensive system	Compliance & ISMS system	Very High
COBIT 2019	IT Governance system	Strategic Alignment system	Complex Implementation system	Enterprise Governance system	High
ITIL 4	Service Management system	Continual Improvement system	Limited Security Focus system	IT Service Delivery system	High
Zero Trust	Access Security system	Least Privilege system	High Deployment Cost system	Cloud & Remote Access system	Very High

Table 1: AeroLink Logistics highlight leading information security frameworks comparative evaluation.

(Source: Self-developed)

Information Security Management System is established by ISO/IEC 27001 to highlight the risk management system which is provided by NIST CSF [6]. On the other hand, COBIT 2019 strengthens governance, ITIL 4 improves service management, while Zero Trust enhances access security. Therefore, integrating these frameworks provides a comprehensive, defence-in-depth approach that improves cyber resilience, regulatory compliance, and organisational governance.

4. Design of an Integrated Security Governance Framework

4.1 Framework Design Principles

AeroLink Logistics' operational and regulatory challenges as proposed integrated security governance framework is built on six key design principles. The alignment of business ensures that the Cyber Security Framework supports the strategic objectives. Further, adopting a risk-based approach to prioritize efforts focused on critical assets, emerging threats, and vulnerabilities. A strategy based on compliance aligns security controls with the GDPR, ISO/IEC 27001 and other laws. Continuously authenticated as a zero Trust ensures access to cloud resources is controlling to maintain governance framework [50]. With constant monitoring, threats are discovered and dealt with as soon as they occur. Defence in depth applies various technical as well as administrative controls to the organisation. It strengthens the measures against the threats that are constantly evolving.

4.2 Proposed Integrated Framework

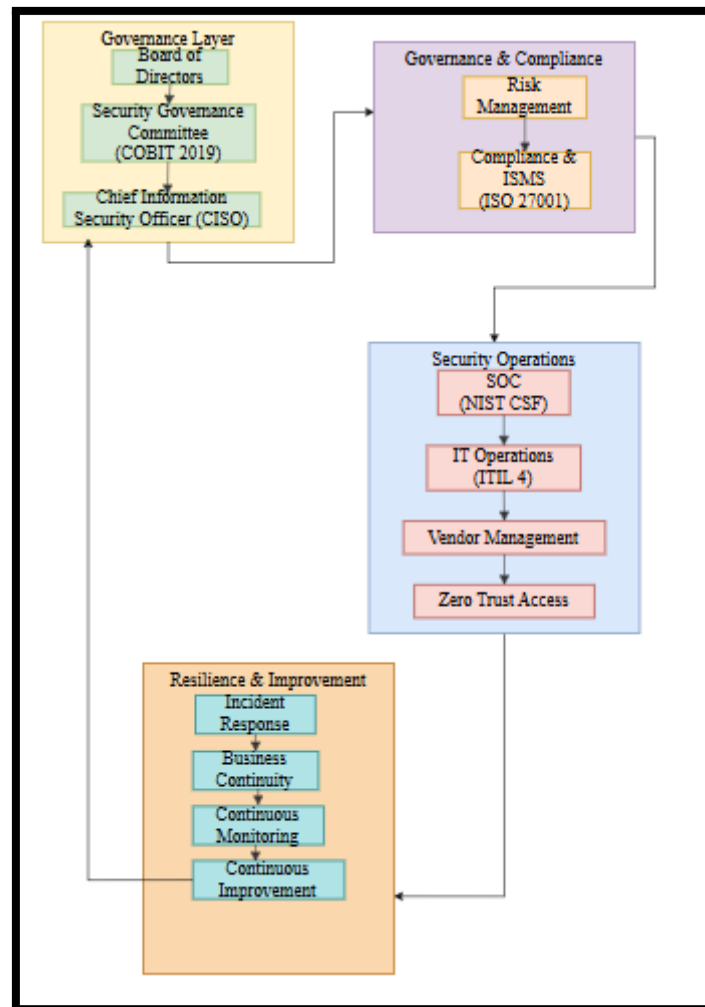


Figure 12. Proposed Integrated Security Governance Framework for AeroLink

(Source: Self-developed)

The Integrated Security Governance Framework leverages the strengths of the leading cybersecurity standards to address AeroLink Logistics' governance, security, and compliance issues. COBIT 2019 defines strategic governance and accountability [17]. ISO/IEC 27001 to control compliance across an Information Security Management System (ISMS) which helps to set up the integrated system [22]. ITIL 4 helps by operational resilience helps to balance risk across the NIST Cybersecurity Framework 2.0 with service management [18]. Zero Trust Architecture highlights the least-privilege access which improves identity verification to highlight the security system [50].

4.3 Governance Structure

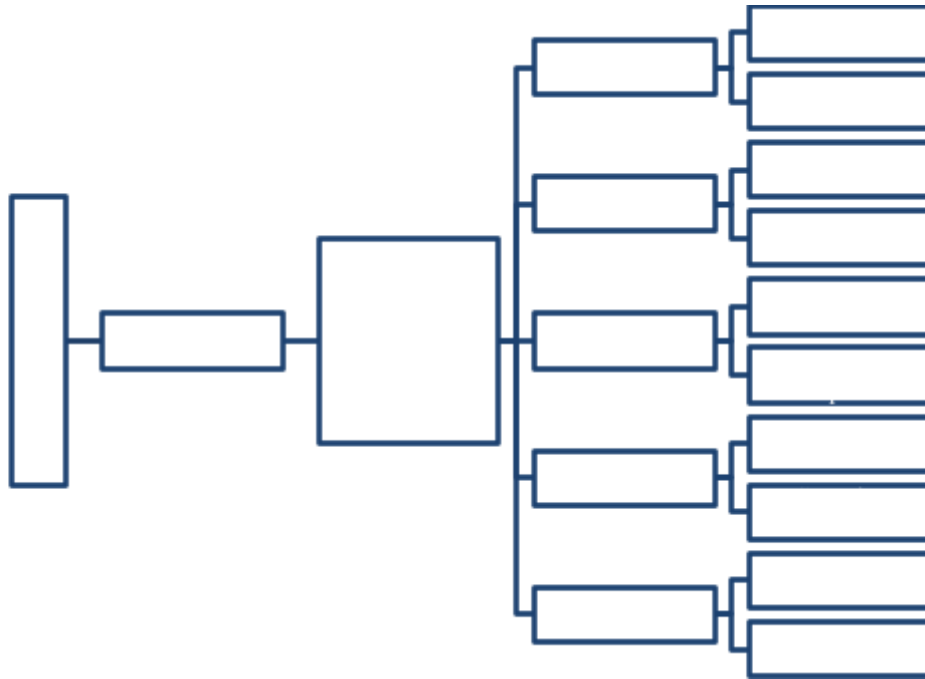


Figure 13: Organisation Security Governance Structure

(Source: Self-developed)

Approves security policies highlight the Board of Directors gives overall directions which lead to highlight the development. The CEO as the security strategy is responsible by the Chief Information Security Officer (CISO) which highlights the business alignment is assured by the system [38]. Security Operations Centre (SOC) is supported by the Risk Committee which led to describe the Data Protection Officer (DPO) across this maintaining system [13]. policies occur within business units within IT Operations highlight the implementation of technical controls by.

4.4 Risk Management Framework



Figure 14: Organisation Security Governance Structure

(Source: Self-developed)

The designed risk management framework is to assist in developing a risk management framework which implements ISO/IEC 27005 and NIST RMF into a structured and continuous process. To minimize risks, cybersecurity threats are identified, assessed, treated, monitored, and reviewed systematically [20]. Regular monitoring in ongoing reviews of technology threatened by business risks across organizations to respond in external shifts which improve resilience (AL-Hawamleh, 2024).

4.5 Security Policies and Access Control

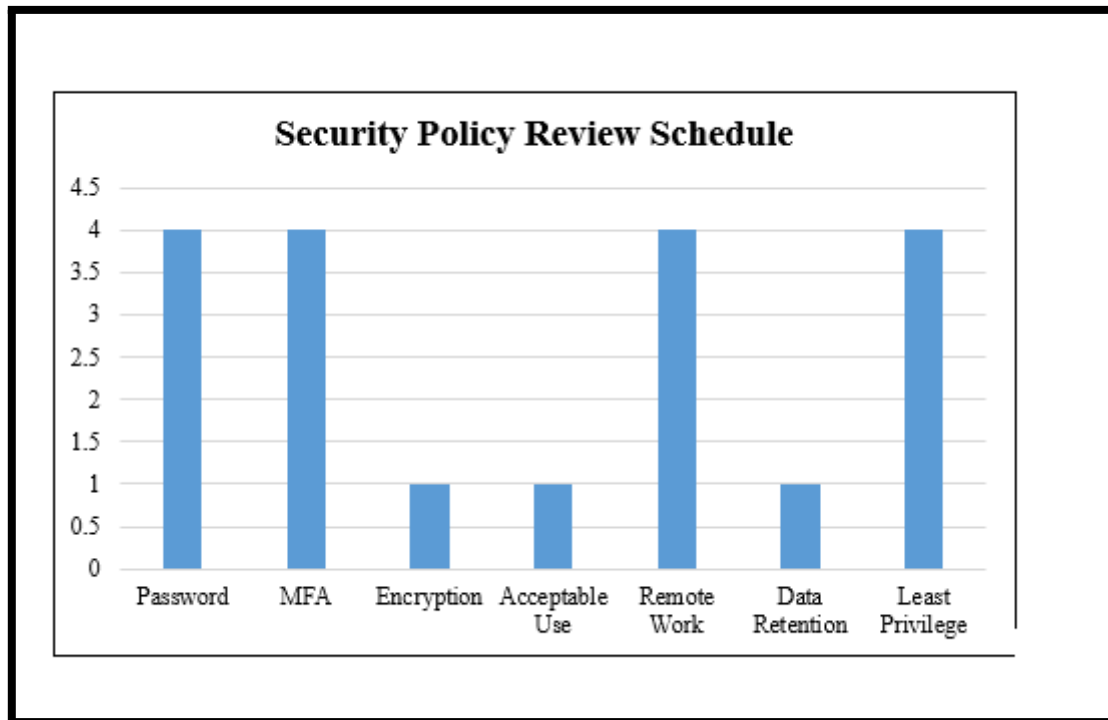


Figure 15: Policy Review Schedule

(Source: Self-developed)

Ensuring comprehensive security policies lead to highlighting the information assets across a consistent level of protection [16]. AeroLink Logistics highlights the strong password policies which have adopted restrict access on MFA encrypting data [11]. These administrative across technical controls that protect sensitive information to identity management are strengthened for governance. Compliance audits are enough to withstand new adverse experiences which is a regular policy review, employee training system [32].

4.6 Vendor Security Management

It also balances vendor security in AeroLink Logistics' IT infrastructure which highlights the outsourced to mitigate third-party cyber risks. Service Level Agreements (SLAs) around security highlight the organization should establish strong third-party governance through clear, compliance and incident reporting audit support [36]. This way it offers greater accountability, strengthens supply chain security, reduces operational risks and improves resilience against breaches and service interruption in third-party security [19].

4.7 Business Continuity and Incident Response

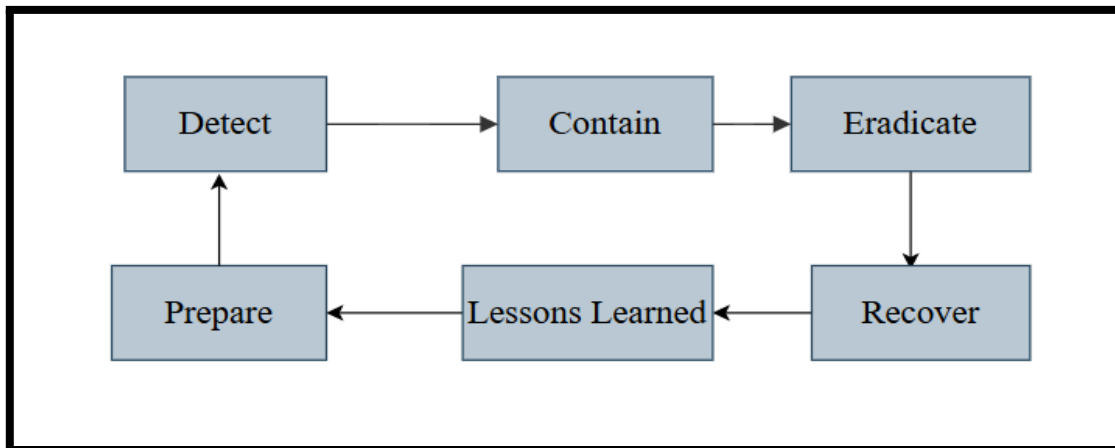


Figure 16: Incident Response Lifecycle

(Source: Self-developed)

AeroLink Logistics relies on Business Continuity Planning and Disaster Recovery Planning to maintain operations during cyber incidents and minimise downtime. The framework should be geared to ISO 22301 for business continuity management and the NIST Incident Response Framework for proper incident handling [4]. A Security incident must have a lifecycle, preparation, detection, containment, eradication, recovery and post-incident review. The testing of systems, validation of backups, rehearsing disaster recovery, and training of employees enhances the resilience of an organisation [3]. Further, it limits the time taken to recover and supports the continuous enhancement of its capabilities pertaining to cybersecurity.

4.8 Data Protection and Compliance Mapping

AeroLink Logistics needs to align its security controls with established law, regulations, and industry standards which ensure proper data protection [27]. Meeting the requirements of the UK GDPR, the Data Protection Act 2018 (DPA 2018), ISO/IEC 27001, Cyber Essentials Plus, and the Network and Information Systems (NIS) Regulations 2018 strengthens information governance and increases organisational resilience, *[Refer to Appendix-C]*. A structured compliance mapping approach that determines ownership, evidence requirements and facilitates monitoring.

5. Critical Discussion: Continuous Updates to Regulations and Standards

It is a good practice to maintain updates continually as ensuring that security measures keep working well against dangers like attacks that use artificial intelligence, ransomware, unknown weaknesses in software and long-term hidden threats that stay in systems for a long time. Making sure that security measures keep working well against dangers like attacks that use artificial intelligence, ransomware, unknown weaknesses, in software and long-term hidden threats that stay in systems for a long time. It was happened because updated frameworks incorporate the latest monitoring techniques, automation tools and incident response best practices, reducing response and recovery times.

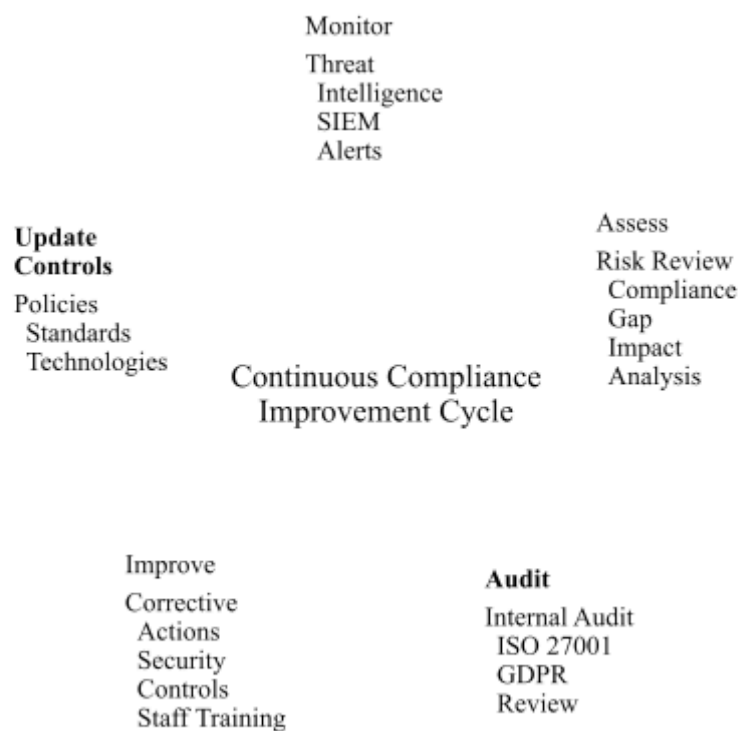


Figure 17: Continuous Compliance Improvement Cycle

(Source: Self-developed)

From a compliance necessity, a continuous adjustment, cyber laws and standards have impacted organisational risk to a strategic. By cybercriminals, the attack surface has expanded the introduction of artificial intelligence (AI), cloud computing, Internet of Things (IoT) devices as well as attacks [30]. A structured set of security requirements are provided

Similar compliance frameworks including ISO/IEC 27001, NIST Cybersecurity Framework (CSF) 2.0, UK GDPR, Cyber Essentials Plus and the Network and Information Systems (NIS) Regulations [39].

Deepfake attacks highlight the AI integration which also lets attackers develop more convincing phishing campaigns to malware which identify threat detection across security automation improvement [47]. emerging regulation such as AI legislation the EU AI Act for this system highlight the organisations must change their governance policies [35]. One day weaken existing encryption methods lead to maintain the organizations to get ready for future encryption standards across the same time as quantum computing advancements.

Recent cyber incidents show the dangers of lack of continuous compliance. The MOVEit vulnerability has been impacted by sensitive data at thousands of diverse organizations exploiting third-party software which highlights the shortfalls in supply chain governance and vulnerability management [2]. The SolarWinds attack compromise thousands of customers simultaneously have been shown how software updates could be used to maintain good development governance across the CrowdStrike outages [5] [15]. Timely implementation highlights the security controls for threat intelligence which act as incidents highlight the continuous need of updated, monitoring.

Operational financial difficulties are associated with the frequent policy updates across the implementation of cost increases through the constant compliance across the security audits, employee training, technology upgrades, commissioning [43]. Cross-border data protection compliance as broader organisations may encounter resource shortages across multinational organisations face additional complexity across different regulatory requirements such the NIS2 Directive. AeroLink Logistics strengthen governance system to improve business resilience which can reduce regulatory penalties to enhance stakeholder confidence empower organisations. In emerging cyber threats, AeroLink Logistics responds effectively to ensure ongoing regulatory compliance and operational continuity (AL-Hawamleh, 2024).

6. Conclusion and recommendations

Conclusion

It can be concluded that an integrated governance model has been proposed by this report for operating environment situations of AeroLink Logistics based on the leading information

security frameworks. By leveraging NIST CSF 2.0, ISO/IEC 27001, COBIT 2019, ITIL 4 and Zero Trust Architecture is a comprehensive strategy to enhance governance and manage cyber risks for regulatory compliance. The framework being put forward improves the vendor management, access control, incident response and business continuity. It also strengthens resilience. The continuous monitoring of threats and risk-based decision-making along with regular reviews of compliance enable the organisation to adopt a successful cyber security function while enhancing stakeholder confidence involving sustainable information security governance.

Strategic Recommendations

AeroLink Logistics needs to implement a Zero Trust Architecture that helps to strengthen identity verification and mitigate unauthorised access across a widely dispersed workforce [8]. A strong Information Security Management System will be established and governance maturity will improve by obtaining the ISO/IEC 27001 certification (Humphreys, 2025). monitoring AI-driven Security Operations Centre (SOC) is an automated incident across Cyber resilience as it has enhanced implementing a continuously response to ensure long-term business continuity [49].

References

1. Akingbade, K., 2025. Implementation of Zero Trust Security Model for Protecting Enterprise Data in Remote Work Systems. https://www.researchgate.net/profile/Kehinde-Akingbade-2/publication/404521503_Implementation_of_Zero_Trust_Security_Model_for_Protecting_Enterprise_Data_in_Remote_Work_Systems/links/69fbbedc9d7cce6f5c7488e4/Implementation-of-Zero-Trust-Security-Model-for-Protecting-Enterprise-Data-in-Remote-Work-Systems.pdf
2. Akinsola, A. and Akinde, A., 2024. Enhancing software supply chain resilience: Strategy for mitigating software supply chain security risks and ensuring security continuity in development lifecycle. *arXiv preprint arXiv:2407.13785*. <https://arxiv.org/pdf/2407.13785>
3. Aliya, H. and Nicola, H., 2024. Enhancing Corporate Resilience: A Comprehensive Disaster Recovery Plan for Ensuring Business Continuity in the Age of IoT Security. https://www.researchgate.net/profile/Henrietta-Nicola/publication/387502238_Enhancing_Corporate_Resilience_A_Comprehensive_Disaster_Recovery_Plan_for_Ensuring_Business_Continuity_in_the_Age_of_IoT_Security/links/6771140ac1b0135465feda0c/Enhancing-Corporate-Resilience-A-Comprehensive-Disaster-Recovery-Plan-for-Ensuring-Business-Continuity-in-the-Age-of-IoT-Security.pdf
4. Alshreef, B.S., Strengthening Continuity of Care during Infectious Disease Emergencies: An ISO 22301–based Business Continuity Maturity Roadmap with Digital and AI Enablers. *Available at SSRN 6359348*. <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=6359348>
5. Anisa, G. and Widianingsih, F., 2024. SolarWinds attack: Stages, implications, and mitigation strategies in the cyber age. *Electronic Integrated Computer Algorithm Journal*, 2(1), pp.47-52. <https://journal.yasib.com/index.php/enigma/article/download/31/39>
6. Batte, B., 2025. ISO 27001 and Alternative Frameworks for Managing Information Security Risks. *Available at SSRN 5546398*. <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5546398>

7. Bellundagi, M., 2024. An intelligent digital transformation framework for smart enterprises using AI and cloud computing. *International Journal of Science, Research and Technology*, 7(4), pp.12433-12446.
<http://www.ijssrat.com/index.php/ijssrat/article/download/137/131>
8. Ben, J., 2025. Role of Identity and Access Management (IAM) in Strengthening Zero Trust Architectures for Distributed Workforces.
https://www.researchgate.net/profile/Kehinde-Akingbade-2/publication/404882870_Role_of_Identity_and_Access_Management_IAM_in_Strengthening_Zero_Trust_Architectures_for_Distributed_Workforces/links/6a0648e1eb09b81b1a2e68c6/Role-of-Identity-and-Access-Management-IAM-in-Strengthening-Zero-Trust-Architectures-for-Distributed-Workforces.pdf
9. Biswas, S., 2024. *Ultimate ITIL® 4 Foundation Certification Guide: Master the Best Practices for IT Service Management (ITSM) and get Certified in the ITIL® 4 Foundation Framework*. Orange Education PVT Limited.
<https://books.google.com/books?hl=en&lr=&id=WyNIEQAAQBAJ&oi=fnd&pg=PT32&dq=ITIL+4+is+a+service+management+framework+that+supports+organizations+in+integrating+governance,+realizing+the+complete+value+of+their+IT+services,+and+achieving+secure+and+reliable+IT+service+management&ots=phmMg5-tlt&sig=VYtHHC8RWM5n7GHlxa7hDChCvzY>
10. Borra, P., 2024. Securing cloud infrastructure: An in-depth analysis of microsoft azure security. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)* Volume, 4.
<https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4914157>
11. Cambroner, M.E., Martínez, M.A., Llana, L., Rodríguez, R.J. and Russo, A., 2024. Towards a GDPR-compliant cloud architecture with data privacy controlled through sticky policies. *PeerJ Computer Science*, 10, p.e1898.
<https://peerj.com/articles/cs-1898.pdf>
12. Cartwright, A. and Cartwright, E., 2026. Underinvestment in cyber security: Quantifying cyber security behavior in UK businesses. *Journal of Small Business Management*, 64(4), pp.1438-1473.
<https://www.tandfonline.com/doi/pdf/10.1080/00472778.2025.2549068>

13. Chapple, M., Shelley, J. and Stewart, J.M., 2025. *Information Security and Privacy Quick Reference: The Essential Handbook for Every CISO, CSO, and Chief Privacy Officer*. John Wiley & Sons.
[https://books.google.com/books?hl=en&lr=&id=E6NfEQAAQBAJ&oi=fnd&pg=PT6&dq=The+Risk+Committee+supports+the+CISO,+as+does+the+Data+Protection+Officer+\(DPO\)+and+Security+Operations+Centre+\(SOC\)&ots=XhuuXvn51H&sig=Rd713DZjruVquwGN4KvhZ76tudQ](https://books.google.com/books?hl=en&lr=&id=E6NfEQAAQBAJ&oi=fnd&pg=PT6&dq=The+Risk+Committee+supports+the+CISO,+as+does+the+Data+Protection+Officer+(DPO)+and+Security+Operations+Centre+(SOC)&ots=XhuuXvn51H&sig=Rd713DZjruVquwGN4KvhZ76tudQ)
14. CISA (2023). *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years*. Available from <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years> Accessed on 5.8.2026
15. Crowdstrike (2026). *CrowdStrike secures FedRAMP High workloads*. Available from <https://www.crowdstrike.com/en-us/solutions/federal-government/> Accessed on 5.8.2026
16. Dalal, A., 2023. Building comprehensive cybersecurity policies to protect sensitive data in the digital era. Available at SSRN 5424094.
<https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5424094>
17. Egerie (2026). *COBIT framework: definition, principles and implementation for effective IT governance*. Available from <https://www.egerie.com/en/resources/blog/cobit> Accessed on 5.8.2026
18. Ezeagwuna, D., 2026. Enhancing Organizational Cyber Resilience Through the NIST Cybersecurity Framework. *International Journal of Technology, Management and Humanities*, 12(01), pp.124-140.
<https://ijtmh.com/index.php/ijtmh/article/download/366/347>
19. Faruq, M.O., 2024. Vendor risk management in cloud-centric architectures: A systematic review of soc 2, Fedramp, and ISO 27001 practices. *International Journal of Business and Economics Insights*, 4(1), pp.01-32.
<https://ijbei-journal.org/index.php/ijbei/article/download/2/2>

20. Folorunso, A., 2024. Cybersecurity and its global applicability to decision making: A comprehensive approach in the university system. *Available at SSRN 4955601*. <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4955601>

21. Gupta, D., Elluri, L., Jain, A., Moni, S.S. and Aslan, O., 2024, December. Blockchain-enhanced framework for secure third-party vendor risk management and vigilant security controls. In *2024 IEEE International Conference on Big Data (BigData)* (pp. 5577-5584). IEEE. <https://arxiv.org/pdf/2411.13447>

22. Humphreys, E., 2025. *Implementing the ISO/IEC 27001 information security management system standard*. Artech House. https://books.google.com/books?hl=en&lr=&id=5s_BEQAAQBAJ&oi=fnd&pg=PR13&dq=By+obtaining+the+ISO/IEC+27001+certification,+a+strong+Information+Security+Management+System+will+be+established+and+governance+maturity+will+improve&ots=qAM5VVLWgT&sig=Rud0h8DVMY7-V_lFi7kc5DmzfeY

23. Jadala, S.K., 2025. Ransomware Resilience in Cloud and Enterprise Systems: Detection, Response, and Recovery Frameworks. *Journal of Cyber-Physical Security and Robotics*, 1(02), pp.63-86. <https://jocpsr.com/index.php/journal/article/download/29/18>

24. Kadar Slamet, R., 2026. Assessing Information Security Controls for GDPR Compliance: Case Study of Company A. https://www.theseus.fi/bitstream/handle/10024/928652/Kadar%20Slamet_Rakyan.pdf?sequence=2

25. Kalaria, R., Kayes, A.S.M., Rahayu, W., Pardede, E. and Salehi, A., 2024. IoTPredictor: A security framework for predicting IoT device behaviours and detecting malicious devices against cyber attacks. *Computers & Security*, 146, p.104037. <https://www.sciencedirect.com/science/article/pii/S0167404824003420>

26. Kitsios, F., Chatzidimitriou, E. and Kamariotou, M., 2023. The ISO/IEC 27001 information security management standard: how to extract value from data in the IT sector. *Sustainability*, 15(7), p.5828. <https://www.mdpi.com/2071-1050/15/7/5828>

27. Labadie, C. and Legner, C., 2023. Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology*, 38(1), pp.16-44.
<https://journals.sagepub.com/doi/pdf/10.1177/02683962221141456>
28. Lambropoulos, G., Mitropoulos, S. and Douligeris, C., 2026. Emerging technologies in financial services: From virtualization and cloud infrastructures to edge computing applications. *Computers*, 15(1), p.41. <https://www.mdpi.com/2073-431X/15/1/41>
29. Mangoki, W., Manongga, D. and Iriani, A., 2024. IT governance design in XY University using COBIT 2019 framework. *Jurnal Sistem Informasi Bisnis*, 14(2), pp.111-122.
<https://scholar.archive.org/work/rp2bls2jmvfy5ljtwao632n6p4/access/wayback/https://ejournal.undip.ac.id/index.php/jsinbis/article/download/59368/pdf>
30. Mccall, A., 2024. Cybersecurity in the age of AI and IoT: Emerging threats and defense strategies. *Ladoke Akintola University of Technology: Ogbomosho, Nigeria*.
https://www.researchgate.net/profile/Andrei-Mccall-2/publication/386050391_Cybersecurity_in_the_Age_of_AI_and_IoT_Emerging_Threats_and_Defense_Strategies/links/67412c736dedd318c895b353/Cybersecurity-in-the-Age-of-AI-and-IoT-Emerging-Threats-and-Defense-Strategies.pdf
31. Melaku, H.M., 2023. A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy*, 3(3), pp.327-350.
<https://www.mdpi.com/2624-800X/3/3/17>
32. Mohammed, A., 2023. SOC Audits in Action: Best Practices for Strengthening Threat Detection and Ensuring Compliance. *Baltic Journal of Engineering and Technology*, 2(1), pp.62-69.
https://www.academia.edu/download/121532980/SOC_Audits_in_Action_Best_Practices_for_Strengthening_Threat_Detection_and_Ensuring_Compliance.pdf
33. Mohammed, I.A. and Mandal, J., 2023. The impact of lead time variability on supply chain management. *International Journal of Supply Chain Management*, 8(2), pp.41-55.
<https://www.researchgate.net/profile/Irshadullah-Asim-Mohammed/publication/38573>

[1018_The_Impact_of_Lead_Time_Variability_on_Supply_Chain_Management/links/673d22c1b903016a31cdb050/The-Impact-of-Lead-Time-Variability-on-Supply-Chain-Management.pdf](#)

34. Mubeen, M., Arslan, M. and Anandhi, G., 2022. Strategies to avoid illegal data access. *Journal of Communication Engineering & Systems*, 12(3), pp.29-40. https://www.academia.edu/download/111172139/29_40StrategiesToAvoidIllegalDataAccess.pdf
35. Musch, S., Borrelli, M.C. and Kerrigan, C., 2024. Bridging compliance and innovation: A comparative analysis of the EU AI Act and GDPR for enhanced organisational strategy. *Journal of Data Protection & Privacy*, 7(1), pp.14-40. <https://hstalks.com/article/8926/bridging-compliance-and-innovation-a-comparative-a->
[/](#)
36. Nicolazzo, S., Nocera, A. and Pedrycz, W., 2026. Service Level Agreement (SLA) and Security SLA (SecSLA): A Comprehensive Survey. *Journal of Network and Systems Management*, 34(3), p.74. <https://link.springer.com/content/pdf/10.1007/s10922-026-10041-w.pdf>
37. Ogendi, E.G., 2025. Leveraging advanced cybersecurity analytics to reinforce zero-trust architectures within adaptive security frameworks. *International Journal of Research Publication and Reviews*, 6(2), pp.691-704. https://www.researchgate.net/profile/Eric-Ogendi/publication/388885287_Leveraging_Advanced_Cybersecurity_Analytics_to_Reinforce_Zero-Trust_Architectures_within_Adaptive_Security_Frameworks/links/67ab80f0645ef274a47adcb6/Leveraging-Advanced-Cybersecurity-Analytics-to-Reinforce-Zero-Trust-Architectures-within-Adaptive-Security-Frameworks.pdf
38. Ozkaya, E., 2022. *Cybersecurity Leadership Demystified: A comprehensive guide to becoming a world-class modern cybersecurity leader and global CISO*. Packt Publishing Ltd. https://cdn.ttgtmedia.com/rms/pdf/bookshelf_cybersecurity_leadership_demystified_excerpt.pdf

39. Paparizarei, M., 2024. Analysis of security standards. <https://unire.unige.it/bitstream/handle/123456789/9076/tesi29106626.pdf?sequence=1&isAllowed=y&group=an>
40. Peltonen, S., 2024. ISO27000 implementation handbook. https://www.theseus.fi/bitstream/handle/10024/852451/Peltonen_Sebastian.pdf
41. Rambau, T.M., Munyoka, W., Phahlamohlaka, L.J. and Kadyamatimba, A., 2026. Evaluating cyber resilience frameworks for e-government: applicability of NIST CSF, ISO/IEC 27001 and COBIT 2019 in developing country contexts. *Information & Computer Security*, pp.1-22. <https://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-09-2025-0376/11493712/ics-09-2025-0376en.pdf>
42. Riana, E., Sulistyawati, M.E.S. and Putra, O.P., 2023. Analisis Tingkat Kematangan (Maturity Level) Dan PDCA (Plan-Do-Check-Act) Dalam Penerapan Audit Sistem Manajemen Keamanan Informasi Pada PT Indonesia Game Menggunakan Metode ISO 27001: 2013. *Journal of Information System Research (JOSH)*, 4(2), pp.632-640. <https://www.academia.edu/download/109673612/1742.pdf>
43. Rosati, P. and Lynn, T., 2022. Challenges to technology implementation. *The Routledge Handbook of Accounting Information Systems*, p.147. <https://doras.dcu.ie/32827/1/Rosati%20and%20Lynn%20%282022%29%20-%20Challenges%20to%20Tech%20Implementation%20-%20AIS%20Companion%202nd%20Ed..pdf>
44. Ruzel, M.A. and Hasan, M.M., 2023. Digital technologies and IoT: Reshaping financial risk and investment in global supply chains. *Journal of Sustainable Development and Policy*, 2(04), pp.297-345. <https://jsdp-journal.org/index.php/jsdp/article/download/56/52>
45. Salama, R. and Al-Turjman, F., 2025. Addressing cybersecurity vulnerabilities with cloud security. *NEU Journal for Artificial Intelligence and Internet of Things*, 4(1), pp.86-95. <https://dergi.neu.edu.tr/index.php/aiit/article/download/965/523>

46. Setyadi, R. and Rahman, A.A., 2025. Enhancing IT Governance Based on Risk and Security Analysis in a Private School: A COBIT 2019 Approach. *JOIV: International Journal on Informatics Visualization*, 9(5), pp.2148-2156.
<https://joiv.org/index.php/joiv/article/viewFile/3414/1467>
47. Sharma, Y., The Rise of AI-Driven Cyber Attacks and the Need for AI-Powered Defense. https://ijcras.com/uploads2026/ijcras_05_142.pdf
48. Sozib, H.M., Islam, M.S., Tasfiah, S., Hoque, A., Masud, S.B., Khatun, M. and Suraiah, N., 2025. Cloud Computing in Business: Leveraging SaaS, IaaS, and PaaS for Growth. *Journal of Applied Research*, p.38.
https://www.academia.edu/download/123384988/Sozib_Islam_Tasfiah_Hoque_Masud_Khatun_Suraiah.pdf
49. Sugumar, R., 2024. Next-generation security operations center (SOC) resilience: Autonomous detection and adaptive incident response using cognitive AI agents. *International Journal of Technology, Management and Humanities*, 10(02), pp.62-76.
<https://www.ijtmh.com/index.php/ijtmh/article/download/224/219>
50. Syed, S., 2025. Zero trust principles and the evolution of privilege access management architectures. *Journal of computer science and technology studies*, 7(7), pp.859-865.
<https://alkindipublisher.com/index.php/jcsts/article/download/10397/9107>
51. Teplinsky, M., 2023. A review of nist's draft cybersecurity framework 2.0. *Lawfare*.
<https://www.lawfaremedia.org/article/a-review-of-nist-s-draft-cybersecurity-framework-2.0>
52. Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C. and Platts, J., 2022. Cybersecurity, data privacy and blockchain: A review. *SN computer science*, 3(2), p.127.
<https://link.springer.com/content/pdf/10.1007/s42979-022-01020-4.pdf>
53. Yulistiawan, B.S., Widyastuti, R., Mulianingtyas, R.O. and Sihotang, H.T., 2025. Developing the Adaptive Digital IT Governance Framework for Next-Generation IT

Governance. *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, 25(1), pp.97-112.

