



LEVEL 7 ASSESSMENT SPECIFICATION

Programme: MSc Cybersecurity and Digital Forensics

Module: Data Security, Governance and Compliance

Module code: ACCA7028

Lecturer: Dr Ayman El Hajjar

***TOPIC: CRITICAL EVALUATION AND INTEGRATED
CYBERSECURITY GOVERNANCE FRAMEWORK FOR
AEROLINK LOGISTICS (ALL)***

Student name: Sneha Parth bhesaniya

Student id:2544720

Abstract

This report profoundly analyses AeroLink Logistics' (ALL) cybersecurity governance, risk and ultimately the compliance challenges within the outsourced as well as digitally dependent operating environment. It critically assesses the NIST CSF 2.0, ISO/IEC 27001/27002, COBIT 2019, ITIL 4, Zero Trust and the Cloud Shared Responsibility Model, and thus identifies their respective strengths as well as limitations for ALL. The analysis closely integrates the UK legal, regulatory, as well as ethical requirements in combination with the risks emerging from the cloud services, IoT, and remote access, third parties and finally the data processing. Moreover, an integrated security governance framework is proposed, supported through the defined accountability, risk management, technical controls, incident response, business continuity and finally consistent assurance. In addition, the prioritised recommendations offer this business with a practical roadmap towards stronger adaptability, adherence, as well as sustainable cybersecurity governance.

Table of Contents

1. Introduction.....	4
1.1 Background.....	4
1.2 Problem Statement.....	5
1.3 Aim and Objectives.....	5
2. AeroLink Logistics: Organisation Background and Case Analysis.....	6
2.1 Organisation Overview.....	6
2.2 Security, Governance and Compliance Challenges.....	7
2.3 Assumptions and Design Context.....	8
3. Research and Critical Evaluation of Information Security Frameworks and Models.....	9
3.1 Information Security Governance and GRC Overview.....	9
3.2 NIST Cybersecurity Framework 2.0.....	10
3.3 ISO/IEC 27001:2022 and ISO/IEC 27002.....	11
3.4 COBIT 2019.....	12
3.5 ITIL 4.....	13
3.6 Zero Trust Architecture.....	14
3.7 Cloud Shared Responsibility Model.....	15
3.8 Comparative Critical Evaluation and Framework Selection.....	15
4. Proposed Integrated Security Governance Framework.....	16
4.1 Proposed Integrated Framework Overview.....	16
4.2 Governance and Strategic Security Structure.....	17
4.3 Enterprise Cyber Risk Management.....	18
4.4 Security Policies, Data Governance and Procedures.....	18
4.5 Compliance, Legal and Ethical Governance.....	19
4.6 Vendor and SLA Security Management.....	19
4.7 Incident Response and Cyber Crisis Management.....	20
4.8 Business Continuity and Disaster Recovery.....	20
5. Critical Discussion: Why Continuous Updates to Regulations and Standards Are Necessary	22
6. Recommendations and Implementation Roadmap.....	23
7. Conclusion.....	25
References.....	26

1. Introduction

1.1 Background

Digital transformation is drastically transforming the overall logistics through the help of cloud platforms, IoT, AI analytics and remote connectivity and thus enhancing visibility along with operational effectiveness [1].

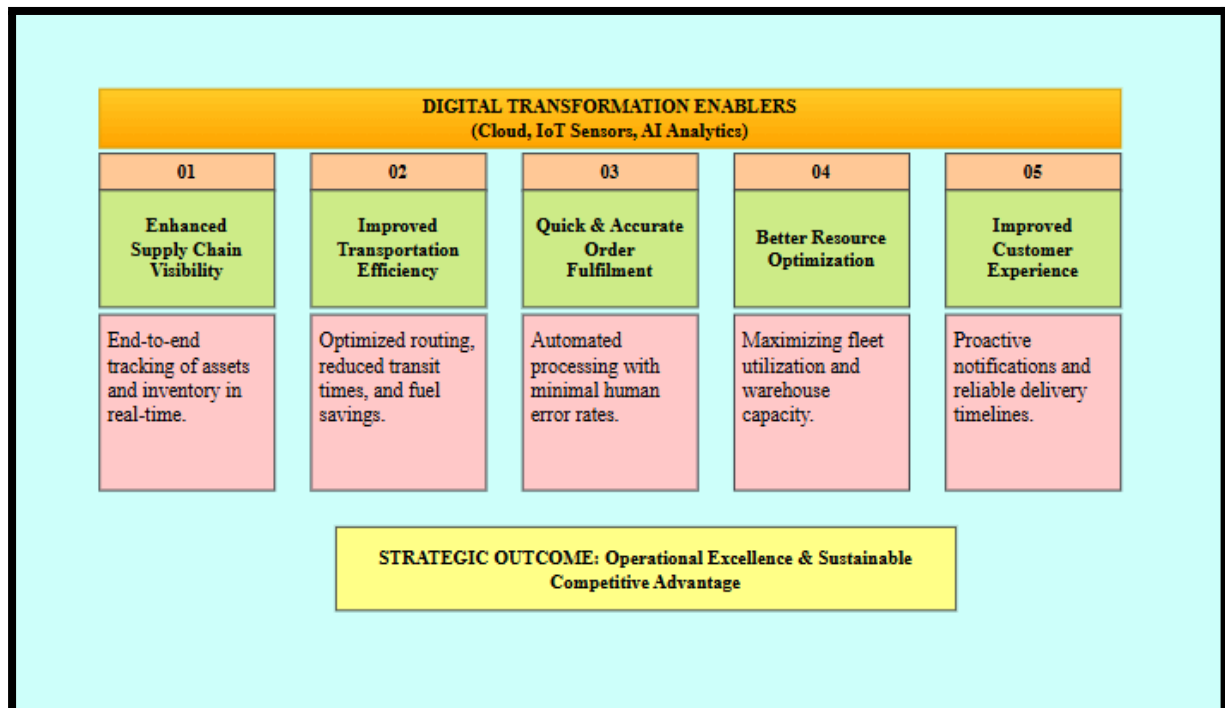


Figure 1: Advantages of digital transformation in logistics

(Source: Self-developed)

AeroLink Logistics (ALL) increasingly rely on cloud computing, IoT-powered tracking, as well as AI-powered analytics to support its multinational logistics operations. Though these technologies assist in enhancing operational visibility alongside effectiveness, they also expand the interconnected security dependencies. The combination of remote access, third-party platforms and unmanaged devices maximises the exposure towards cyber threats and thus makes effective governance and accountability pivotal alongside the technical security controls [2].

1.2 Problem Statement

The security weakness of ALL is primarily a governance problem instead of an isolated technical deficiency. With approximately 88% of its IT infrastructure outsourced through IaaS and SaaS, repeated breaches incorporating the shipment data in combination with the PII expose weaknesses within risk management, vendor accountability, encryption, incident response and ultimately compliance auditing [3]. The absence of a unified security framework further maximises the organisational exposures.

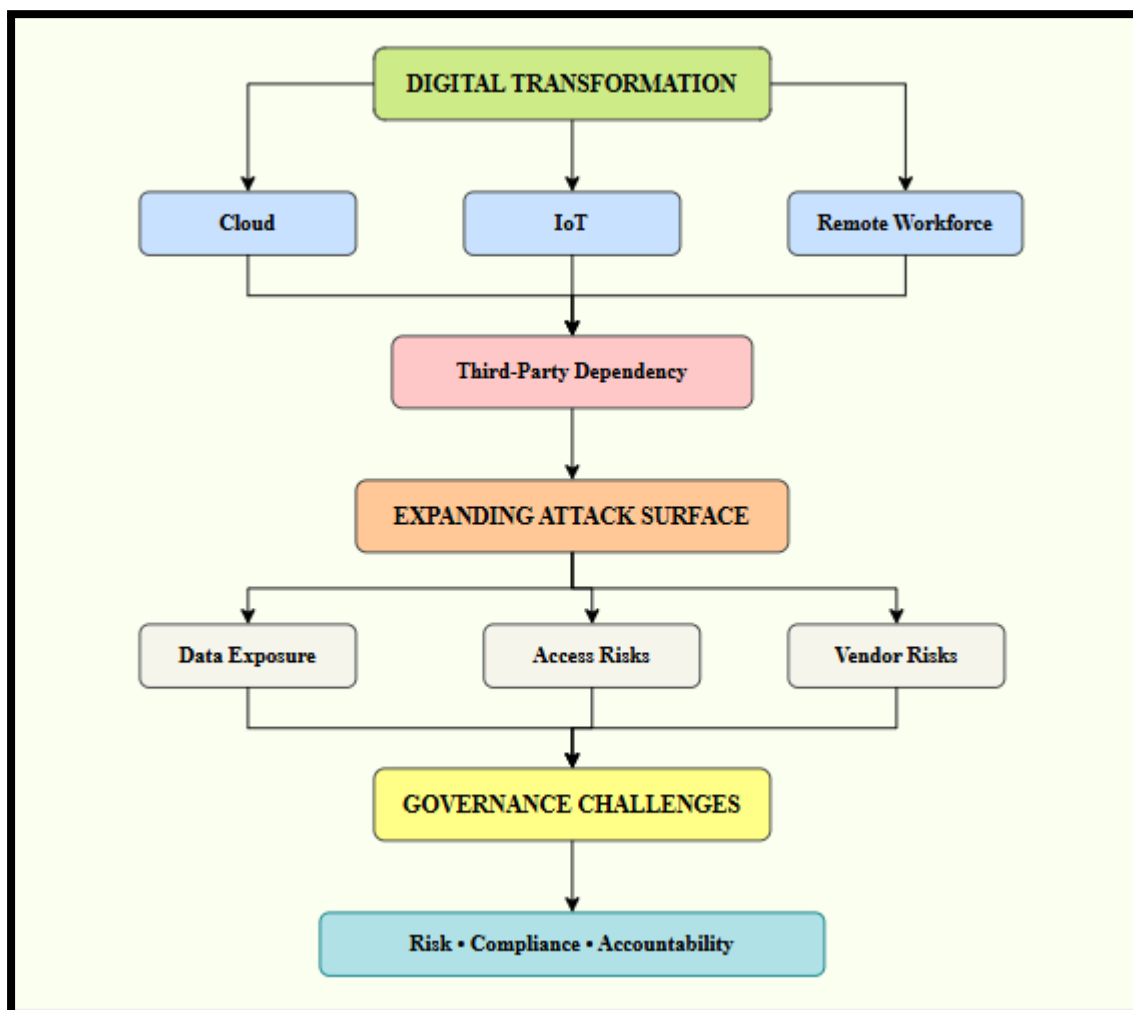


Figure 2: Digital Transformation Vs Expanding Attack Surface

(Source: Self-developed)

1.3 Aim and Objectives

Aim

The aim of this study is to profoundly investigate the relevant security frameworks and models and utilise their complementary capabilities to develop an integrated governance, risk and adherence approach for AeroLink Logistics (ALL).

Objectives

- To critically assess the key security frameworks and models.
- To profoundly investigate the security, governance, as well as compliance gaps of ALL.
- To analyse the relevant legal and ethical requirements.
- To recommend measurable controls for both adaptability and enhancements.

2. AeroLink Logistics: Organisation Background and Case Analysis

2.1 Organisation Overview

AeroLink Logistics (ALL) operates its business within the multinational logistics sector where transportation, warehousing and distribution rely increasingly on digital coordination. Besides that, real-time tracking, IoT systems, cloud platforms, and finally AI analytics support operational visibility within its activities [4]. This digitally connected model closely links ALL with the employees, suppliers and logistics partners across different locations. Therefore, the operating structure is not completely controlled internally; it also depends substantially on the external IaaS and SaaS providers for transforming how technology-powered services are delivered.

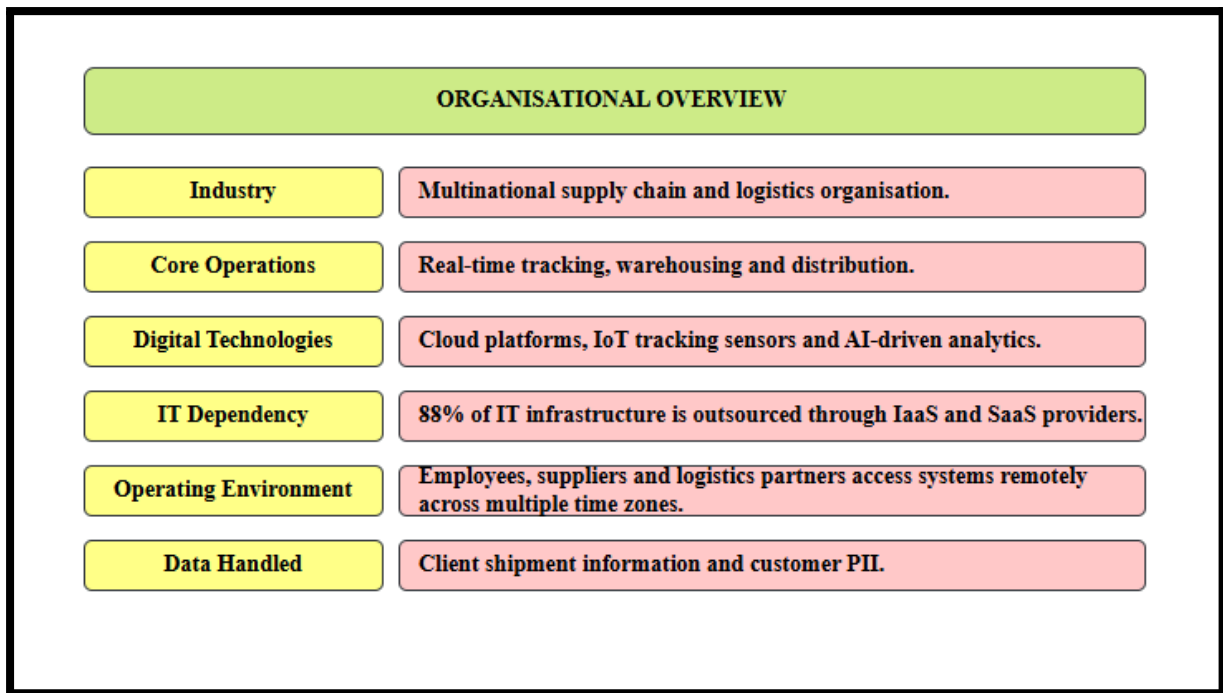


Figure 3: Organisational overview

(Source: Self-developed)

2.2 Security, Governance and Compliance Challenges

The principal weakness of this company depends on the interaction between technological reliance as well as governance fragmentation. Its 88% outsourced IT infrastructure creates greater third-party exposures compared to internally controlled environments, while the remote access through the unmanaged devices maximises the levels of uncertainty over who can access the corporate resources and under what conditions [5]. Previous breaches incorporating the shipment information along with PII showcase that these concerns are already material instead of hypothetical. At the governance level, the absence of a unified security framework along with centralised risk management restricts consistent risk ownership and prioritisation as well [6,7]. This is compounded through immature compliance auditing, vendor-accountability concerns, encryption weaknesses, and finally the gaps across incident response and thus turning isolated failures into profound operational consequences.

2.3 Assumptions and Design Context

Area	Assumption	Rationale / Impact
------	------------	--------------------

Company size	Medium-to-large multinational	It profoundly supports scalable yet enterprise-level controls
Headquarters	UK-based headquarters	It profoundly supports the requirements of UK GDPR/DPA
Regulatory	UK regulatory context	Supports the strict GDPR/DPA compliance [8].
Cloud	Outsourced IaaS/SaaS environment	Requires shared security responsibility
Security maturity	Immature governance	Requires foundational controls first [9].
Budget	Moderate resources	It supports the phased implementation
Security Operations	Limited centralised monitoring	Requires both stronger detection as well as response [10].
Access	Remote access via unmanaged devices	Requires both Zero Trust along with MFA
Third parties	High vendor dependency	Requires stronger oversight from the vendors

Table 1: Assumptions and Design Context

(Source: Self-developed)

3. Research and Critical Evaluation of Information Security Frameworks and Models

3.1 Information Security Governance and GRC Overview

Security governance establishes accountability for security decisions, risk ownership, and ultimately adherence oversight. A GRC model closely aligns governance, risk management, and adherence to assure the consistent security decisions and accountability [9,11]. With respect to All, this is specifically significant because 88% of its IT infrastructure is outsourced, thus creating a sense of dispersed responsibility across providers. Therefore, effective governance requires more than technical controls; it needs to closely connect organisational accountability, risk decisions, supplier oversight and ultimately security assurance [12].

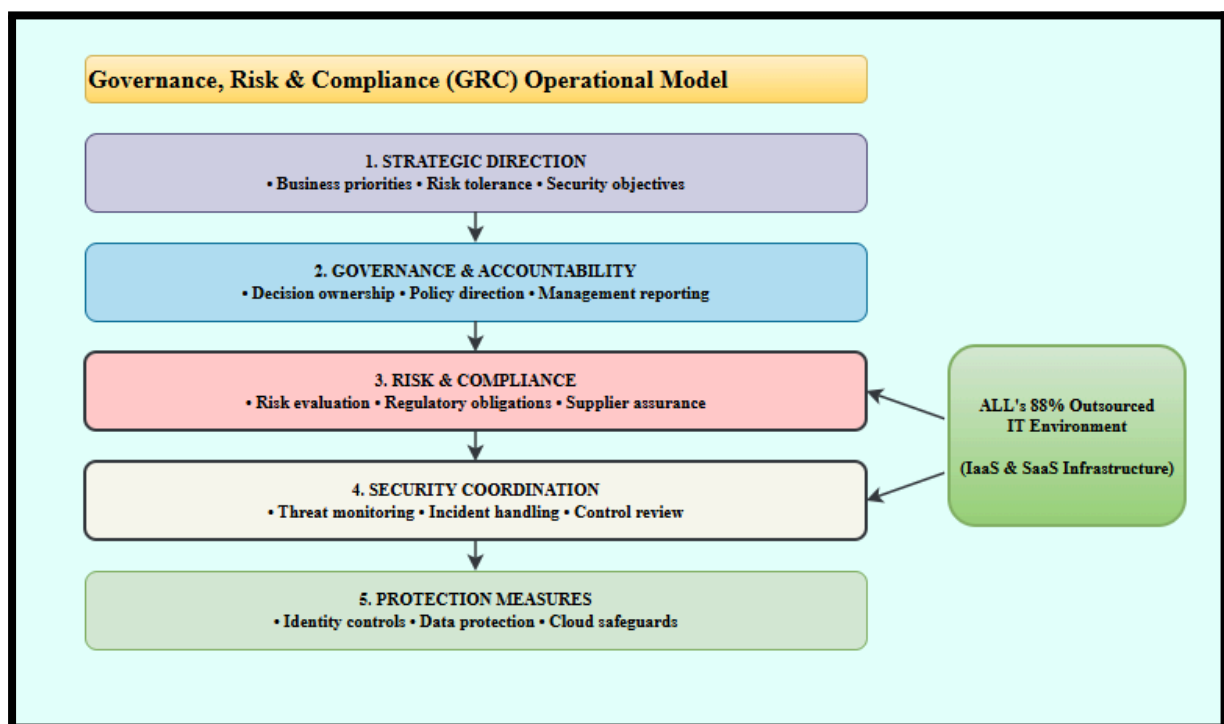


Figure 4: Security Governance Framework

(Source: Self-developed)

3.2 NIST Cybersecurity Framework 2.0

NIST CSF 2.0 organises the cybersecurity outcomes through the help of six functions including Govern, Identify, Protect, Detect, Respond, and ultimately Recover [13]. This outcome-based structure is relevant to ALL, as the firm lacks a unified security framework along with centralised risk management procedures. Instead of prescribing fixed controls, NIST enables organisations to select actions as per their risk context [14]. This flexibility suits the outsourced environments of ALL; however, it also places profound responsibility on management for defining the ownership, prioritise the risks and translating the desired outcomes into measurable controls.

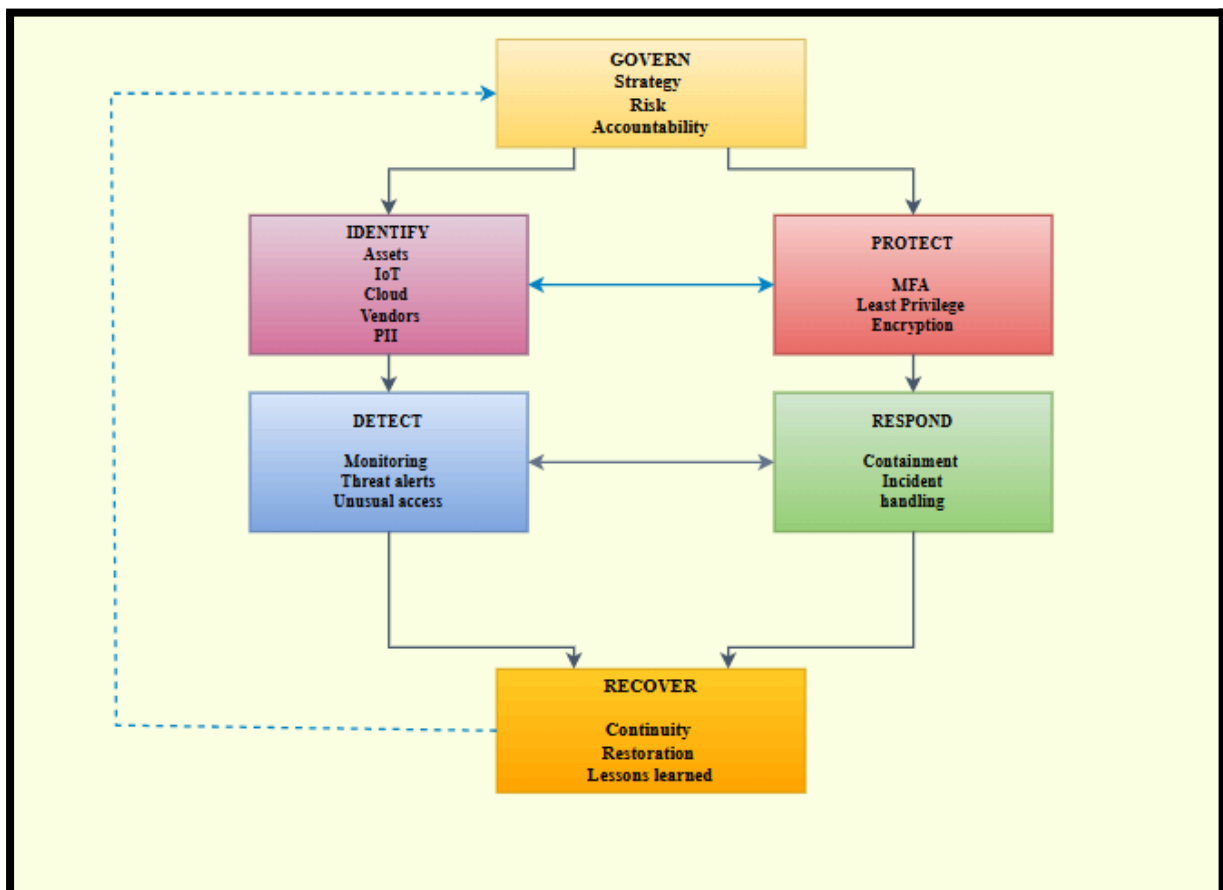


Figure 5: NIST Cybersecurity Framework

(Source; Self-developed)

3.3 ISO/IEC 27001:2022 and ISO/IEC 27002

ISO/IEC 27001:2022 presents requirements for successfully establishing, implementing, maintaining and ultimately enhancing an Information Security Management System (ISMS) [15]. Unlike the NIST's outcome-oriented flexibility, ISO 27001 gives ALL a more formal management structure for governing the information security risks along with showcasing conformity [16]. This helps in directly addressing the poor governance as well as immature adherence auditing of these logistics firms. However, its structured ISMS approach can require more profound organisational commitment than the flexible guidance of the NIST. ISO/IEC 27002 can then support the practical selection as well as successful implementation of the security controls within the ISMS [17].

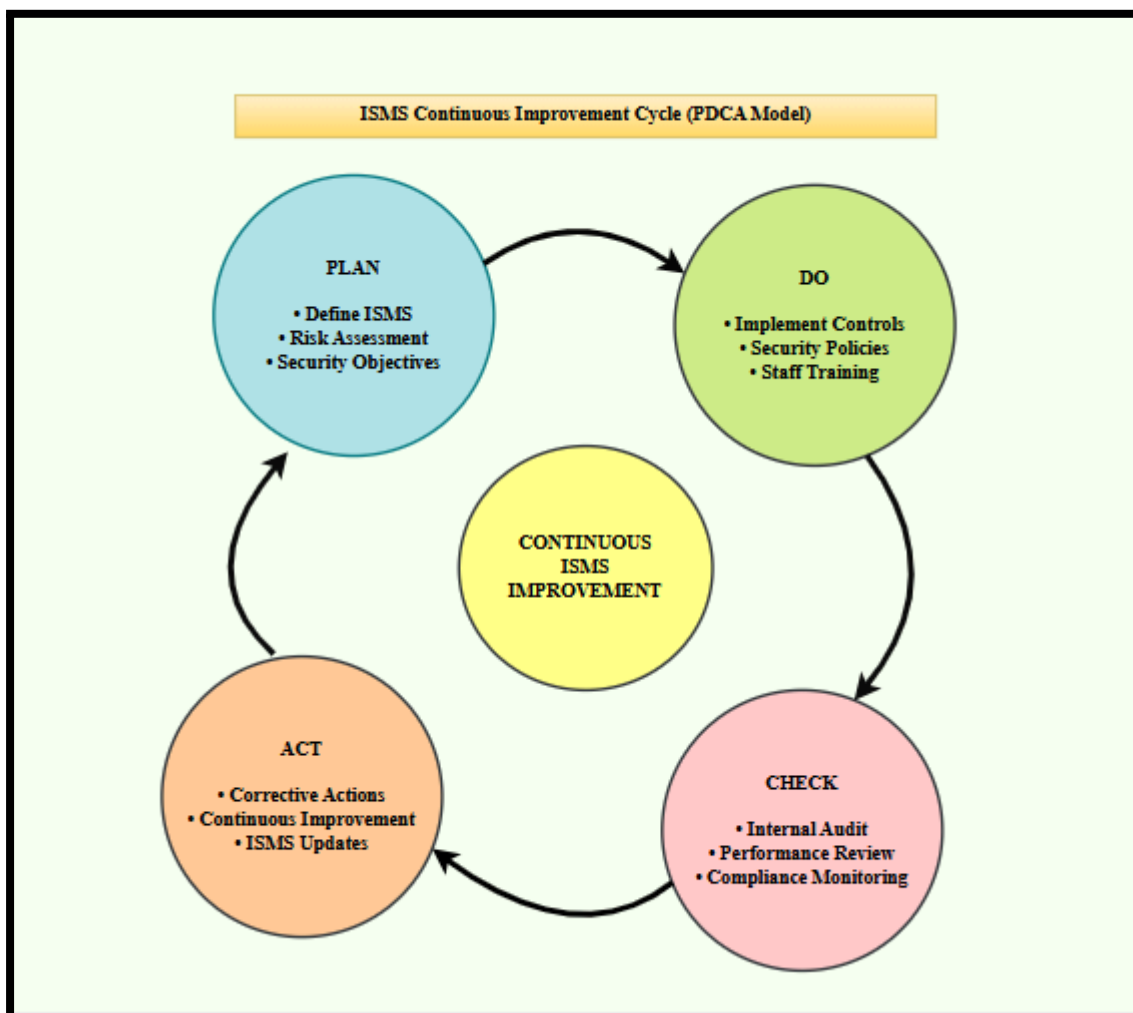


Figure 6: PDCA Cycle for ISO/IEC 27001

(Source: Self-developed)

3.4 COBIT 2019

COBIT 2019 extends the cybersecurity management towards the enterprise-wide governance of information and technology [18]. Its 40 governance and management objectives support the close alignment between the technology decisions, accountability and the organisational goals. This properly suits ALL where the outsourced IT disperses the responsibility across both the internal and external stakeholders. Compared with NIST's cybersecurity focus in combination with the ISO 27001's ISMS requirements, COBIT presents a sense of stronger governance alignment, but it does not replace either [19]. For ALL, this framework mainly assists in enhancing the governance while clarifying the accountability.

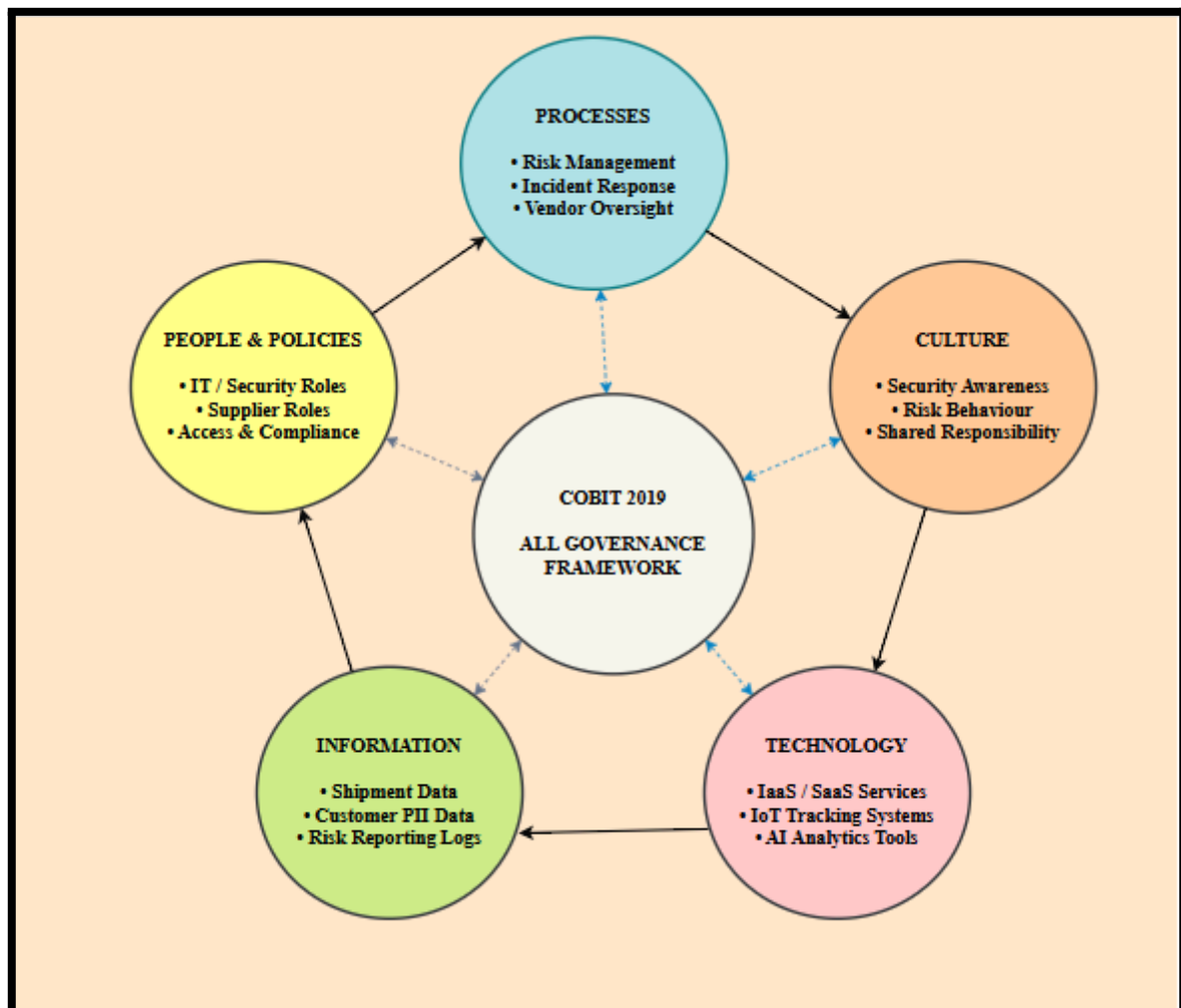


Figure 7: COBIT 2019 Governance Components

(Source: Self-developed)

3.5 ITIL 4

ITIL 4 initially addresses all aspects with the help of IT service management instead of cybersecurity governance [20]. Its incident, problem, change, suppliers, and ultimately the continual enhancements practices are closely relevant where service disruptions can influence the overall logistics operations. Compared with COBIT's governance emphasis, ITIL is more operational, while NIST offers profound cybersecurity risk convergence [21]. As a result, ITIL can fortify the incident, service and ultimately the change procedures of ALL. However, it needs to complement NIST, ISO 27001 and COBIT instead of operating as a primary security framework.

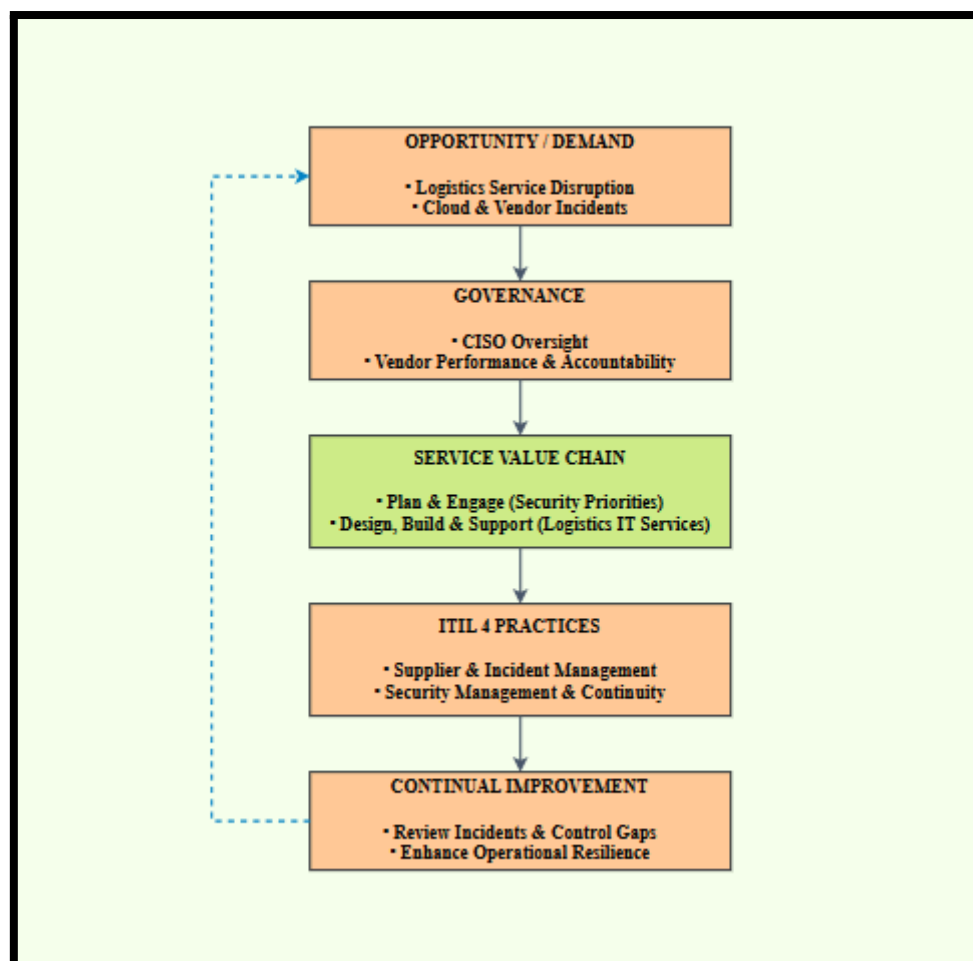


Figure 8: ITIL 4 Service Value System

(Source: Self-developed)

3.6 Zero Trust Architecture

Zero Trust directly addresses remote access of ALL, along with the unmanaged-device exposure through consistently verifying users, devices and finally the access requests while enforcing least privilege [22]. Unlike NIST, ISO 27001 and COBIT, this framework revolves more specifically around access security compared to enterprise governance. As an example, BeyondCorp of Google presents a real-world case of Zero Trust through leveraging the user identity as well as device context to control application access instead of completely depending on the network location [23, 24]. With respect to ALL, this model complements risk management of NSIT and accountability of COBIT instead of replacing them.

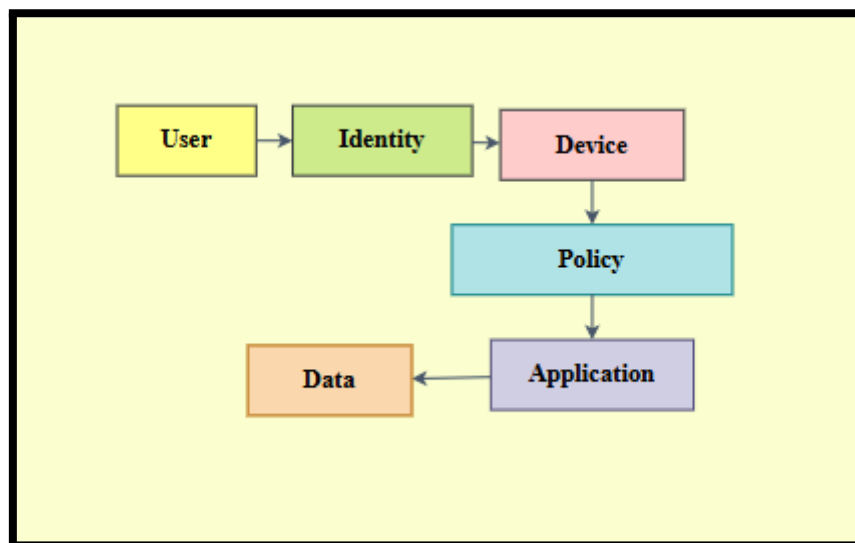


Figure 9: Zero Trust Model

(Source: Self-developed)

3.7 Cloud Shared Responsibility Model

The Cloud Shared Responsibility model clarifies how security obligations are classified between not only the cloud providers but also the customers [25]. This is critical for ALL

given its heavy dependence on the outsourced IaaS and SaaS services. Unlike the NIST or COBIT, this does not offer complete governance; rather, it helps in clarifying the accountability of the cloud [26]. With respect to ALL, this fortifies vendor oversight through preventing outsourcing from becoming an excuse for unclear security ownership.

3.8 Comparative Critical Evaluation and Framework Selection

Framework	Primary purpose	Major strength	Key limitation	ALL application
NIST CSF 2.0	Cybersecurity risk	Flexible risk management	Not certification-focused	High
ISO 27001	ISMS	Governance/certification	Resource intensive	High
COBIT 2019	Governance	Accountability/alignment [27].	Complexity	High
ITIL 4	Service management	Operational resilience	Limited cyber governance	Medium
Zero Trust	Access/security	Remote/cloud protection	Implementation complexity [28].	High
Shared Responsibility	Cloud accountability	Clarifies responsibilities	Provider-specific application	High

Table 2: Comparative table

(Source: Self-developed)

4. Proposed Integrated Security Governance Framework

4.1 Proposed Integrated Framework Overview

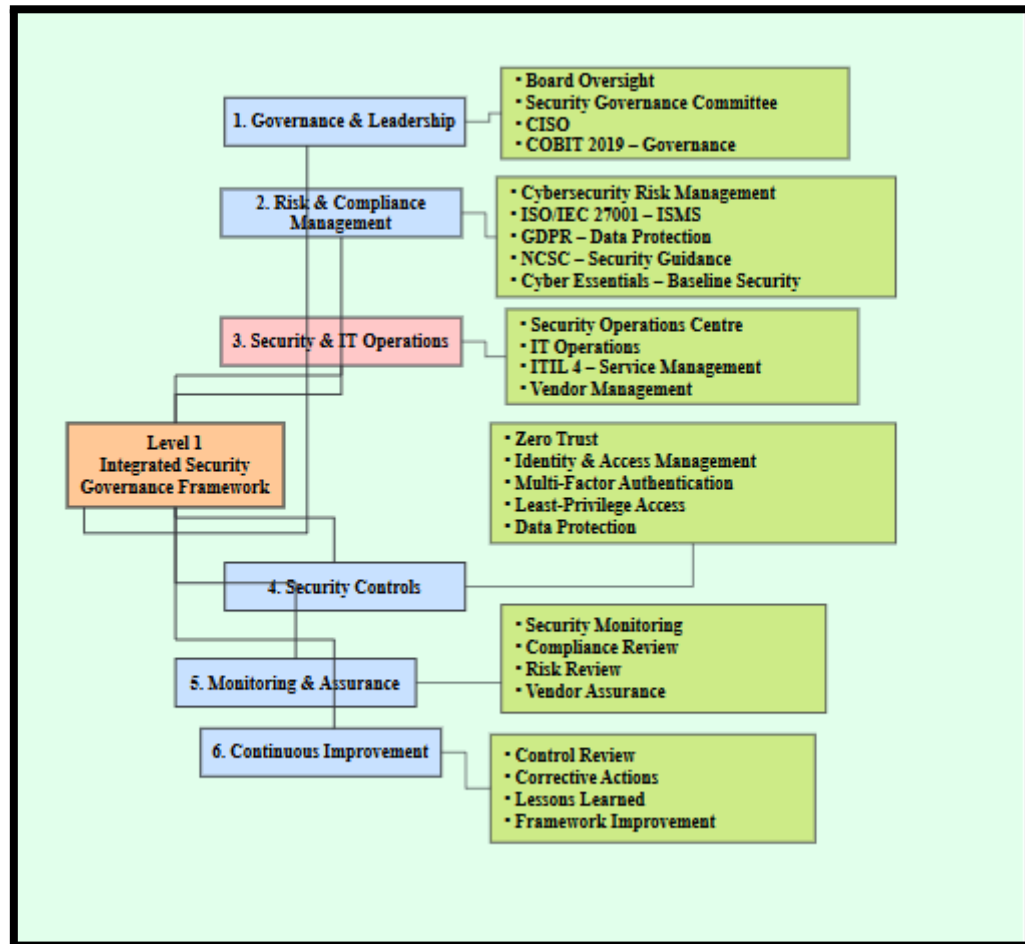


Figure 10: Security Governance Framework

(Source: Self-developed)

This framework establishes a top-down governance structure which starts with the Board’s strategic oversight and extends through the Security Governance Committee, CISO, risk, compliance, operational and finally the incident-response functions. Continuous monitoring supports the ongoing enhancement. A holistic cybersecurity as well as risk management approach closely aligns with the different models like ISO/IEC 27001 for ISMS, NIST CSF 2.0 for cyber-risk management, COBIT 2019 for governance, Zero Trust for identity-centric security, and ITIL 4 for service management. This integrated approach not only fortifies the governance of ALL but also the adaptability and strict adherence.

4.2 Governance and Strategic Security Structure

The Board offers strategic oversight and approves the security priorities, while the Security Governance Committee coordinates with the governance, risk and ultimately the assurance decision *[refer to Appendix 1]*. Besides that, the CISO helps in developing the security strategy alongside coordinates the SOC with risk and security operations [29]. The DPO supervise the personal-data protection in combination with the GDPR obligations, while the CIO/IT helps in successfully implementing both the technology and the service controls as well [30]. Moreover, the legal/compliance monitors the regulatory requirements, whereas the Vendor Management effectively controls the third-party accountability, which is specifically significant for ALL's outsourced IT environments. This structure not only fortifies ownership but also assurance [31].

4.3 Enterprise Cyber Risk Management

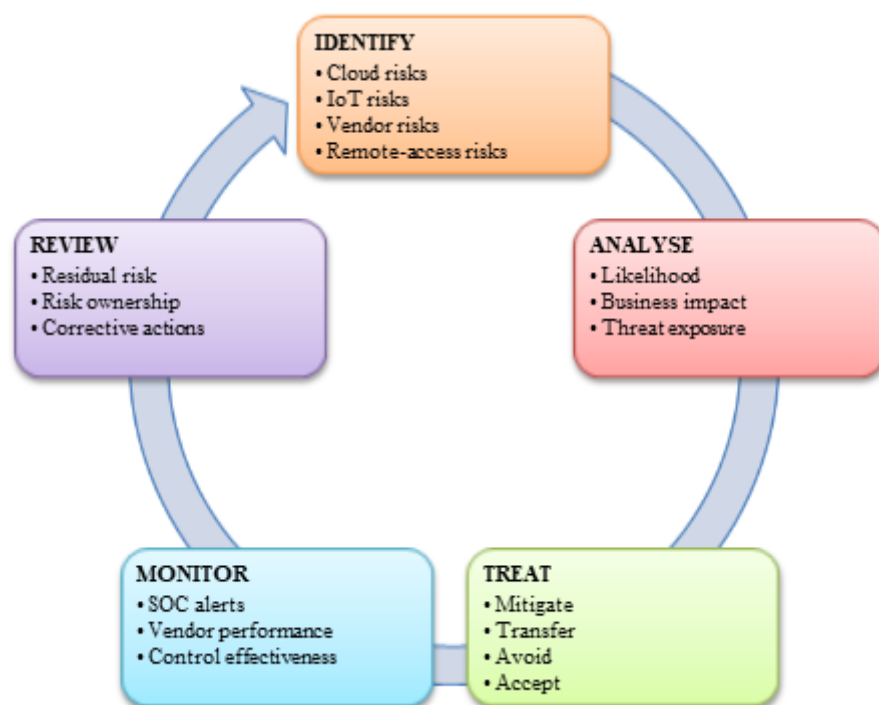


Figure 11: Cyber Risk Management Lifecycle

(Source: Self-developed)

ALL needs to identify the risks within the cloud services, IoT, vendors and finally the remote access, then critically analyse each as per both likelihood and business influence [32]. Each

risk needs to have defined owners as well as treatment decisions, incorporating the mitigation, along with the transfer, acceptance or avoidance [33]. Moreover, the residual risk needs to remain visible after controls are applied instead of being treated as excluded. In addition, continuous monitoring needs to reinvestigate the changing exposure, specifically where the outsource providers and the unmanaged devices influenced the ALL's control environment. This develops an evidence-based cycle from the identification through the help of treatment, ownership, and review *[refer to Appendix 2]*.

4.4 Security Policies, Data Governance and Procedures

This logistics company requires to successfully implementing integrated security as well as data governance covering access, remote working, BYOD and ultimately acceptable utilisation [34]. Besides that, least-privilege access in combination with encryption needs to safeguard sensitive information, while classification, retention and finally minimisation help in controlling data exposures.

4.5 Compliance, Legal and Ethical Governance

ALL requires close alignment of its security governance with the UK GDPR and the Data Protection Act 2018, while applicable NIS-related obligations, ISO/IEC 27001, Cyber Essentials Plus and ultimately the NCSC guidance assist in fortifying the assurance. However, strict adherence should not be treated as certification alone. Moreover, the ethical governance requires a sense of proportionate employee monitoring along with the responsible utilisation of data and AI, minimising data collection, transparency and finally clear accountability [35]. For ALL, this is specifically significant where cloud services, remote working and ultimately third-party providers process both organisational as well as personal information. Furthermore, the regular auditing needs to be test both the regulatory conformity and whether the security practices remain fair, necessary and ultimately proportionate.

4.6 Vendor and SLA Security Management

ALL requires its third-party vendors to fortify their third-party governance through the help of security-focused SLAs, measurable KPIs and finally the contractual security clauses. Given its outsourced environments, vendors are required to effectively manage encryption, MFA, and backups in combination with timely patching, with defined incident-reporting

obligations [36]. In addition, periodic audits are required to verify whether these requirements are actually met instead of depending on the contractual assurances. In essence, it can be asserted that the performance of the vendor requires review consistently along with the escalated security weakness.

Requirement	SLA Check
Encryption	Required
MFA	Mandatory
Backup	Defined frequency
Patch Management	Defined timeframe
Audit	Periodic review
Incident Reporting	Defined escalation

Table 3: Vendor SLA Checklist

(Source: Self-developed)

4.7 Incident Response and Cyber Crisis Management

All requires to develop an incident-response procedures covering preparation, detection analysis, containment, eradication, and ultimately recovery, followed by documented lessons learned. Besides that, both the SOC/CSIRT and SIEM require support for rapid detection in combination with investigations and escalation as well [37]. Moreover, the pre-defined procedures need to address third-party incidents along with the regulatory notification. With respect to the outsourced environment of ALL, the vendors require clear reporting and escalation obligations, while regular table top exercises need to test the decision-making, communication, and ultimately the preparedness of recovery and thus expose the weakness before a major cyber incident takes place [38].

4.8 Business Continuity and Disaster Recovery

ALL requires effective sustainment of a Business Continuity Plan (BCP) along with the Disaster Recovery Plan (DRP), which will cover the critical logistics services, cloud systems, as well as the essential data [38]. Besides that, the recovery priorities need to highlight the operational influence, whereas the adaptability relies on reliable backups, alternative services and defined responsibilities as well [39,40]. Moreover, the regular testing needs to validate whether the recovery arrangements actually work under any kind of disruptions. In addition, the results need to inform a sense of enhancements towards the recovery procedures and thus ensure that ALL can not only prepare but also respond, recover and resume their business operations without depending on untested assumptions.

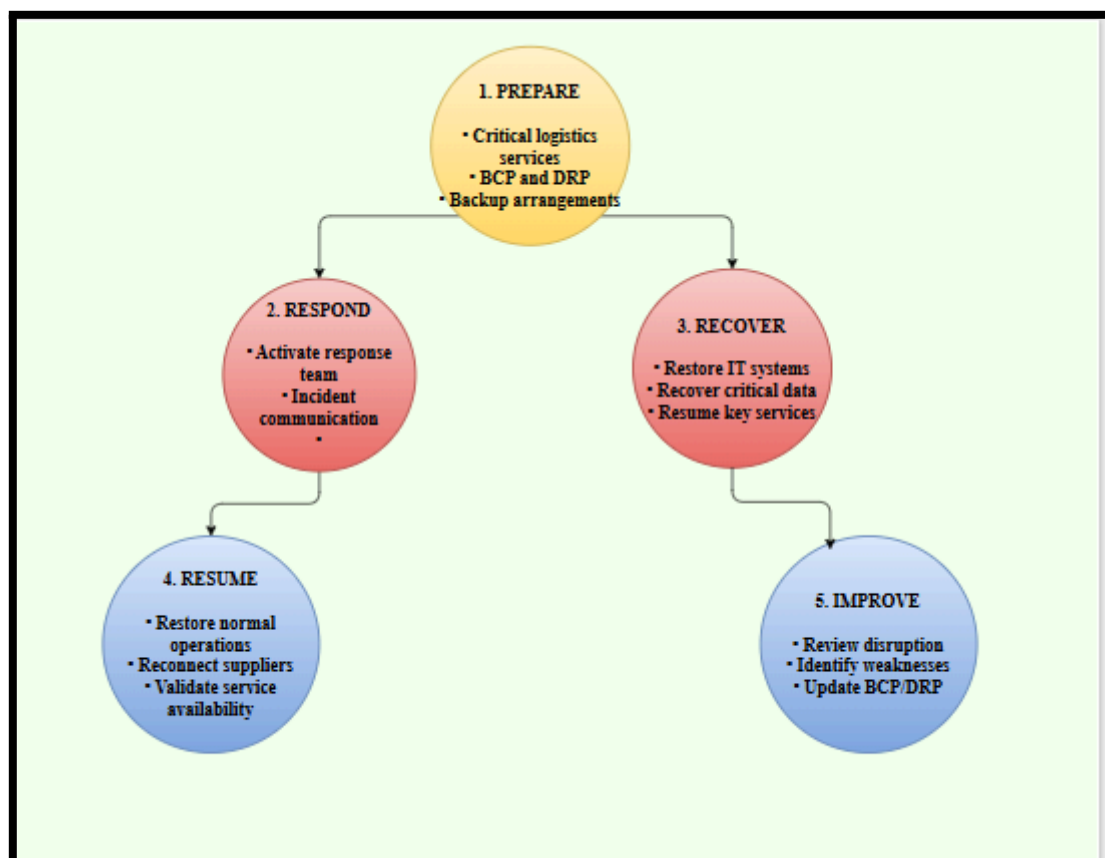


Figure 12: Business Continuity and Disaster Recovery

(Source: Self-developed)

4.9 Technical Security Architecture and Access Controls

ALL requires strong defence-in-depth as cloud services, along with remote access, IoT and finally third-party connectivity, create multiplier paths for attack. Besides that, IAM and MFA require control of both identity and access, while network segmentation often restricts lateral movement. Moreover, the EDR presents endpoint protection, while SIEM/SOC profoundly guides the centralised monitoring and response and the DLP help in lowering the inappropriate data movement. In addition, the encryption helps in safeguarding the sensitive information and thus developed a sense of layered controls rather than heavily relying on a single defensive mechanism.

5. Critical Discussion: Why Continuous Updates to Regulations and Standards Are Necessary

Continues update is a good thing to reducing phishing techniques where regular updates ensure security controls remain effective against new attack methods. Continuous updates help organisations remain legally compliant such as UK GDPR, Data Protection Act 2018, ISO/IEC 27001:2022, NIST CSF 2.0 is important to maintain governance policies in risk register technique.

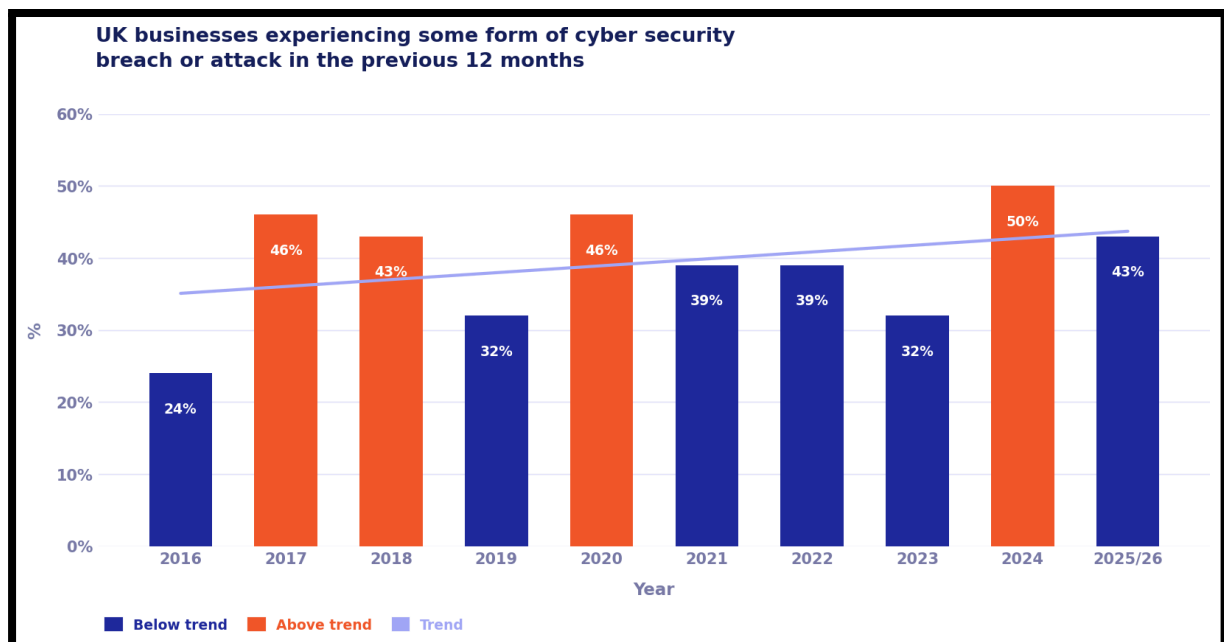


Figure 13: Cyber Attacks Growth (2016–2026)

(Source: [41])

Continuous updates are required as the security exposure of ALL is not static. The latest UK Cyber Security Breaches Survey discloses that approximately 45% of the transport as well as storage business experienced a cyber-breach compared with 43% of UK business [41]. Moreover, only 17% of the transport business reported having board-level responsibility for the cyber security compared with 31% of the overall [42]. This showcases a poor governance which directly relevant to ALL, where outsourced IT already disperses the security accountability.

Real world incidents reinforce this concerns. As an example, ransomware disruption of Royal Mail in the year 2023 showcase how cyber incidents can influence the continuity of the logistics business whereas as the Microlise's 2024 cyber incident reveals the vulnerability of logistics operations towards technology disruptions [43,44]. These cases highlight that ALL cannot treat cybersecurity primarily as technical protection; its framework requires to connect the business continuity along with the supplier governance, incident response and ultimately executive accountability. Compared with a static compliance approach, ALL requires continuous alignment with the NIST CSF 2.0, ISO revisions, NCSC guidance, Cyber Essentials and UK GDPR, in combination with the emerging threats from AI, deepfakes, zero-days and ultimately the cloud dependency. Thus, continuous adherence is more suitable for ALL than periodic certification because its outsourced as well as digitally reliant operating model can change the risk profile faster than the formal review cycles.

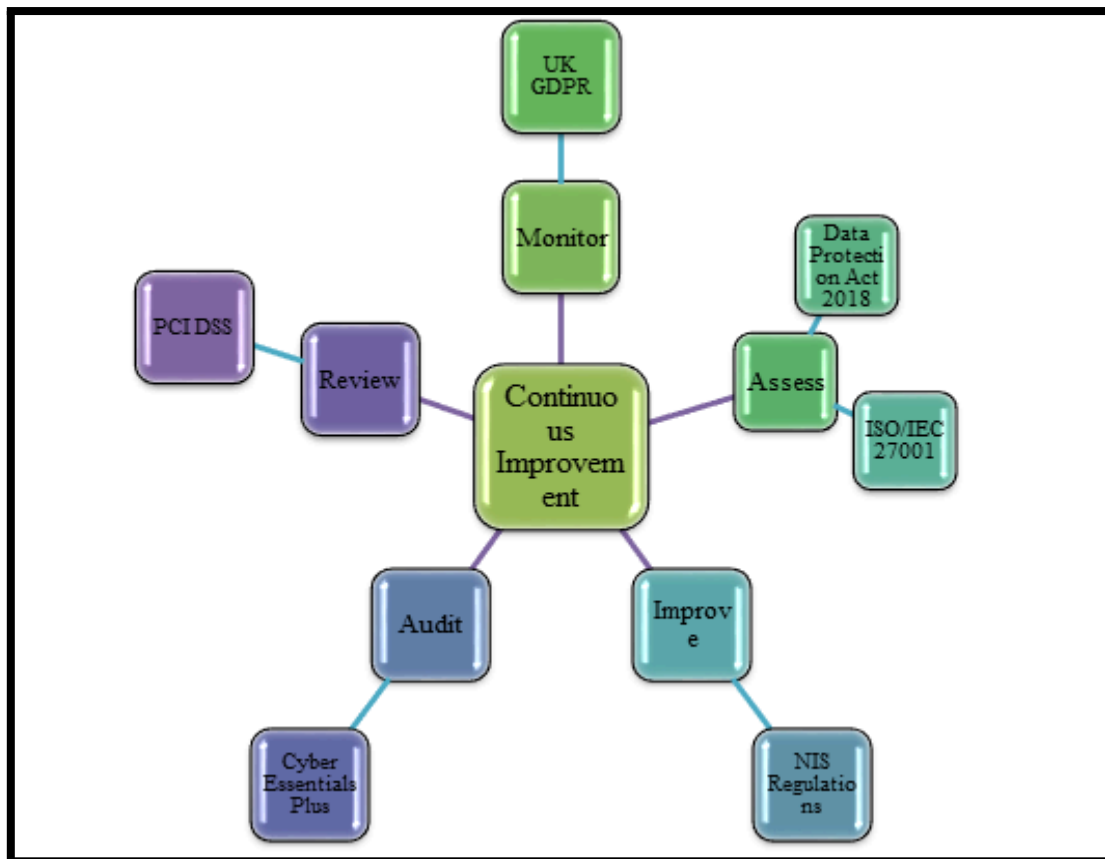


Figure 14: Continuous Compliance Improvement Cycle

(Source: Self-developed)

6. Recommendations and Implementation Roadmap

This supply chain and logistics company requires prioritising the recommendations as per the risk, their urgency and ultimately the implementation dependency *[Refer to Appendix 3]*.

Immediately, the company requires establishing the Security Governance Committee, assigning clear security ownership, successfully implementing MFA, fortifying the access controls, developing a central risk register and finally starting with the vendor security assessments [45].

On medium term, this company needs to embrace a NIST CSF 2.0, build an ISO/IEC 27001 ISMS, profoundly implement Zero Trust, fortifies the capabilities of SOC and thus boost the overall data governance [46].

In long-term, the company requires prioritising the shift towards the ISO/IEC 27001 certification readiness, consistent strict adherence, AI security governance and finally the continues vendor assurance [47].

Action	Owner	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	KPI / Measure
MFA Implementation	CISO													% coverage
Central Risk Register	CISO													Risk register completion
Vendor Security Review	CISO													% critical vendors assessed
NIST CSF 2.0	CISO / IT													% control adoption
Zero Trust Controls	CISO / IT													% priority controls implemented
ISO 27001 ISMS	CISO / DPO													ISMS readiness

Audit Readiness	CIS O / DPO																Audit readiness %
--------------------	-------------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	-------------------------

Table 3: Gantt Chart

(Source: Self-developed)

7. Conclusion

In conclusion it can be asserted that ALL requires an integrated security governance approach instead of isolated technical controls. Closely integrating the Aligning ISO/IEC 27001, NIST CSF 2.0, COBIT 2019, Zero Trust and ITIL 4 within the business practices of ALL can not only fortify the governance but also the risk management, adaptability and finally the compliance. Moreover, the prioritised implementation, consistent monitoring as well as vendor assurance will allow ALL to respond profoundly towards the changing cyber threats.

References

1. Anumula, S.K., Bhwsar, R. and Patil, M., 2026. The digital backbone for architecting smart operations with a unified namespace. *Discover Computing*, 29(1), p.300. <https://link.springer.com/content/pdf/10.1007/s10791-026-10195-w.pdf>
2. Lakhpati, V., 2025. Leveraging technology in third party risk management. *Journal of Financial Compliance*, 9(3), pp.241-251. <https://www.ingentaconnect.com/content/hsp/jfc/2025/00000009/00000003/art00004>
3. Laine, M., 2025. Procurement and Implementation of SaaS Services: Challenges Related to Information Security and Data Protection from a Product Owner's Perspective. https://www.theseus.fi/bitstream/handle/10024/896340/Laine_Meri.pdf?sequence=2
4. Villegas-Ch, W., García-Ortiz, J. and Sánchez-Viteri, S., 2024. Toward intelligent monitoring in IoT: AI applications for real-time analysis and prediction. *IEEE access*, 12, pp.40368-40386. <https://ieeexplore.ieee.org/iel7/6287639/6514899/10471529.pdf>
5. Pierides, M. and Mulligan, J., 2025. Key themes of resiliency, outsourcing and third-party risk management regimes. *Journal of Securities Operations & Custody*, 17(2), pp.102-118. <https://www.ingentaconnect.com/content/hsp/jsoc/2025/00000017/00000002/art00002>
6. Kure, H.I., Islam, S. and Mouratidis, H., 2022. An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, 34(18), pp.15241-15271. https://repository.essex.ac.uk/32252/1/After%20Revision_Final-Submission.pdf
7. Ab Rahim, M.S., Reniers, G., Yang, M. and Siwayanan, P., 2025. Integrating process safety and process security risk management: Practitioner insights for a resilience-oriented framework. *Processes*, 13(2), p.392. <https://www.mdpi.com/2227-9717/13/2/392>
8. Erdos, D., 2026. Post-GDPR Regulatory Enforcement of UK Data Protection: Reality, Scrutiny, Oversight and Future. *University of Cambridge Faculty of Law Research Paper*, (1). <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=6247240>
9. Navandar, P., 2024. Governance, Risk, and Compliance (GRC) in the Age of Identity and Access Governance (IAG) A Framework for Integrated Enterprise Security and Compliance.

International Journal of Research and Applied Innovations, 7(2), pp.10483-10493.
<https://www.ijrai.org/index.php/ijrai/article/download/601/552>

10. Repetto, M., 2023. Adaptive monitoring, detection, and response for agile digital service chains. *Computers & Security*, 132, p.103343.
<https://www.sciencedirect.com/science/article/pii/S0167404823002535>

11. 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=A+GRC+model+closely+aligns+governance,+risk+management,+and+adherence+to+assure+the+consistent+security+decisions+and+accountability&ots=YVF-zaVzgu&sig=jC8IMiCy0BptF87zAKKqfHHm3U>

12. Akinsola, K., 2025. Legal compliance in corporate governance frameworks: best practices for ensuring transparency, accountability, and risk mitigation. *Accountability, and Risk Mitigation* (January 31, 2025).
<https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5126542>

13. Edwards, J., 2024. *A comprehensive guide to the NIST cybersecurity framework 2.0: Strategies, implementation, and best practice*. John Wiley & Sons.
<https://books.google.com/books?hl=en&lr=&id=JysbEQAAQBAJ&oi=fnd&pg=PR19&dq=NIST+CSF+2.0+organises+the+cybersecurity+outcomes+through+the+help+of+six+function+s+including+Govern,+Identify,+Protect,+Detect,+Respond+and+ultimately+Recover.+&ots=bNNMWxSl5l&sig=O-ljDM4qVFvBeFDfk3NctGB4fdI>

14. Parmar, M. and Miles, A., 2024, May. Cyber security frameworks (CSFs): An assessment between the NIST CSF v2. 0 and EU standards. In *2024 Security for Space Systems (3S)* (pp. 1-7). IEEE.
https://indico.esa.int/event/528/attachments/5988/10190/Cyber_Security_Frameworks_CSFs_An_Assessment_Between_the_NIST_CSF_v2.0_and_EU_Standards.pdf

15. Nurmi, P., 2024. Enhancing ISO 27001: 2022 Implementation Through Project Management.
https://www.theseus.fi/bitstream/handle/10024/863059/Nurmi_Pessi.pdf?sequence=2

16. Podrecca, M., 2023. ISO/IEC 27001: An empirical multi-method research. https://tesidottorato.depositolegale.it/bitstream/20.500.14242/91311/1/Final%20Thesis_Matteo%20Podrecca.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+27001:2022+presents+requirements+for+successfully+establishing,+implementing,+maintaining+and+ultimately+enhancing+an+Information+Security+Management+System+\(ISMS\).+&ots=qAM5VVH1kP&sig=ZGciPDg2YYH8bUHvozzzPAk96Ys](https://books.google.com/books?hl=en&lr=&id=5s_BEQAAQBAJ&oi=fnd&pg=PR13&dq=ISO/IEC+27001:2022+presents+requirements+for+successfully+establishing,+implementing,+maintaining+and+ultimately+enhancing+an+Information+Security+Management+System+(ISMS).+&ots=qAM5VVH1kP&sig=ZGciPDg2YYH8bUHvozzzPAk96Ys)
18. 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>
- 19.. Hussain, M.H., Riaz, A. and Butt, A., 2025. Integrating COBIT 2019 with zero trust architecture: A strategic approach to GRC in cybersecurity. *VFAST Transactions on Software Engineering*, 13(4), pp.124-136. <https://vfast.org/journals/index.php/VTSE/article/download/2245/1796>
20. Lopes, S., Leite, P., Carvalho, S. and Teixeira, P., 2024, April. Using ITIL as part of the NIST Cybersecurity Framework. In *2024 12th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE. <https://ieeexplore.ieee.org/abstract/document/10527256/>
21. 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
22. Roy, K.S., SECURING THE FUTURE: INTRODUCTION TO ZERO TRUST IN CYBERSECURITY. https://www.researchgate.net/profile/Vinayakumar-Ravi/publication/381947270_Zero_Trust_Awareness_Creating_a_Culture_Aware_of_Security/links/6841dcc9c33afe388aca5e5f/Zero-Trust-Awareness-Creating-a-Culture-Aware-of-Security.pdf.

23. Purohit, P.K., Joshi, V. and Dangi, A., Zero-Trust Security Architectures: Principles, Frameworks, and Enterprise Implementation Challenges. https://ijsate.com/wp-content/uploads/2026/04/V3I4P81_IJSATE0426113.pdf.

24. Prasun, P., 2023. Zero-trust security architectures for cloud and enterprise systems. *International Journal of Advanced Research in Computer Science & Technology (IJARCST)*, 6(6), pp.9373-9377. <https://www.ijarcst.org/index.php/ijarcst/article/download/32/31>

25. REYES, C. and MENDOZA, C., 2023. Exploring the impact of shared responsibility models on cloud security posture and vulnerability management. *Quarterly Journal of Emerging Technologies and Innovations*, 8(1), pp.1-10. https://www.researchgate.net/profile/Cristina-Reyes-14/publication/386220026_EXPLORING_THE_IMPACT_OF_SHARED_RESPONSIBILITY_MODELS_ON_CLOUD_SECURITY_POSTURE_AND_VULNERABILITY_MANAGEMENT/links/67493ef5f309a268c013f65f/EXPLORING-THE-IMPACT-OF-SHARED-RESPONSIBILITY-MODELS-ON-CLOUD-SECURITY-POSTURE-AND-VULNERABILITY-MANAGEMENT.pdf

26. Alexander, L., 2025. THE ROLE OF SHARED RESPONSIBILITY MODELS IN MITIGATING CLOUD SECURITY RISKS. https://www.researchgate.net/profile/Luna-Alexandra/publication/391271139_THE_ROLE_OF_SHARED_RESPONSIBILITY_MODELS_IN_MITIGATING_CLOUD_SECURITY_RISKS/links/6810950460241d51401fb850/THE-ROLE-OF-SHARED-RESPONSIBILITY-MODELS-IN-MITIGATING-CLOUD-SECURITY-RISKS.pdf

27. Renuka, K. and Kanmani, M.C., 2026. *Strategic Use of Technology in Management*. LexArcheus Publications. <https://books.google.com/books?hl=en&lr=&id=czPCEQAAQBAJ&oi=fnd&pg=PA1&dq=CObIT+2019+Governance+Accountability/alignment+Complexity+High&ots=qJeh3BuJAe&sig=HHv4JOHsioGDi3TyO9ueqYuav4E>

28. Nalluri, S., Malyala, M.M., Kandagiri, H., Jakku, P.C. and Kandagiri, K.K., 2025, June. AI-Enhanced Zero Trust Architecture for Cloud Security with Quantum Resilience. In *2025 6th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)* (pp. 1085-1092). IEEE. https://www.researchgate.net/profile/Suryaprakash-Naluri/publication/394480346_AI-Enhanc

[ed Zero Trust Architecture for Cloud Security with Quantum Resilience/links/68a26c847984e374ace95075/AI-Enhanced-Zero-Trust-Architecture-for-Cloud-Security-with-Quantum-Resilience.pdf](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+coordinates+the+SOC+with+risk+and+security+operations.&ots=rn_GhWYJ-4&sig=fPHMoKRpcY7n2QMu4jXZUNEV3J4)

29. 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+coordinates+the+SOC+with+risk+and+security+operations.&ots=rn_GhWYJ-4&sig=fPHMoKRpcY7n2QMu4jXZUNEV3J4

30. Gutterman, A.S., 2023. Management of Technology Activities. *Available at SSRN 4528090*. <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4528090>

31. Dosovitchkaia, L., 2024. Agile IT vendor management: vendor management in outsourced agile teams. https://lutpub.lut.fi/bitstream/handle/10024/167958/mastersthesis_dosovitchkaia_liubov.pdf?sequence=3&isAllowed=y

32. Singh, N., Buyya, R. and Kim, H., 2024. Securing cloud-based internet of things: challenges and mitigations. *Sensors*, 25(1), p.79. <https://www.mdpi.com/1424-8220/25/1/79>

33. Pallaria, A., 2023. Risk-mitigation techniques: from (re-) insurance to alternative risk transfer. https://iris.uniroma1.it/bitstream/11573/1670475/1/Tesi_dottorato_Pallaria.pdf

34. Downer, K. and Bhattacharya, M., 2022, February. BYOD security: A study of human dimensions. In *Informatics* (Vol. 9, No. 1, p. 16). MDPI. <https://www.mdpi.com/2227-9709/9/1/16>.

35. Bibi, P., 2024. Establishing transparency and accountability in AI: Ethical standards for data governance and automated systems. *Birkstedt, T., Minkinen, M., Tandon, A., & Mäntymäki, M.(2023). AI governance: themes, knowledge gaps and future agendas. Internet Research*, 33(7), pp.133-167. https://www.researchgate.net/profile/Palwasha-Bibi-2/publication/384967741_Establishing_Transparency_and_Accountability_in_AI_Ethical_Standards_for_Data_Governance_and_Automated_Systems/links/670fc38224a01038d0f04435/Establishing-Transparency-and-Accountability-in-AI-Ethical-Standards-for-Data-Governance-and-Automated-Systems.pdf

36. Wang, J. and Eng, P., 2026. Addressing the Security Challenges of Information Technology/Operational Technology Integration. <https://ospe.on.ca/wp-content/uploads/2026/07/Cybersecurity-Report-Jul2026-Final.pdf>
37. Amin, F., 2025, November. Adaptive Cyber Risk Management Framework for Critical Infrastructures: Integrating IDS, SOC, and CSIRT for Resilient Threat Mitigation. In *International Conference on Data Science, Computation and Security* (pp. 222-239). Cham: Springer Nature Switzerland. https://link.springer.com/chapter/10.1007/978-3-032-24075-0_20
38. Kilroy II, P.K., 2024. *Cyber Defense Planning in Tabletop Exercises and Consideration of a Fractured Flaw Theory for Security Applications*. Liberty University. <https://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=6318&context=doctoral>
39. Kesa, D.M., 2023. Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations. *World Journal of Advanced Research and Reviews*, 18(3), pp.970-992. <https://www.academia.edu/download/126217626/WJARR-2023-1166.pdf>
40. Tatineni, S., 2023. Cloud-based business continuity and disaster recovery strategies. *International Research Journal of Modernization in Engineering, Technology, and Science*, 5(11), pp.1389-1397. https://www.academia.edu/download/109038414/fin_irjmets1700193452.pdf
41. Amtivo (2026). *The Biggest Cyber Attacks Year by Year*. Available from <https://amtivo.com/uk/standards/cyber-essentials/insights/the-biggest-cyberattacks-by-year/>. Accessed on 5.8.2026
42. 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 5.8.2026
43. Manners-Bell, J., 2023. *Supply Chain Risk Management: How to design and manage resilient supply Chains*. Kogan Page Publishers. <https://books.google.com/books?hl=en&lr=&id=k93eEAAQBAJ&oi=fnd&pg=PP1&dq=Royal+Mail+in+the+year+2023+showcase+how+cyber+incidents+can+influnce+the+continuit>

y+of+the+logistics+business+whereas++&ots=v0ej0Ba5-A&sig=Ynk9zsEpUN1AQYG_3FasaQq6UGA

44. Mascellino. A., (2024). *Cyber-Attack on Microlise Disrupts DHL and Serco Tracking Services*. Available from <https://www.infosecurity-magazine.com/news/cyberattack-microlise-disrupts-dhl/>. Accessed on 5.8.2026

45. Salihu, A., 2025. Assessing Security Controls. In *Cybersecurity Audit Essentials: Tools, Techniques, and Best Practices* (pp. 163-244). Berkeley, CA: Apress. https://link.springer.com/chapter/10.1007/979-8-8688-1712-0_3

46. 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

47. Ramli, A., Darus, M.Y., Ali, F.H.M., Bakar, M.R.A., Kamarzaman, N.S. and Kasiran, Z., 2025, August. Strengthening Trust and Security through ISO 27001 Compliance: A Conceptual Framework for Information Management. In *2025 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)* (pp. 31-36). IEEE. <https://ieeexplore.ieee.org/abstract/document/11265109/>.

