

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: Harsh Shaileshbhai Dhokiya

Studnt Id: 2545109

Abstract

This report critically analyses the information security governance, risk and compliance challenges within AeroLink Logistics (ALL), through concentrating on its cloud-based, IoT-powered, remote and outsourced technology environment. It profoundly examines the NIST CSF 2.0, ISO/IEC 27001, COBIT 2019, ITIL 4 and Zero Trust in order to determine their relevance towards the security requirements of this firm. Moreover, an integrated governance model has been proposed to address the fragmented accountability, third-party exposure, access risks, compliance gaps and ultimately the operational disruptions. The report further investigates why security standards and regulations need to continually evolve in response to emerging technologies, cyber threats, and the global regulatory challenges as well. In addition, the strategic recommendations offer a sense of phased actions to fortify governance, adaptability, compliance and continual security enhancement as well.

Table of Contents

1. Introduction.....	4
1.1 Digital and Security Context	4
1.2 Organisational Security Problem.....	5
1.3 Aim and Report Direction	5
2. AeroLink Logistics: Organisational and Security Assessment	5
2.1 Operational and Technology Profile.....	5
2.2 Evaluation of Existing Security Exposure	6
2.3 Case Assumptions.....	7
3. Critical Review of Information Security Frameworks and Models	8
3.1 Security Governance and GRC Foundations	8
3.2 NIST Cybersecurity Framework 2.0.....	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 Security Model	13
3.7 Comparative Evaluation and Selection	14
4. Proposed Integrated Security Governance and Compliance Model for ALL	15
4.1 Design Rationale and Strategic Principles	15
4.2 Integrated Security Governance Model	15
4.3 Accountability and Governance Arrangement	16
4.4 Risk Identification, Treatment and Monitoring.....	17
4.5 Compliance, Legal and Ethical Considerations	17
4.6 Vendor Security Management.....	18
4.7 Resilience, Continuity and Incident Handling	18
4.8 Business Continuity and Disaster Recovery	19
5. Critical Evaluation: Why Security Standards and Regulations Must Evolve.....	19
6. Conclusion and Strategic Recommendations	21
6.1 Conclusion.....	21
6.2 Strategic Recommendations	21
References	23
Appendices	30
Appendix 1: RACI Matrix	30
Appendix 2: ALL Cybersecurity Risk Register	32
Appendix 3: Strategic Recommendations Implementation Gantt Chart	33

1. Introduction

1.1 Digital and Security Context

Rapid adoption of cloud computing, artificial intelligence (AI), Internet of Things (IoT) and remote working has expanded the organisational attack surfaces and thus maximised the reliance on interconnected digital services [1]. UK government data showcases that approximately 43% of businesses within the country has experienced a cyber-breach or attack in the FY 2025/2026, which showcases the continuing exposure created through the digital information [2]. As a result, strong security governance is pivotal for effectively managing the evolving risks.

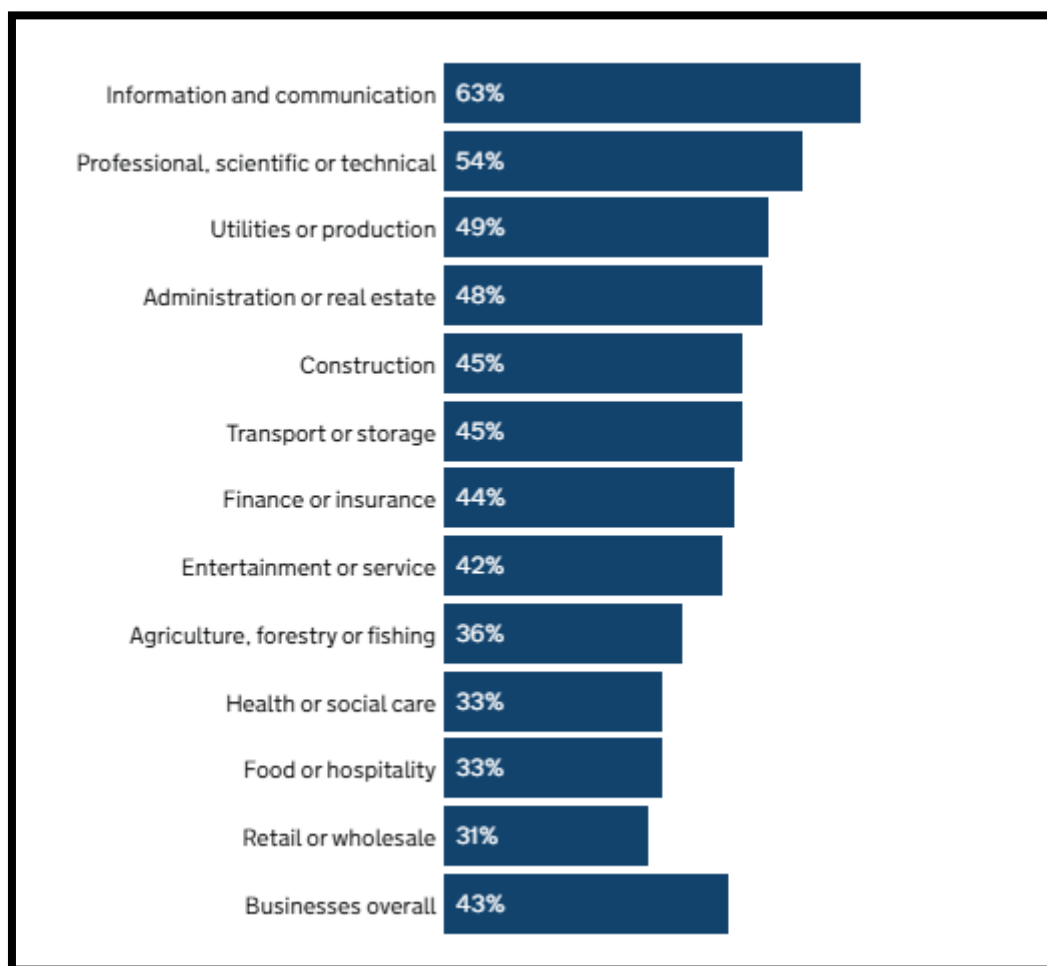


Figure 1: Statistics of cybersecurity breaches

(Source: [2])

1.2 Organisational Security Problem

Aerolink Logistics (ALL) is a multinational supply chain and logistics organisation operating within an increasingly technology-dependent environment. However, its current security position is affected through aspects like data breaches, fragmented governance, unclear security responsibilities, third-party dependency, inadequate compliance oversight, and finally the weakness across security as well as continuity arrangements [3]. These issues create notable information security risks along with operational threats, which emphasise the drastic need for a coordinated governance approach.

1.3 Aim and Report Direction

This report aims to critically analyse the established information security frameworks and develop an integrated governance approach which will address security, risk, adherence and adaptability as well. It first examines the organisational context along with security challenges, then it investigates the relevant frameworks, proposes a tailored governance model and critically discusses the continual regulatory as well as standards updates before presenting the recommendations and conclusions.

2. AeroLink Logistics: Organisational and Security Assessment

2.1 Operational and Technology Profile

Aerolink Logistics (ALL) is a multinational supply chain as well as logistics organisation delivering real-time tracking, warehousing and distribution services towards the international clients. Its operations heavily rely on cloud platforms, IoT-powered tracking as well as AI powered analytics, while remote working supports easy access across geographically dispersed locations [4]. Approximately 88% of its IT infrastructure is outsourced, which makes both the technology and third-party service dependencies strategically significant [5]. These characteristics develop a complicated environment which requires a sense of coordinated security, governance and operational adaptability.

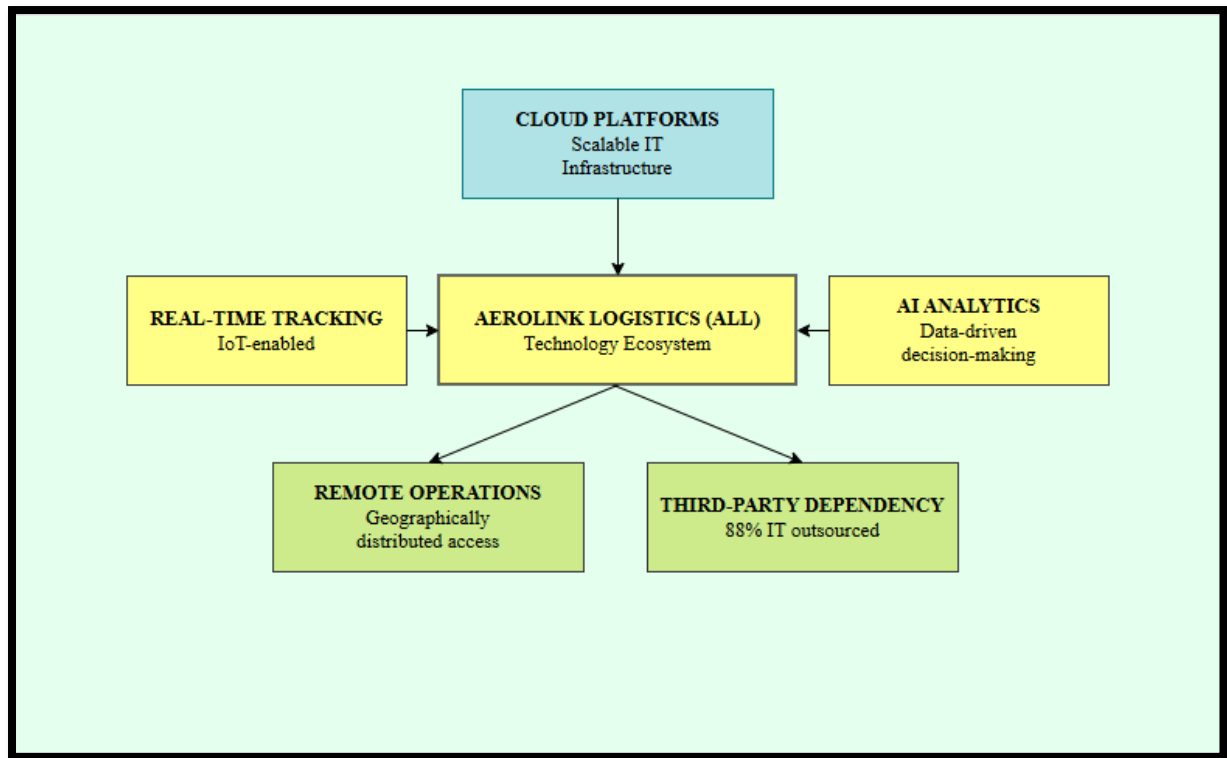


Figure 2: All Operational and Technology Ecosystem

(Source: Self-developed)

2.2 Evaluation of Existing Security Exposure

The high cloud dependence of Aerolinks enhances scalability; however, it also maximises the exposure towards the misconfiguration and shared responsibility failures, which requires both cloud governance as well as consistent configuration monitoring [6]. IoT also enhances the effectiveness of the tracking [7]. However, poor device security in combination with limited monitoring can develop entry points for attackers and thus make authentication, patching, as well as network segmentation necessary [8,9]. On the flip side, remote access also helps across boosting the overall flexibility of the business operation, however unmanaged devices often weaken the identity as well as endpoint assurance, which require MFA, along with device verification and least-privilege access as well. Compared with internal systems, extensive third-party reliance reduces direct security control while maximising supply chain exposure [10]. As a result, vendor due diligence, enforceable SLAs, along with a sense of continuous assurance are pivotal. Collectively, these weaknesses require centralised governance, adherence oversight, and finally reliable continuity planning.

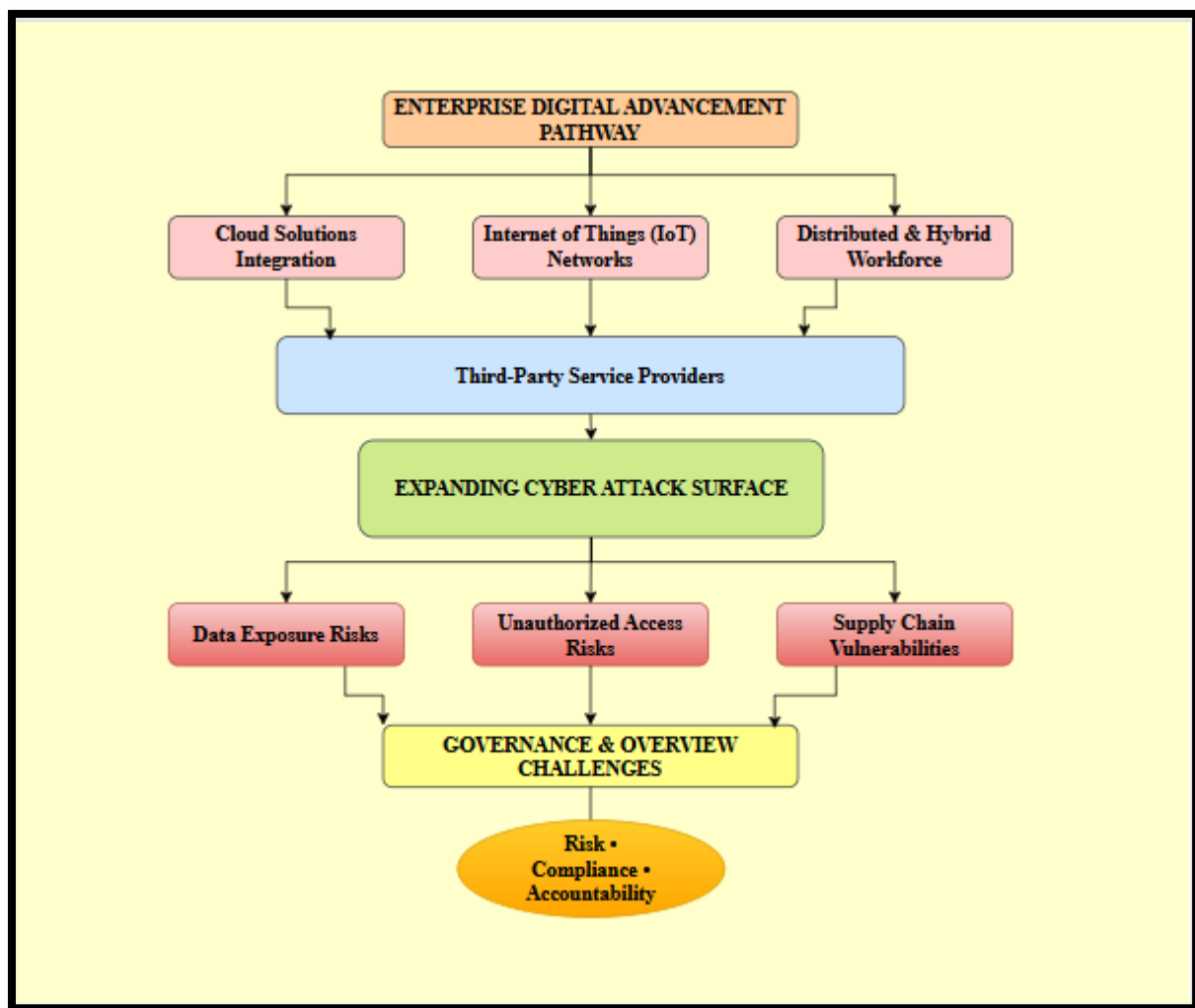


Figure 3: Digital Technology Adoption and Increasing Cybersecurity Exposure

(Source: Self-developed)

2.3 Case Assumptions

Area	Assumption	Purpose
Organisation	UK-based multinational	To establish the regulatory context
Technology	Cloud, IoT and AI-enabled.	To guide the technology-risk assessment
Workforce	Hybrid and remote	For justifying the zero Trust controls
Security maturity	Developing	Requires formal governance

Compliance	UK GDPR applicable	To support the proper compliance assessment
Certification	ISO 27001 not established	To identify the need for ISMS development
Resources	Moderate budget	To allow the prioritised, proportionate controls

Table 1: Case assumptions

(Source: Self-developed)

3. Critical Review of Information Security Frameworks and Models

3.1 Security Governance and GRC Foundations

Information and security governance establishes the organisational direction through closely aligning the governance, risk and compliance (GRC) with strategic decision-making [11, 12]. The GRC model connects the security objectives with a sense of risk ownership, regulatory obligations, as well as management accountability, which allows organisations to move beyond isolated technical controls [13]. Its value lies within effectively coordinating the policies, responsibilities and assurance mechanisms, while the contains oversights supports the informed decision making along with stronger organisational adaptability.

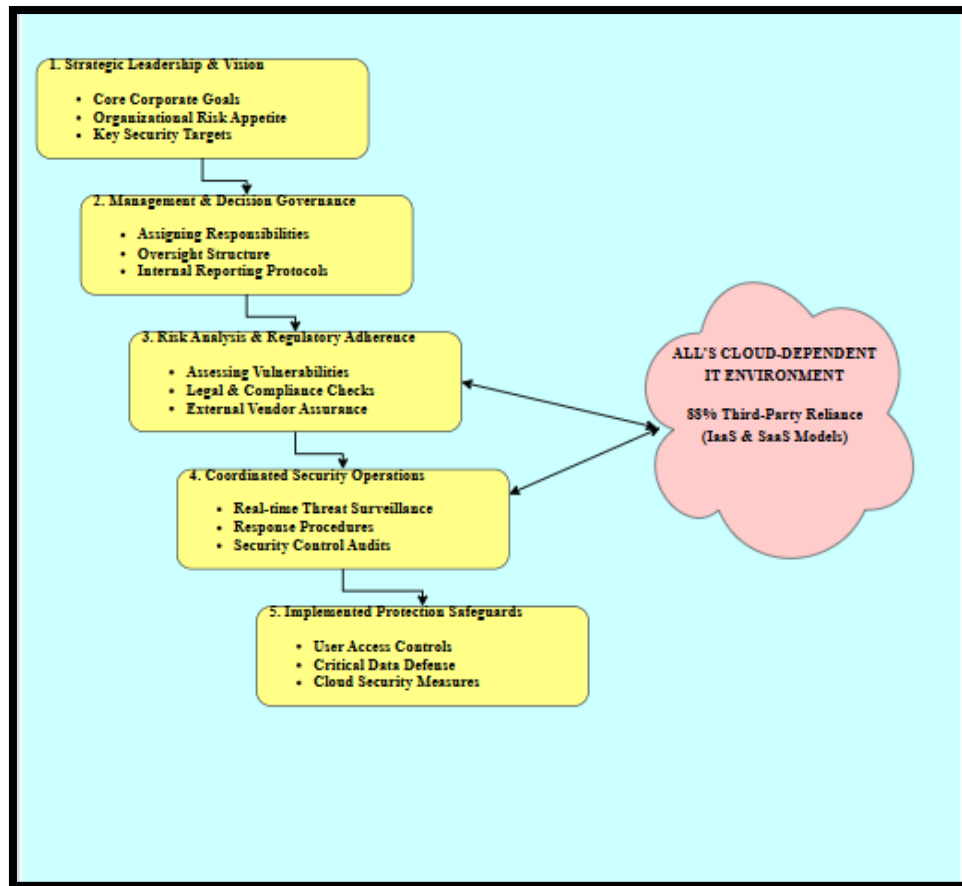


Figure 4 :Security Governance Hierarchy

(Source: Self-developed)

3.2 NIST Cybersecurity Framework 2.0

NIST CSF 2.0 presents a risk-based structure through the help of Govern, Identify, Protect, Detect, Respond and Recover [14]. With respect to ALL, it can assist in effectively organising the security risks which arise from cloud services, IoT devices, remote access and ultimately third-party [15]. Besides that, its flexible approach also guides the changing operational needs, but it does not offer adequate detailed controls for every security requirement. Therefore, NIST can help Aerolinks in enhancing their risk management approaches; however, it requires a sense of additional controls for effective implementation [16].

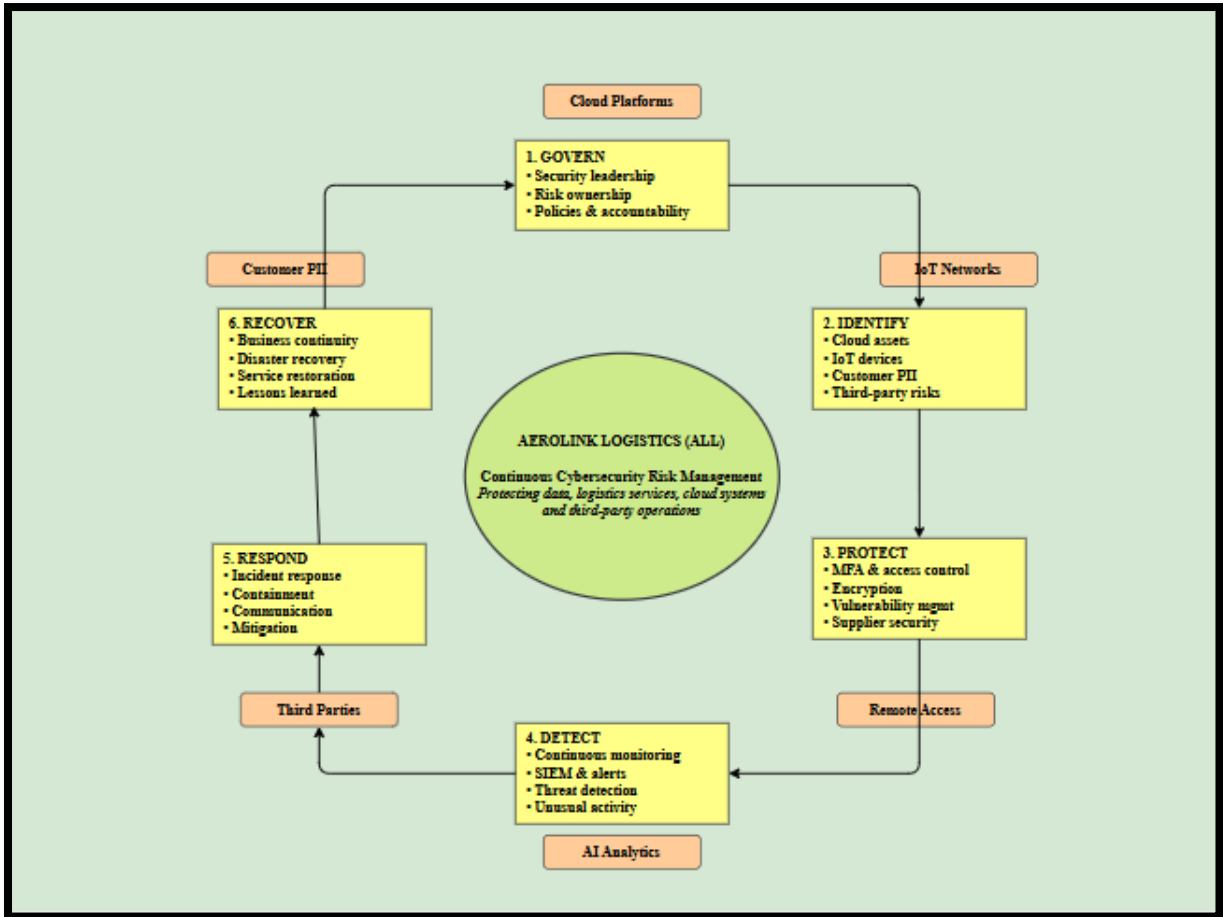


Figure 5: NIST CSF 2.0 Lifecycle

(Source: Self-developed)

3.3 ISO/IEC 27001 and ISO/IEC 27002

ISO/IEC 27001 helps in establishing an Information Security Management System (ISMS) while ISO/IEC 27002 supports the practical implementation of the security controls [17]. With respect to Aerolinks, fragmented governance and the absence of the formal security assurance often maximise the exposure towards the data breaches, along with adherence gaps. Therefore, successfully implementing an ISMS can help in formalising the risk assessments, responsibilities and finally the control monitoring [18]. However, its resource requirements mean that the company needs to prioritise controls as per its most critical operations and information risks.

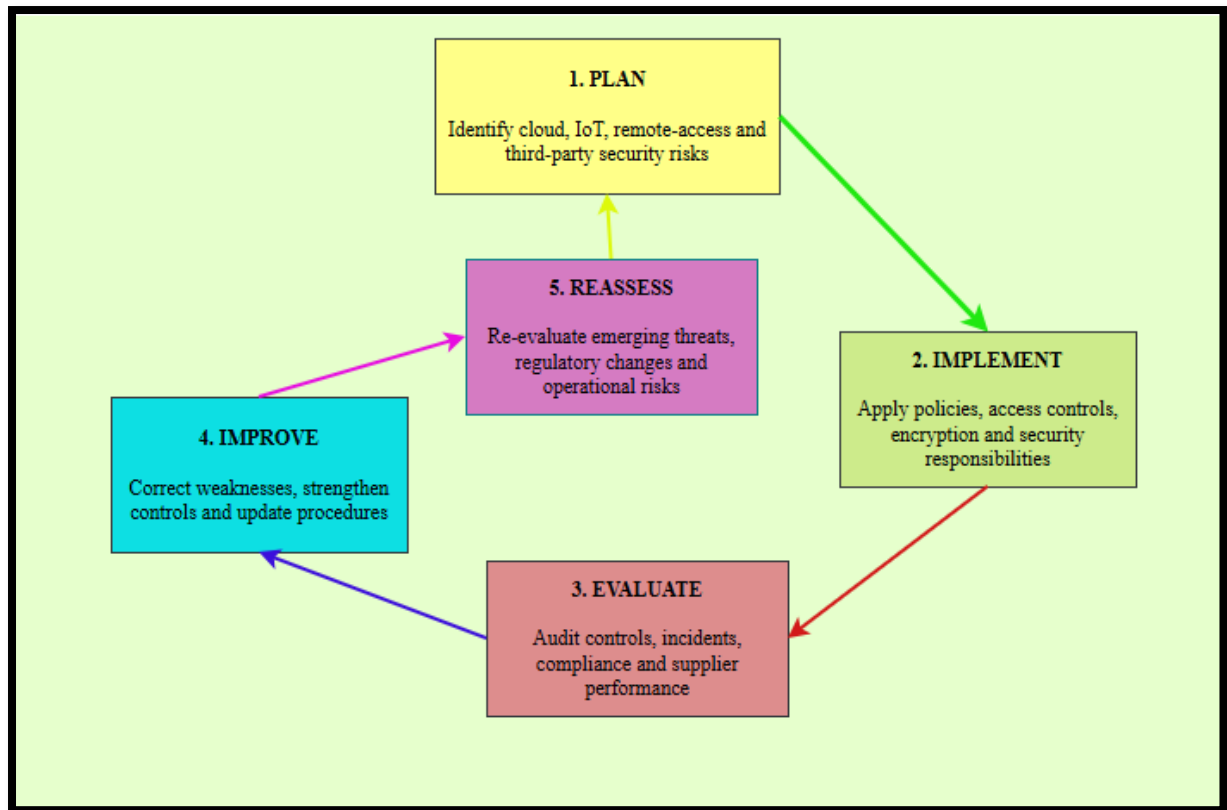


Figure 6: ISMS Continual Improvement Cycle

(Source: Self-developed)

3.4 COBIT 2019

COBIT 2019 focuses on governance, accountability, decision-making and performance, and thus extends the security management focused which has been previously established through the ISO/IEC 27001 [19]. With respect to Aerolinks, unclear responsibilities along with fragmented oversight can hinder control over both technology as well as external providers. In this context, COBIT can address this through the help of defined governance roles which closely align with the objectives and performance monitoring of the [20, 21]. However, unlike the ISO 27001's comprehensive ISMS orientation, COBIT is broader. As a result, the Aerolinks company is required to utilise this model to fortify its governance instead of replacing the operational security controls.

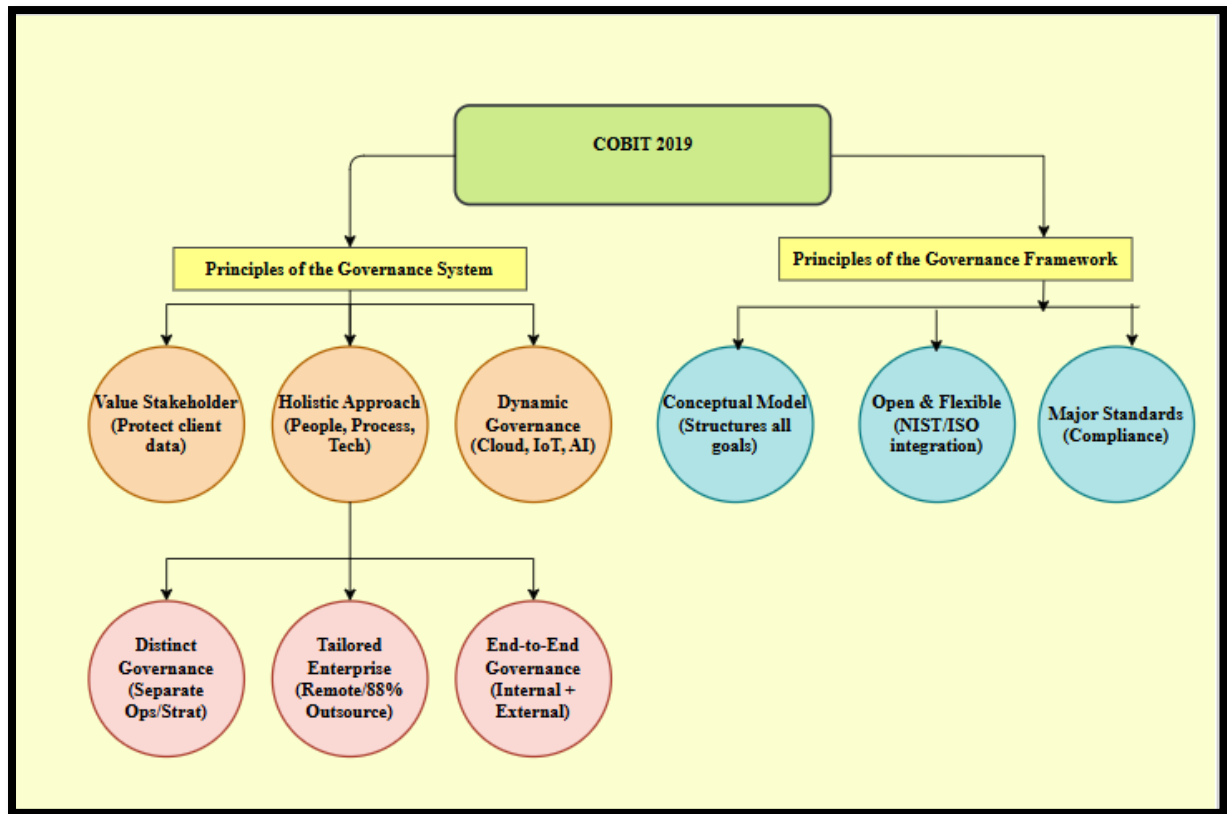


Figure 7: COBIT Governance and Management Relationship

(Source: Self-developed)

3.5 ITIL 4

ITIL 4 effectively supports IT service management through perfectly linking the service value, value streams, incident management and finally the continual [22, 23]. With respect to Aerolinks, this matters because disruptions towards the cloud-based tracking, warehousing and distribution services can quickly interrupt the continuity of logistics alongside client commitments. Besides that, its value-stream approach can assist in identifying where service weaknesses take place and thus enhance the delivery services, while incident management supports faster restoration. As a result, ITIL can help in fortifying the service availability of this logistics firm while maintaining operational consistency through the help of continual enhancements.

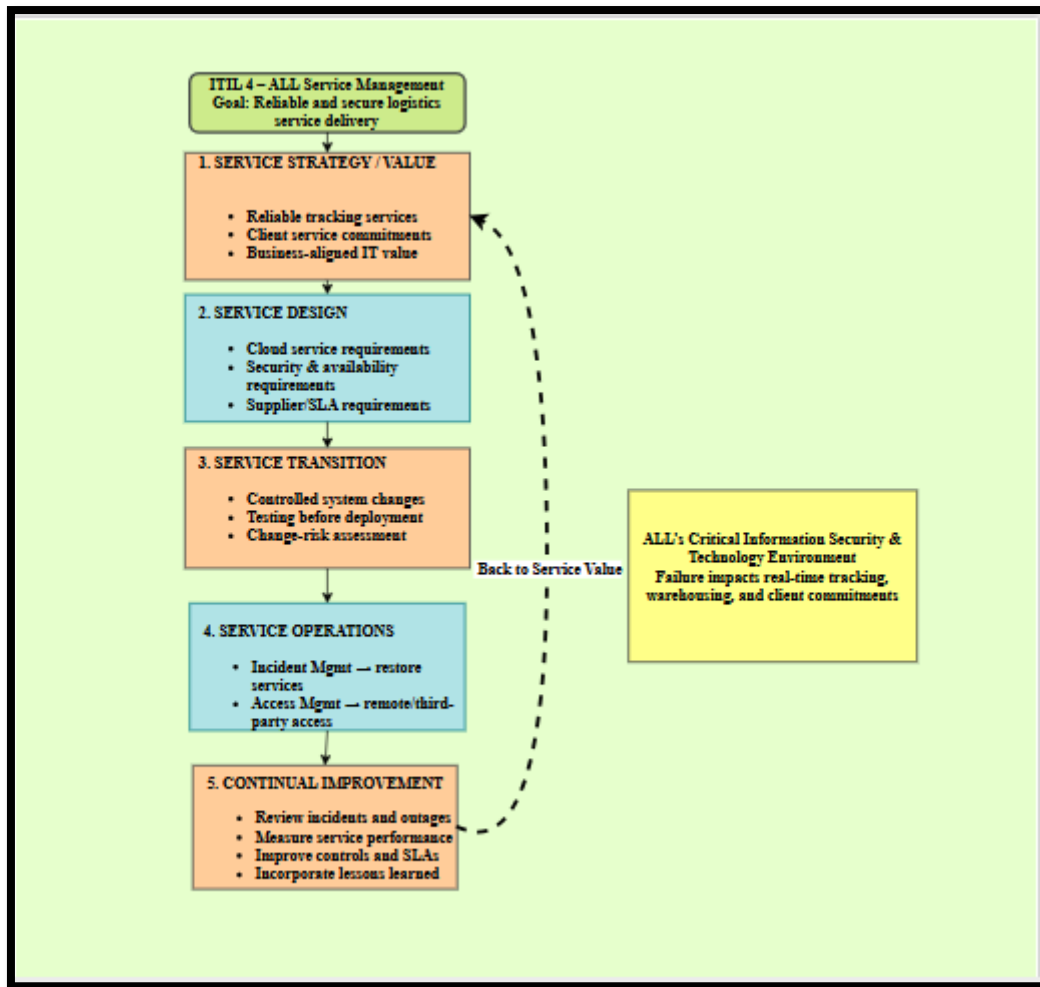


Figure 8: ITIL 4 Service Value System

(Source: Self-developed)

3.6 Zero Trust Security Model

Zero Trust assist in replacing implicit trust with continuous verification, least-privilege access, MFA and the micro segmentation and, thus making it specifically relevant to the remote workforce of Aerolinks in combination with the unmanaged devices and third-party connections as well [24]. Though NIST CSF 2.0 presents the greater cybersecurity risk management procedures and COBIT 2019 assists in addressing the governance, Zero Trust solely concentrates on effectively controlling access towards resources [25]. With respect to Aerolinks, embracing the zero trust model will assist in lowering unauthorised access while restricting the impact of compromised identities or devices.

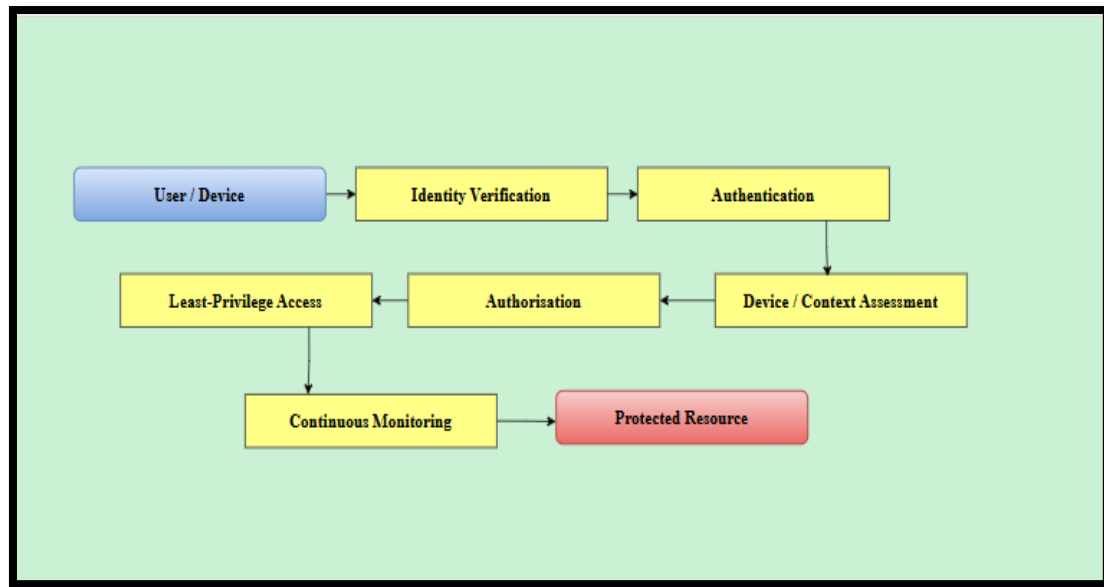


Figure 9: Zero Trust Model

(Source: Self-developed)

3.7 Comparative Evaluation and Selection

Framework	Primary Contribution	Key Strength	Main Limitation	Relevance to ALL	Recommended Role
NIST CSF	Cyber risk lifecycle	Flexible	Less prescriptive	High	Operational security [26].
ISO 27001	ISMS	Formal governance	Resource intensive	High	Security management
COBIT	IT governance	Accountability	Can be complex	High	Strategic governance
ITIL 4	IT service management	Service resilience	Not security-specific	Medium/High	Service operations
Zero Trust	Access security	Strong remote-access model	Implementation complexity	Very High	Access architecture [27].

Table 2: Comparative analysis

(Source: Self-developed)

4. Proposed Integrated Security Governance and Compliance Model for ALL

4.1 Design Rationale and Strategic Principles

The model prioritises business-security alignment, as fragmented responsibilities can disconnect the protection from the logistics objectives. Besides that, the risk-based decisions help in addressing the cloud, IoT and finally the third-party exposures of Aerolinks through concentrating resources on critical threats [28]. Moreover, regulatory compliance also lowers the existing data-protection gaps. Not only this, Zero Trust restricts crucial risks from remote and unmanaged access, while defence in depth presents layered protection against breaches [29]. Ultimately, continuous monitoring identifies suspicious activity within the interconnected environments, while continual enhancements ensure the controls evolve with incidents, emerging technologies or changing threats.

4.2 Integrated Security Governance Model

The model operates as a layered governance architecture with each approach effectively performing a distinct function. COBIT 2019 establishes the governance direction along with the accountability, while ISO 27001 translate this direction into an ISMS and a formal control environment [30]. On the flip side, the NIST CSF2.0 structures the overall activities of cybersecurity within the risk lifecycle, while ITIL 4 effectively embeds security within service delivery, incidents, as well as operational procedures [31]. Moreover, the Zero Trust model operates within these layers through consistently verifying identities, devices and finally access requests. At the implementation level, the Board, in combination with the Security Committee, provides oversight, whereas the CISO coordinates risk and security functions profoundly and ultimately the operational teams help in executing the controls, vendor management, incident response, as well as continuity activities *[refer to Appendix 1]*

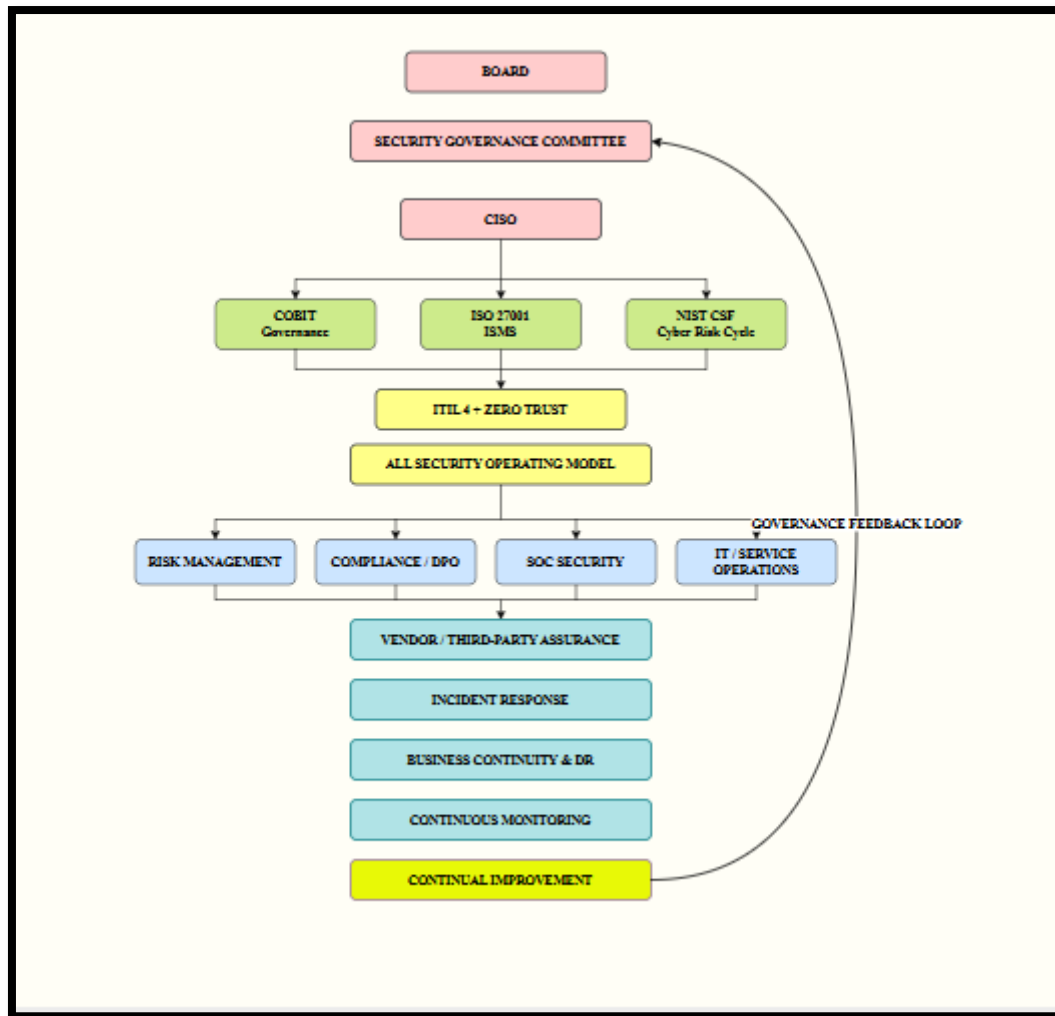


Figure 10: ALL Integrated Security Governance Model

(Source: Self-developed)

4.3 Accountability and Governance Arrangement

Aerolinks requires clearly separating the security responsibilities because its existing governance is fragmented, while the accountability is unclear as well. The Board is required to approve the security strategy along with the risk appetite, while the Security Governance Committee effectively coordinates the priorities across the business functions [32]. Moreover, the CISO needs to profoundly supervise the overall implementation procedures supported through risk, compliance/DPO, SOC and ultimately the IT operations teams [33]. Moreover, the vendor manager is required to enforce the security requirements through the help of both SLAs and assurance reviews. This structure helps to develop a sense of clear ownership from

the strategic oversight to the operational execution and thus enhances accountability, adherence, and finally coordinated responses towards security incidents.

4.4 Risk Identification, Treatment and Monitoring

Aerolinks requires a structured procedure as the cloud platforms, IoT devices, remote access and ultimately the extensive third-party reliance also create different forms of security exposure. Drawing on both ISO/IEC 27005 and the NIST risk management approach, first the crucial risks need to be identified across different critical assets, information and services before critically analysing their likelihood as well as business influence [34]. Moreover, prioritisation also needs to direct the resources towards the high-impact risks, specifically those influencing both the customer PII and logistics continuity as well. In addition, appropriate treatment might incorporate reducing, transferring, avoiding or accepting risks as per the defined risk appetite [*refer to Appendix 2*]. Furthermore, the continuous monitoring needs to track control effectiveness, incidents, supplier performance, and finally the emerging threats [35]. Moreover, regular review is also required as the technology, vulnerabilities, and finally the regulatory requirements change consistently. Therefore, this cycle will allow ALL to move from fragmented risk handling toward evidence-based, continuously reviewed security decisions.

4.5 Compliance, Legal and Ethical Considerations

ALL is required to closely align its security governance with the UK GDPR and the Data Protection Act 2018, supported through the relevant NIS obligations, along with the ISO/IEC 27001, Cyber Essentials Plus and NCSC guidance as well. However, adherence requires showing a sense of effective protection instead of simply attaining the certification [36]. Moreover, the ethical practices also require proportionate employee monitoring in combination with the responsible utilisation of data and AI, data minimisation, transparency and a sense of clear accountability [37]. This is specifically significant because the cloud, remote-working and the third-party agreements of the ALL incorporate both the organisational as well as personal information. Therefore, regular audits need to check compliance and whether security practices are fair and necessary.

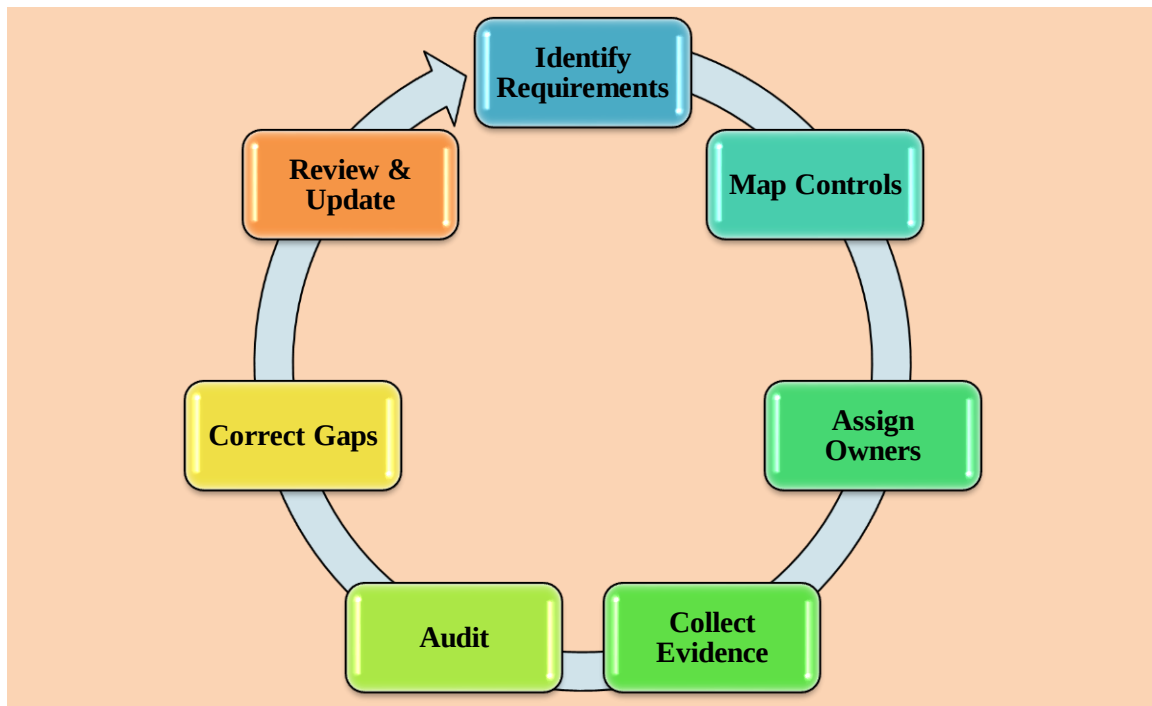


Figure 11: Compliance Mapping Lifecycle

(Source: Self-developed)

4.6 Vendor Security Management

The 88% outsourced IT infrastructure of Aerolinks makes vendor security a major governance concern, as weaknesses within the suppliers can not only hinder the cloud services but also directly affect sensitive information. Therefore, vendor management requires starting with security due diligence through critically investigating the suppliers before engagement and periodically thereafter [38]. Moreover, the SLAs also require specifying the requirements for data protection along with encryption, access control, incident reporting, availability, recovery and finally breach notifications. Unlike the simple contractual monitoring, continuous supplier assurance needs to incorporate audits, performance reviews and ultimately the evidence of control effectiveness [39]. Moreover, the clear responsibilities and escalation procedures are required to be established for the security failures. This approach allows Aerolinks to diminish third-party risks while effectively managing reliable as well as secure logistics services.

4.7 Resilience, Continuity and Incident Handling

The resilience strategy of Aerolinks requires prioritising the availability of the critical logistics services instead of solely concentrating only on preventing cyberattacks [40]. Besides that, the Business Impact Analysis (BIA) needs to identify the pivotal functions while establishing both

the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for tracking, warehousing and ultimately distribution [41]. Moreover, incident handling also requires defining the escalation, in combination with the communication and recovery priorities as well. In essence, it can be asserted that regular simulation exercises can disclose weaknesses within these arrangements, while the post-incident review requires converting the operational lessons into enhanced continuity planning.

4.8 Business Continuity and Disaster Recovery

ALL requires both Business Continuity Planning (BCP) and a Disaster Recovery Plan (DRP) because disruptions to the cloud platforms, IoT tracking, and outsourced services can hamper the overall supply chain and logistics operations of the firm. BCP needs to profoundly manage the essential business functions during the disruption, while DRP needs to restore the critical systems as well as data within the defined recovery requirements. Moreover, regular testing needs to verify whether the recovery procedures work under realistic disruption scenarios or not. In addition, the results from both testing as well as actual incidents need to be reviewed and used to enhance the recovery arrangements and thus ensure that Aerolinks can not only prepare but also respond, recover, resume and improve consistently, keeping pace with the volatile business market.

5. Critical Evaluation: Why Security Standards and Regulations Must Evolve.

Continuous updating of the security standards is required as the technology, threats, and finally the regulatory expectations develop faster than the static controls. Besides that, AI, generative AI, cloud and the IoT help in expanding both automation and connectivity, while quantum computing might eventually weaken the existing cryptographic protections [42]. Therefore, Aerolinks requires prioritising adaptive risk assessment in combination with stronger identity controls, encryption reviews and ultimately continuous monitoring instead of heavily depending on established safeguards indefinitely. In a similar way, different significant incidents like MOVEit, SolarWinds and the CrowdStrike-related disruption exemplified different weaknesses: supply chain exposure, trusted software compromise and finally the dependency on critical technology can bypass the assumptions underlying traditional security governance.

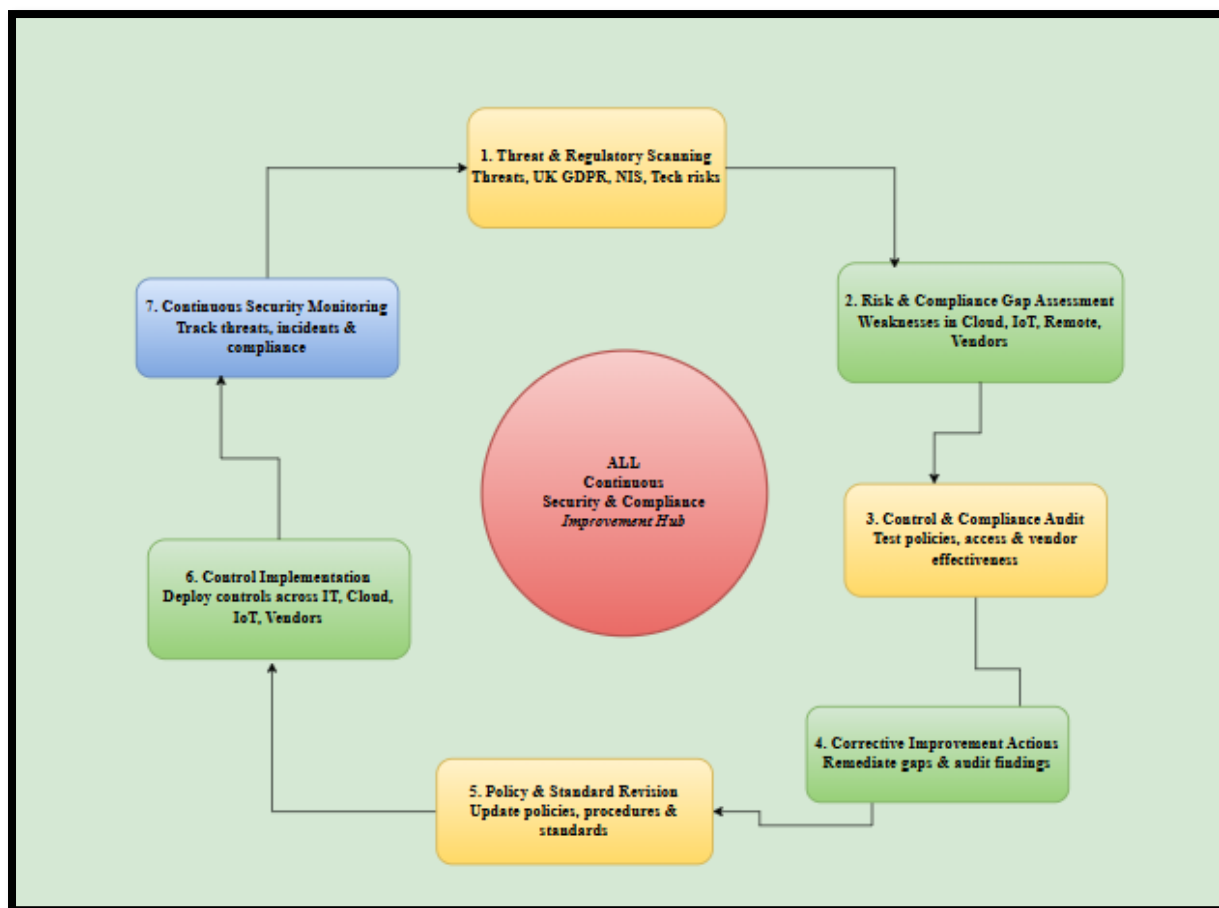


Figure 13: Continuous Security and Compliance Improvement Loop

(Source: Self-developed)

Compared with periodic reviews, continuous threat intelligence as well as reassessment will allow Aerolinks to identify zero-day vulnerabilities, ransomware techniques and ultimately credential attacks earlier and thus adjust the controls accordingly. Regulatory pressures also develop a similar need for change. Moreover, the UK GDPR, NIS/NIS2 developments, the EU AI Act, Cyber Essentials, ISO revisions and NIST updates increasingly require organisations to showcase current as well as risk-based security practices. Furthermore, updating the standards can enhance adaptability, regulatory alignment, risk visibility and finally stakeholder confidence. However, continual change can also create several issues like cost constraints, skill shortages, implementation demands, vendor dependencies and finally compliance fatigue [43]. With respect to Aerolinks, the solution is not to update the controls indiscriminately but also to prioritise the changes as per the emerging risk, regulatory significance as well as supplier

exposure of the logistics business. This makes the security governance adaptive rather than merely compliant.

6. Conclusion and Strategic Recommendations

6.1 Conclusion

The analysis found that Aerolinks cannot address its interconnected security weakness through the help of single framework. In these circumstances, amalgamation the COBIT 2019, ISO/IEC 27001, NIST CSF 2.0, ITIL 4 and Zero Trust presents complementary governance, risk, service and access protection. Moreover, the integrated model also clarifies accountability, fortifies adherence, and thus assists in enhancing adaptability across cloud, IoT, remote access and third-party environments. Ultimately, it moves Aerolinks from fragmented security practices towards coordinated yet risk-based and gradually enhancing governance.

6.2 Strategic Recommendations

Short-term:

In the short term, this logistics company requires to establish the Security Governance Committee while confirming the CISO and RACI responsibilities, perform enterprise-wide risk assessments, and address the immediate weakness through the help of MFA, least-privilege access, encryption and finally the critical reviews of the vendor [44].

Medium-term:

In the medium term, the organisation requires to successfully implement the ISO 27001-based ISMS while fortifying the NIST-aligned monitoring as well as incident response, formalise the supplier SLAs, perform the GDPR adherence reviews and finally test the BCP/DRP arrangements *[refer to Appendix 3]*.

Long-term:

Aerolinks requires to successfully embed the Zero Trust frameworks within its cloud, remote and third-party access, develop mature threat intelligence capabilities, and finally needs to reassess the controls against the emerging technologies and changing regulations [45]. Moreover, regular audits, scenario testing, along with management reviews, need to support the continuous enhancements. This phased approach is preferable as it will allow the Aerolinks

company to prioritise the high-risk weaknesses first, manage the implementation capacity effectively and ultimately fortify organisational adaptability.

References

1. Alotaibi, B., 2023. A survey on industrial Internet of Things security: Requirements, attacks, AI-based solutions, and edge computing opportunities. *Sensors*, 23(17), p.7470. <https://www.mdpi.com/1424-8220/23/17/7470>
2. GOV.UK (2026). *Cyber security breaches survey 2025/2026*. Available from <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026>. Accessed on 8.8.2026
3. Alamu, R., The Role of IT Governance in Enhancing Organizational Cybersecurity. https://www.researchgate.net/profile/Rapheal-Alamu/publication/389966358_The_Role_of_IT_Governance_in_Enhancing_Organizational_Cybersecurity/links/67da8ec18901690dd03ae4e3/The-Role-of-IT-Governance-in-Enhancing-Organizational-Cybersecurity.pdf
4. Nagaty, K.A., 2023. IoT commercial and industrial applications and AI-powered IoT. In *Frontiers of quality electronic design (QED) AI, IoT and hardware security* (pp. 465-500). Cham: Springer International Publishing. https://www.researchgate.net/profile/Khaled-Nagaty/publication/367025439_IoT_Commercial_and_Industrial_Applications_and_AI-Powered_IoT/links/63d61ee5c97bd76a8244aee8/IoT-Commercial-and-Industrial-Applications-and-AI-Powered-IoT.pdf
5. Hossain, M.I., Sultana, T., Islam, M.N.U., Akther, A., Sarpong, A.F. and Akter, F., 2025. Enhancing Project Management through Outsourcing: Transforming Growth in Information Technology (IT). *Journal of Knowledge Management Practice*, 25(1), p.37. https://www.researchgate.net/profile/Tanzina-Sultana/publication/388838046_Enhancing_Project_Management_through-Outsourcing_Transforming_Growth_in_Information_Technology_IT/links/67be0a1bf5cb8f70d5bff7bf/Enhancing-Project-Management-through-Outsourcing-Transforming-Growth-in-Information-Technology-IT.pdf
6. Oubousken, I., 2026. Cloud Misconfiguration Audit. https://www.theseus.fi/bitstream/handle/10024/924411/Oubousken_Ilyas.pdf?sequence=2

7. Amutha, K.P., Mehanath, N., Karthikeyan, K. and Shanmuganeethi, V., 2026. Internet of Things Applications for Real-Time Monitoring and Tracking: IoT Insights and Real-Time Tracking. In *Industry 6.0 and Digital Transformation in Supply Chain, Assets, and Services* (pp. 101-130). IGI Global Scientific Publishing. <https://www.igi-global.com/chapter/internet-of-things-applications-for-real-time-monitoring-and-tracking/401657>
8. Mallick, M.A.I. and Nath, R., 2024. Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News*, 190(1), pp.1-69. <https://worldscientificnews.com/wp-content/uploads/2024/01/WSN-1901-2024-1-69-1.pdf>
9. Baligodugula, V.V., Ghimire, A. and Amsaad, F., 2024. An overview of secure network segmentation in connected IIoT environments. *Computing&AI Connect*, 1(1), pp.1-10. <https://www.scifiniti.com/uploads/source/articles/computingai-connect/2024/volume1/20240004/article.pdf>
10. 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>
11. Adinata, A.S., 2024. The evaluation of integrated governance, risk, and compliance (GRC) implementation to enhance enterprise risk management (ERM): a case study. *PhD, Faculty of Business & Media, Selinus University of Science and Literature, Indonesia*. <https://uniselinus.education/sites/default/files/2025-03/Ahmed%20Seki%20Adinata.pdf>
12. Brass, M., 2025. *Governance, Risk and Compliance: Demystifying the Risk and Data Privacy Landscape*. CRC Press. [https://books.google.com/books?hl=en&lr=&id=dEyWEQAAQBAJ&oi=fnd&pg=PT7&dq=Information+and+security+governance+establishes+the+organisational+direction+through+closely+aligning+the+governance,+risk+and+compliance+\(GRC\)+with+strategic+decision-making.+&ots=YVF-BfWD8C&sig=nQwbKwTgopUHiQzZY0Y8JE4R-x0](https://books.google.com/books?hl=en&lr=&id=dEyWEQAAQBAJ&oi=fnd&pg=PT7&dq=Information+and+security+governance+establishes+the+organisational+direction+through+closely+aligning+the+governance,+risk+and+compliance+(GRC)+with+strategic+decision-making.+&ots=YVF-BfWD8C&sig=nQwbKwTgopUHiQzZY0Y8JE4R-x0)
13. Jain, A., 2025. Governance, Risk, and Compliance (GRC) Frameworks Using Intelligent Analytics. *International Journal of Computer Technology and Electronics Communication*, 8(6), pp.11716-11721. <https://ijcte.com/index.php/IJCTEC/article/download/380/338>

14. Sahiwala, F., 2026. An integrated risk management approach using the NIST CSF-2.0, NIST 800-82, and IEC 62443 frameworks. https://www.theseus.fi/bitstream/handle/10024/913159/Sahiwala_Fatema.pdf?sequence=2
15. Awurum, N.P., 2026. A Governance Framework for Aligning Artificial Intelligence–Driven Cybersecurity with NIST CSF 2.0 and IEC 62443 in Critical Infrastructure. *Indiana Journal of Economics and Business Management*, 6(4), pp.74-103. [https://indianapublications.com/articles/IJEBM_6\(4\)_74-103_6a68f5eeeb0a23.49971237.pdf](https://indianapublications.com/articles/IJEBM_6(4)_74-103_6a68f5eeeb0a23.49971237.pdf)
16. Kate, A., 2026. Operationalizing the NIST CSF 2.0 “Govern” Function for AI-Augmented Critical Infrastructure Protection: Policy, Accountability, and Risk Ownership Models. https://www.researchgate.net/profile/Austin-Kate-2/publication/403508974_Operationalizing_the_NIST_CSF_20_Govern_Function_for_AI-Augmented_Critical_Infrastructure_Protection_Policy_Accountability_and_Risk_Ownership_Models/links/69d10fb49f53d47411c46806/Operationalizing-the-NIST-CSF-20-Govern-Function-for-AI-Augmented-Critical-Infrastructure-Protection-Policy-Accountability-and-Risk-Ownership-Models.pdf
17. 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=ISO/IEC+27001+helps+in+establishing+an+Information+Security+Management+System+\(ISMS\)+while+ISO/IEC+27002+supports+the+practical+implementation+of+the+security+controls.+&ots=qAM5X-L_IS&sig=ULt052oG3-bOo6B1Cj3un8Oa2mA](https://books.google.com/books?hl=en&lr=&id=5s_BEQAAQBAJ&oi=fnd&pg=PR13&dq=ISO/IEC+27001+helps+in+establishing+an+Information+Security+Management+System+(ISMS)+while+ISO/IEC+27002+supports+the+practical+implementation+of+the+security+controls.+&ots=qAM5X-L_IS&sig=ULt052oG3-bOo6B1Cj3un8Oa2mA)
18. Calder, A., 2023. ISO 27001/ISO 27002: A guide to information security management systems. <https://www.torrossa.com/gs/resourceProxy?an=5751056&publisher=FZO328>
19. Metin, B., Sevim, S.B. and Wynn, M., 2025. Cybersecurity Strategy Development: Towards an Integrated Approach Based on COBIT and ISO 27000 Series Standards. *Standards*, 5(4), p.33. <https://www.mdpi.com/2305-6703/5/4/33>

20. El Marzak, Y., Chahid, A., Faris, S. and Mansouri, K., 2026. Enhancing a NIST SP 800-53-Based Cybersecurity Risk Metamodel with COBIT 2019: A Governance-Centric Perspective. *Engineering, Technology & Applied Science Research*, 16(2), pp.33689-33695. <https://mail.etasr.com/index.php/ETASR/article/download/17097/6433>
21. Herath, T.C., Herath, H.S. and Cullum, D., 2023. An information security performance measurement tool for senior managers: Balanced scorecard integration for security governance and control frameworks. *Information Systems Frontiers*, 25(2), pp.681-721. https://www.researchgate.net/profile/Hemantha-Herath/publication/358909388_An_Information_Security_Performance_Measurement_Tool_for_Senior_Managers_Balanced_Scorecard_Integration_for_Security_Governance_and_Control_Frameworks/links/6390a7aa484e65005bee951c/An-Information-Security-Performance-Measurement-Tool-for-Senior-Managers-Balanced-Scorecard-Integration-for-Security-Governance-and-Control-Frameworks.pdf
22. Harjanto, A. and Aji, R.F., 2024. Improving IT assets management with ITIL 4 framework. *Jurnal Ilmu Komputer dan Informasi*, 17(2), pp.127-143. <https://jiki.cs.ui.ac.id/index.php/jiki/article/download/1195/518>
23. Dhanabal, P., 2025. Demystifying ITIL-based incident management in cloud environments. *Journal of Computer Science and Technology Studies*, 7(8), pp.892-903. <https://alkindipublisher.com/index.php/jcsts/article/download/10652/9400>
24. Gambo, M.L. and Almulhem, A., 2026. Zero trust architecture: A systematic literature review. *Journal of Network and Systems Management*, 34(1), p.25. <https://arxiv.org/pdf/2503.11659>
25. Dalal, A., 2025. Designing zero trust security models to protect distributed networks and minimize cyber risks. Available at SSRN 5268092. <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5268092>
26. 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>

27. Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K.U. and Hamid, Y., 2024. A review and comparative analysis of relevant approaches of zero trust network model. *Sensors*, 24(4), p.1328. <https://www.mdpi.com/1424-8220/24/4/1328>

28. Rasner, G.C., 2021. *Cybersecurity and third-party risk: Third party threat hunting*. John Wiley & Sons. <https://books.google.com/books?hl=en&lr=&id=mw8zEAAAQBAJ&oi=fnd&pg=PT6&dq=+the+risk-based+decisions+help+in+addressing+the+cloud,+IoT+and+finally+the+third-party+exposures+of+Aerolinks+through+concentrating+resources+on+critical+threats.&ots=av7D7PDAD&sig=joAMxvkJTNxX7yS0Z4faLz64q8Y>

29. Jena, A., Bhardwaj, A., Murmu, R., Seeralan, P., Gupta, M. and Sharman, R., 2025. Identifying Opportunities in the Enhancement of an Organization's Third-Party Risk Posture. In *Advances in Enterprise Technology Risk Assessment* (pp. 99-136). IGI Global Scientific Publishing. <https://www.igi-global.com/chapter/identifying-opportunities-in-the-enhancement-of-an-organizations-third-party-risk-posture/358654>

30. 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. <https://journal.universitاسbumigora.ac.id/matrik/article/download/5628/2267>

31. Briain, D.Ó., 2026. Workshop Notes. [https://www.obriain.com/training/nis2-maritime/Cybersecurity in Maritime Domain \(Rosslare\) odt v1.0.2.pdf](https://www.obriain.com/training/nis2-maritime/Cybersecurity%20in%20Maritime%20Domain%20(Rosslare)%20odt%20v1.0.2.pdf)

32. Agarwal, K. and Shah, M., 2024. The role of corporate governance in managing cybersecurity risks: A comprehensive analysis. *LawFoyer Int'l J. Doctrinal Legal Rsch.*, 2, p.352. https://access.heinonline.com/hol/cgi-bin/get_pdf.cgi?handle=hein.journals/lwfyrinl2§ion=23

33. Mitcham, Z.S. and MSA, C., 2024. *Key Security Concepts that all CISOs Should Know- Cyber Guardians: A CISO's Guide to Protecting the Digital World*. eBookIt. com. <https://books.google.com/books?hl=en&lr=&id=30YEEQAAQBAJ&oi=fnd&pg=PA1&dq=Besides+that,+the+CISO+helps+in+developing+the+security+strategy+along+side+coordina>

[tes+the+SOC+with+risk+and+security+operations.&ots=rn_GhWYJ-4&sig=fPHMoKRpcY7n2QMu4jXZUNEV3J4](https://www.sciencedirect.com/science/article/pii/S2667096825000527)

34. Gokkaya, B., Spanaki, K. and Karafili, E., 2025. Strengthening the UK regulatory framework: Enhancing cybersecurity in supply chains. *International Journal of Information Management Data Insights*, 5(2), p.100370. <https://www.sciencedirect.com/science/article/pii/S2667096825000527>

35. Dekker, M. and Alevizos, L., 2024. A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making. *Security and Privacy*, 7(1), p.e333. <https://onlinelibrary.wiley.com/doi/pdfdirect/10.1002/spy2.333>

36. Safitri, E.H.N. and Kabetta, H., 2023, August. Cyber-Risk Management Planning Using NIST CSF V1. 1, ISO/IEC 27005: 2018, and NIST SP 800-53 Revision 5 (A Study Case to ABC Organization). In *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)* (pp. 332-338). IEEE. <https://ieeexplore.ieee.org/abstract/document/10277652/>

37. Aloisi, A. and Gramano, E., 2019. Artificial intelligence is watching you at work: Digital surveillance, employee monitoring, and regulatory issues in the EU context. *Comp. Lab. L. & Pol'y J.*, 41, p.95. <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=3399548>

38. Gema, D., 2026. *Managing IT Suppliers: A Practical Guide to Vendor Management*. CRC Press. <https://books.google.com/books?hl=en&lr=&id=NjyfEQAAQBAJ&oi=fnd&pg=PT5&dq=vendor+management+requires+starting+with+security+due+diligence+through+critically+investigating+the+suppliers+before+engagement+and+periodically+thereafter.&ots=mjL0DkkPlA&sig=ZL7sfAvckvXVw7Dugr25AlsVhJE>

39. Jyoti, S.N. and Akter, M., 2022. Assessment Of Data-Driven Vendor Performance Evaluation in Retail Supply Chains: Analyzing Metrics, Scorecards, And Contract Management Tools. *American Journal of Interdisciplinary Studies*, 3(02), pp.36-61. <https://ajisresearch.com/index.php/ajis/article/download/30/28>

40. Zamykalová, Š., 2025. Critical but also strategic infrastructure must be more resilient than ever. *Central European Journal of Security Studies*, 3(1), pp.76-84.
<https://bibliotekanauki.pl/articles/63884604.pdf>
41. Mohammed, S., 2024. Resilient multi-region cloud architecture for high availability and disaster recovery. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 7(4), pp.10869-10873.
<https://ijrpetm.com/index.php/IJRPETM/article/download/561/530>
42. Ali, G., Samuel, A., Kabiito, S.P., Morish, Z., Thomas, A., Robert, W., Denis, A., Sallam, M., Mijwil, M.M., Ayad, J. and Salau, A.O., 2025. Integration of artificial intelligence, blockchain, and quantum cryptography for securing the industrial internet of things (IIoT): Recent advancements and future trends. *Applied Data Science and Analysis*, 2025, pp.19-82.
<https://journals.mesopotamian.press/index.php/ADSA/article/download/757/1144>
43. Mageed, I.A., 2025. Issues and challenges in transforming management practices through agility. *Systemic analytics*, 3(2), pp.91-111. <https://sa-journal.org/index.php/systemic/article/download/46/57>
44. Stevens, A., 2025. *Enterprise Fortress: The Ultimate Handbook for Enterprise Security Architecture*. CRC Press.
<https://books.google.com/books?hl=en&lr=&id=WfdCEQAAQBAJ&oi=fnd&pg=PP1&dq=Security+Governance+Committee+while+confirming+the+CISO+and+RACI+responsibilities,+perform+enterprise-wide+risk+assessments,+and+address+the+immediate+weakness+through+the+help+of+MFA,+least-privilege+access,+encryption+and+finally+the+critical+reviews+of+the+vendor.+&ots=5rDMvFLoyM&sig=zuqLQa26pCx2d31XhaJxS1Jzabs>
45. Mdaki, J., 2025. A hybrid cybersecurity framework for small businesses: integrating NIST CSF, ISO 27001, and CEO engagement.
https://www.theseus.fi/bitstream/handle/10024/891475/Mdaki_Jacob.pdf?sequence=2

Appendices

Appendix 1: RACI Matrix

Security Activity	Board	Security Governance Committee	CISO	Risk Management	DPO / Compliance	SO C	IT Operations	Vendor Management
Security strategy & risk appetite	A	R	C	C	C	I	I	I
Enterprise security risk assessment	I	A	R	R	C	C	C	C
ISMS & security policies	I	A	R	C	C	C	R	I
GDPR & regulatory compliance	I	A	C	C	R/A	I	C	C
Cloud & IoT security controls	I	A	R	C	I	R	R	C
Remote access & Zero Trust	I	A	R	C	I	R	R	C
Third-party security & SLA assurance	I	A	C	C	C	C	C	R
Security monitoring & threat detection	I	A	A	C	I	R	C	I
Incident response & escalation	I	A	A	C	C	R	R	C

Business continuit y & disaster recovery	A	R	C	R	C	C	R	C
Security performa nce & continual improve ment	I	A	R	C	C	R	C	C

Appendix 2: ALL Cybersecurity Risk Register

Risk	Likelihood	Impact	Risk Owner	Control Response
PII breach	High	Very High	CISO	MFA, encryption, Zero Trust
Cloud misconfiguration	High	High	IT	Secure configurations, audits
IoT compromise	High	High	CISO	Segmentation, patching, monitoring
Unmanaged devices	High	High	CISO	MFA, endpoint controls
Vendor failure	High	Very High	Vendor Manager	Due diligence, SLA controls
Cyberattack	Medium	Very High	SOC	Monitoring, incident response
GDPR non-compliance	Medium	High	DPO	Audits, compliance reviews
Service disruption	Medium	Very High	IT	BCP, disaster recovery
Poor incident response	Medium	High	SOC	Response procedures, testing
Emerging threats	Medium	High	Risk Manager	Continuous risk review

Appendix 3: Strategic Recommendations Implementation Gantt Chart

Recommendation	0–3 Months	4–6 Months	7–12 Months	12+ Months
Governance and RACI				
Risk assessment & priority controls				
ISO 27001 ISMS				
Vendor & SLA assurance				
Incident response and BCP/DRP				
Zero Trust implementation				
Continuous monitoring and improvement				
Emerging-threat and regulatory review				