



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: Naman himansu vaidya

Student ID number: 2540087

Abstract

Modern organisations are facing a greater risk of cyber-attacks than ever due to the uptick in cloud computing, AI, IoT, remote working and outsourced IT services. AeroLink Logistics (ALL) is grappling with a data breach, weak governance, fragmented security management, and failure to comply with standards. The objective of the report is to evaluate leading information security frameworks and integrate security governance framework to ensure operation and regulatory compliance of ALL.

The study takes a critical look at recognised frameworks, notably NIST Cybersecurity Framework (CSF) 2.0, ISO/IEC 27001, COBIT 2019, ITIL 4 and the Zero Trust Security Model, as well as associated UK regulations and governance practices. An integrated governance model is proposed aimed at enhancement of risk management, compliance, vendor security, incident response and business continuity. The outcome indicates that continuous monitoring complemented by regulatory updates and continual improvement being more effective and resilient than single controls or one-off compliance activities, as highlighted in the finding.

Table of Contents

1. Introduction.....	7
1.1 Background.....	7
1.2 Problem Statement.....	7
1.3 Aim.....	8
1.4 Objectives.....	8
1.5 Report Structure.....	8
2. Case Analysis.....	9
2.1 Company Overview.....	9
2.2 Key Security Challenges.....	9
2.3 Assumptions.....	10
3 Research on Information Security Frameworks.....	12
3.1 Overview of Security Governance.....	12
3.2 NIST Cybersecurity Framework 2.0.....	13
3.3 ISO/IEC 27001 and ISO 27002.....	14
3.4 COBIT 2019.....	15
3.5 ITIL 4.....	16
3.6 Zero Trust Security Model.....	17
3.7 Shared Responsibility Model (Cloud).....	18
3.8 Comparative Evaluation.....	19
4 Design of an Integrated Security Governance Framework for AeroLink Logistics.....	20
4.1 Proposed Integrated Framework.....	20
4.2 Governance Structure.....	21
4.3 Security Policies.....	22
4.4 Risk Management Process.....	23
4.5 Compliance Strategy.....	24
4.6 Protection Mechanisms.....	24
4.7 Vendor and SLA Management.....	24
4.8 Incident Response.....	24
4.9 Business Continuity.....	25
5 Critical Discussion: Continuous Updates to Regulations and Standards.....	25
6. Recommendations.....	26
7. Conclusion.....	27

References.....	28
-----------------	----

List of Figures

Figure 1: Cybersecurity Threats	6
Figure 2: Diagram of Digital Transformation	7
Figure 3: Company Overview	8
Figure 4: Security Investment Priority	10
Figure 4: Security Governance Framework	12
Figure 5: NIST Cybersecurity Framework	12
Figure 6: PDCA Cycle for ISO/IEC 27001	13
Figure 7: COBIT 2019 Governance Components	14
Figure 8: ITIL 4 Service Value System	15
Figure 9: Zero Trust Model	16
Figure 10: Cloud Security	17
Figure 11: Security Governance Framework	19
Figure 12: Organisation Chart	20
Figure 13: Security Policy Flow	21
Figure 14: Risk Management Cycle	22
Figure 15: Cyber Threats	22
Figure 16: Continuous Compliance Improvement Cycle	25

List of Tables

Table 1: Assumptions	9
Table 2: Comparative Evaluation across Security Frameworks	18
Table 3: Roles and Responsibilities of Governance	21

1. Introduction

1.1 Background

The pandemic has rapidly changed how businesses work with digital technologies to improve operational efficiencies and business agility. IoT technologies highlight the remote working model which is outsourcing to third-party service providers across organizations, now dependent on cloud computing. These innovations have greatly amplified the scope for cyberattacks, raising vulnerability to ransomware, data loss, inside men, and supply chain assaults. Therefore, organisations need to establish strong information security governance, risk management and compliance to protect critical assets and build stakeholder trust.

1.2 Problem Statement

AeroLink Logistics (ALL) is confronted with significant information security and governance problems due to the dependencies on the cloud, IoT, AI, and outsourcing of IT infrastructure.



Figure 1: Cybersecurity Threats

(Source: Deep Strike, 2025)

The organization has faced multiple incidents of data breaches that compromised access to shipping data along with other PII [24]. In addition, organisations are taking on more risk due to the lack of a consolidated security framework, weak governance processes, poor vendor management and lack of compliance with standards such as GDPR and ISO/IEC 27001 [25]. The limited incident response capability, security responsibilities inconsistencies, and

ineffective business continuity planning further weaken ALL's ability to protect information assets and comply with regulations.

1.3 Aim

The aim of this report is to critically evaluate security framework information for developing an integrated governance, risk management and compliance framework for AeroLink Logistics.

1.4 Objectives

- To review modern security frameworks
- To analyse organisational risks
- To design security governance model
- To recommend compliance improvements
- To evaluate importance of continuous updates

1.5 Report Structure



Figure 2: Diagram of Digital Transformation

(Source: Self-developed)

This report critically appraises the need for updating security rules and standards on a continuous basis, with practical recommendations, and closes with means to strengthen organisational resilience against cyber threats.

2. Case Analysis

2.1 Company Overview

AeroLink Logistics (ALL) is a multinational facility that offers real-time tracking, storage and global distribution services. In order to improve efficiency and customer satisfaction, the company significantly relies on cloud computing, IoT devices, and AI-powered analytics [34]. About 88% of the IT infrastructure is outsourced through IaaS and SaaS providers [52]. The organisation encourages a remote workforce spread across the geography which can be accessed remotely. Operating in several countries, ALL handles customer and shipment data that is sensitive in nature. Consequently, information security, governance and regulatory compliance are a must.

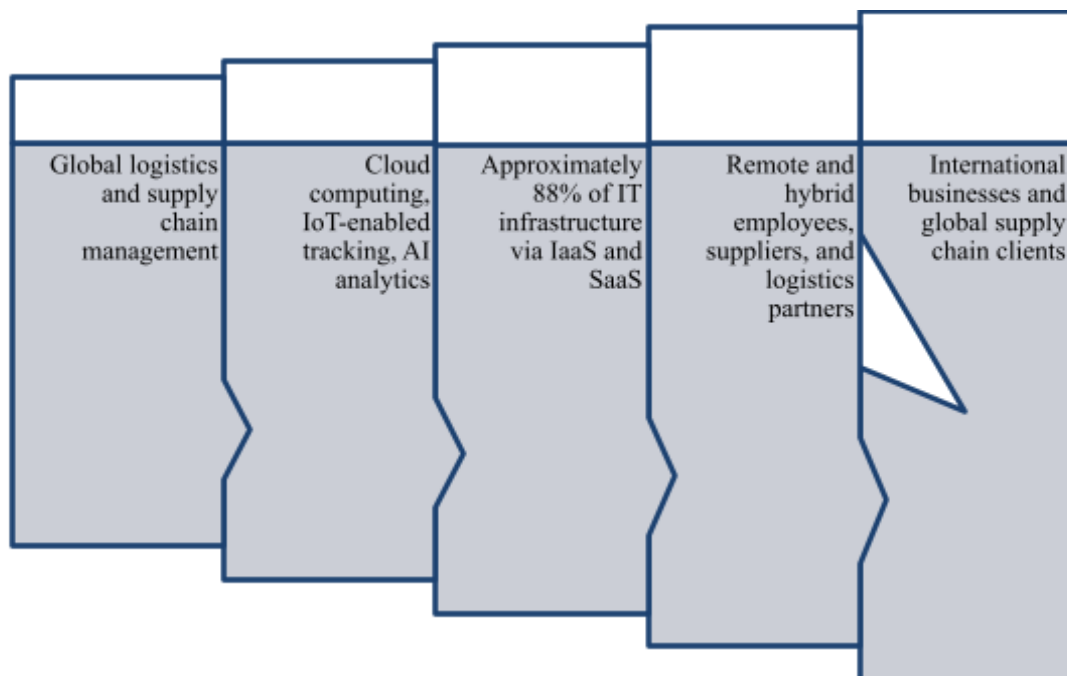


Figure 3: Company Overview

(Source: Self-developed)

2.2 Key Security Challenges

AeroLink Logistics is susceptible to operational, financial, and regulatory risks due to several security vulnerabilities. The failure shows repeated data breaches involving customer shipment information that access controls to monitoring an inadequate PII [8]. The supply chain lessens rely on third-party vendors to provide a service or product which control over outsourced systems can increase security risks [2].

A formal risk management process contributes to limited accountability that highlights a lack of a cohesive governance framework for decision-making. Furthermore, the organisation's evolving with cyber threats comes from poor observance of standards across deficient business continuity planning material [4].

2.3 Assumptions

A number of assumptions related to AeroLink Logistics are made to support the proposed security framework. The organisation is presumed to be a medium-to large-sized multinational company based in the UK and governed by UK GDPR, the Data Protection Act 2018 and other relevant laws [26]; [37]. It is presumed to run a Microsoft Azure cloud environment with a modest cyber security budget and a hybrid workforce accessing from anywhere. Moreover, the organisation is considered to have a low to medium security maturity (i.e. Level 2) which means that while the basic security controls are in place governance, compliance, risk management and continuous monitoring processes are mostly informal and inconsistent [15].

<i>Assumption</i>	<i>Description</i>
Size	Medium to large company
Headquarters	United Kingdom
Regulatory	UK GDPR Data Protection Act 2018 ISO/IEC 27001
Budget	Investment in cybersecurity initiatives
Cloud	Microsoft Azure cloud infrastructure
Model	Hybrid and remote workforce
Security Maturity	Repeatable security practices

Table 1: Assumptions

(Source: Self-developed)

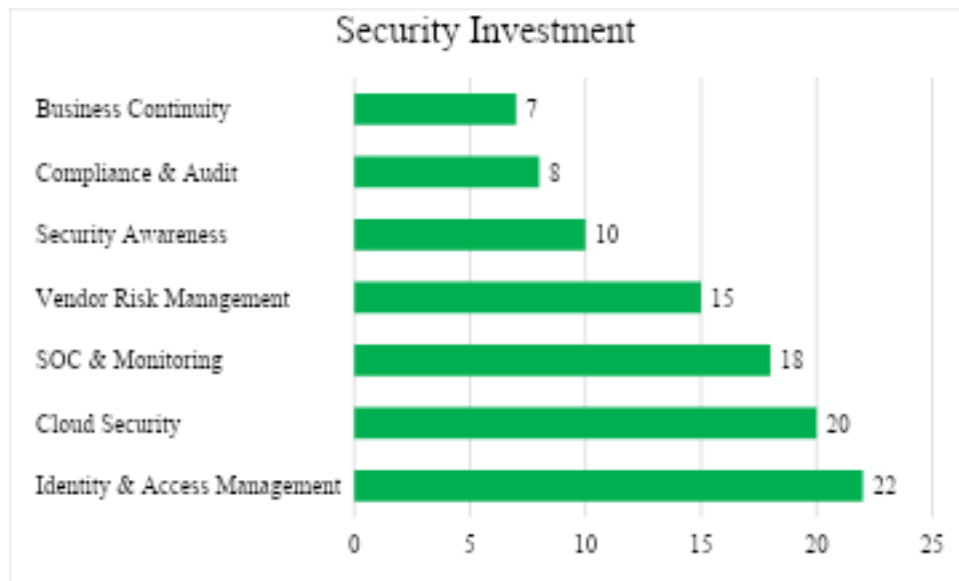


Figure 4: Security Investment Priority

(Source: Self-developed)

3 Research on Information Security Frameworks

3.1 Overview of Security Governance

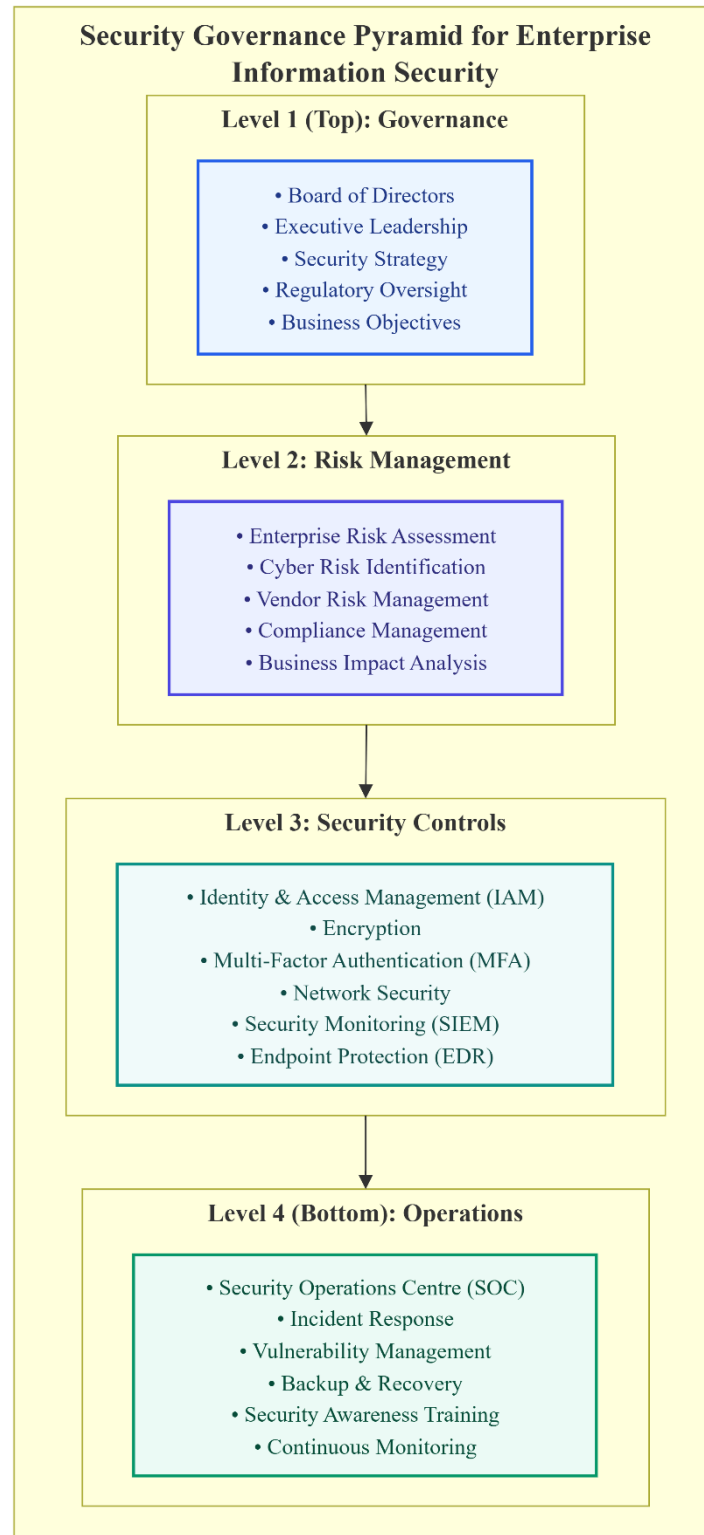


Figure 4: Security Governance Framework

(Source: Self-developed)

Managing cyber risks and regulatory requirements when security strategies are aligned with the organization's objectives. The GRC model refers to the integration of oversight by executives, management of enterprise risk, and compliance with the law into decision making. In the UK, organisations are increasingly turning to GRC (governance, risk and compliance) practices in order to comply with legal requirements, including the UK GDPR, Data Protection Act 2018, and ISO/IEC 27001 [26]. For example, British Airways suffered a data breach highlighting the organisation strengthened its governance and compliance practices with the aim of improving accountability and data protection in 2018 [13]. This highlights that an effective governance can lessen cyber risk, help organizations maintain resilience and comply with regulations.

3.2 NIST Cybersecurity Framework 2.0

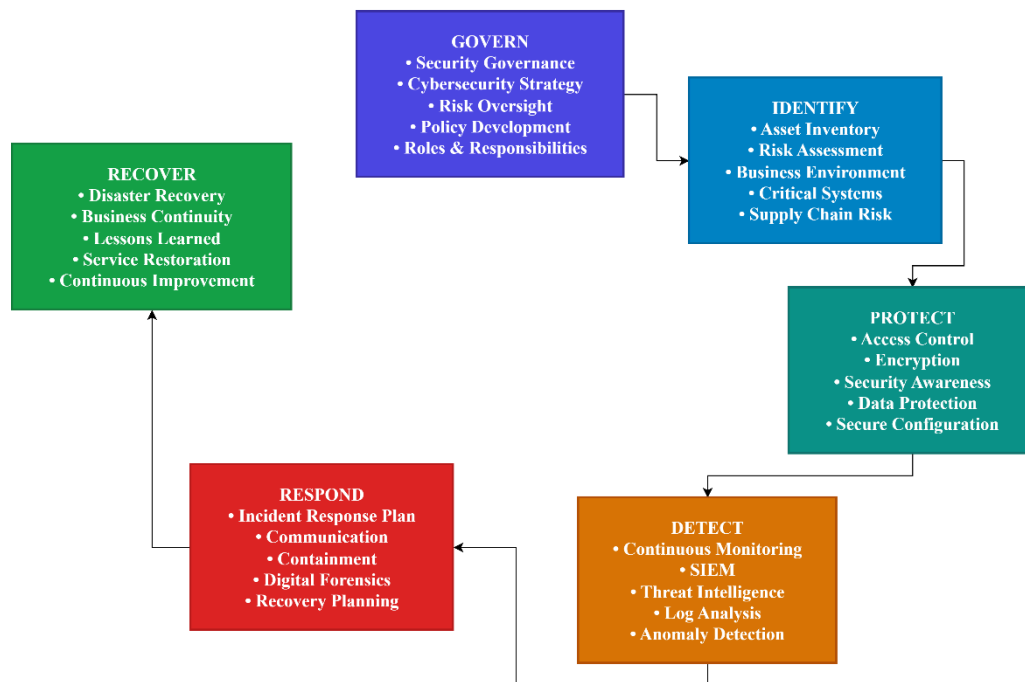


Figure 5: NIST Cybersecurity Framework

(Source; Self-developed)

NIST Cybersecurity Framework CSF 2.0 has six core functions such as Govern, Identify, Protect, Detect, Respond, and Recover that helps an organisation to manage the risks [19].

The framework has been accepted by Microsoft and other major infrastructure providers to enhance cyber resilience. Flexibility, risk-based decision-making, and compatibility with other standards, ISO/IEC 27001 are among its strengths [35].

3.3 ISO/IEC 27001 and ISO 27002



Figure 6: PDCA Cycle for ISO/IEC 27001

(Source: Self-developed)

Establishing an Information Security Management System (ISMS) by using standards ISO/IEC 27001 are recognized in the world [29]. The Annex A is highlighting ISO/IEC 27002, which provides guidance on implementing the controls specified to the work [36]. A third-party standard requires risk assessments in using the PDCA cycle to highlight risk treatments along with continual improvement such as HSBC maintains ISO/IEC 27001

certification [28]. For everyone, an advanced security management system such as ISO/IEC 27001 is a great framework for establishing this system [29].

3.4 COBIT 2019

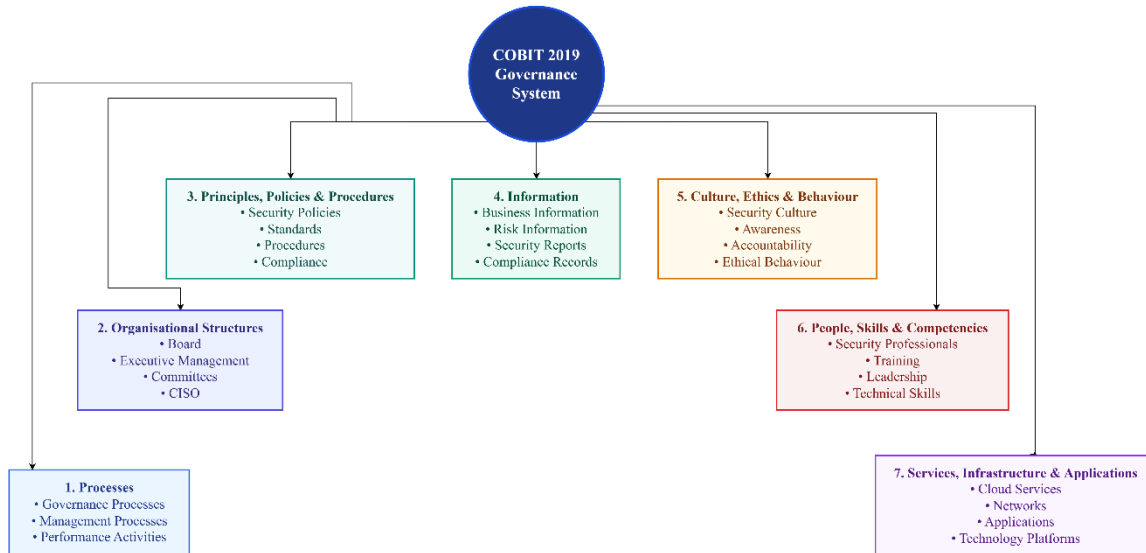


Figure 7: COBIT 2019 Governance Components

(Source: Self-developed)

A key performance measurement highlights the successful strategy decision making for launching good governance processes for COBIT 2019, which is developed by ISACA, as a governance and management framework that aligns IT business objectives [7]. Barclays's governance frameworks to strengthen IT governance are implementing COBIT principles along with operational accountability [10]. COBIT 2019 can enhance executive oversight across cybersecurity initiatives which highlight a high documentation that highlights the implementation complexity can inflate organizational cost.

3.5 ITIL 4

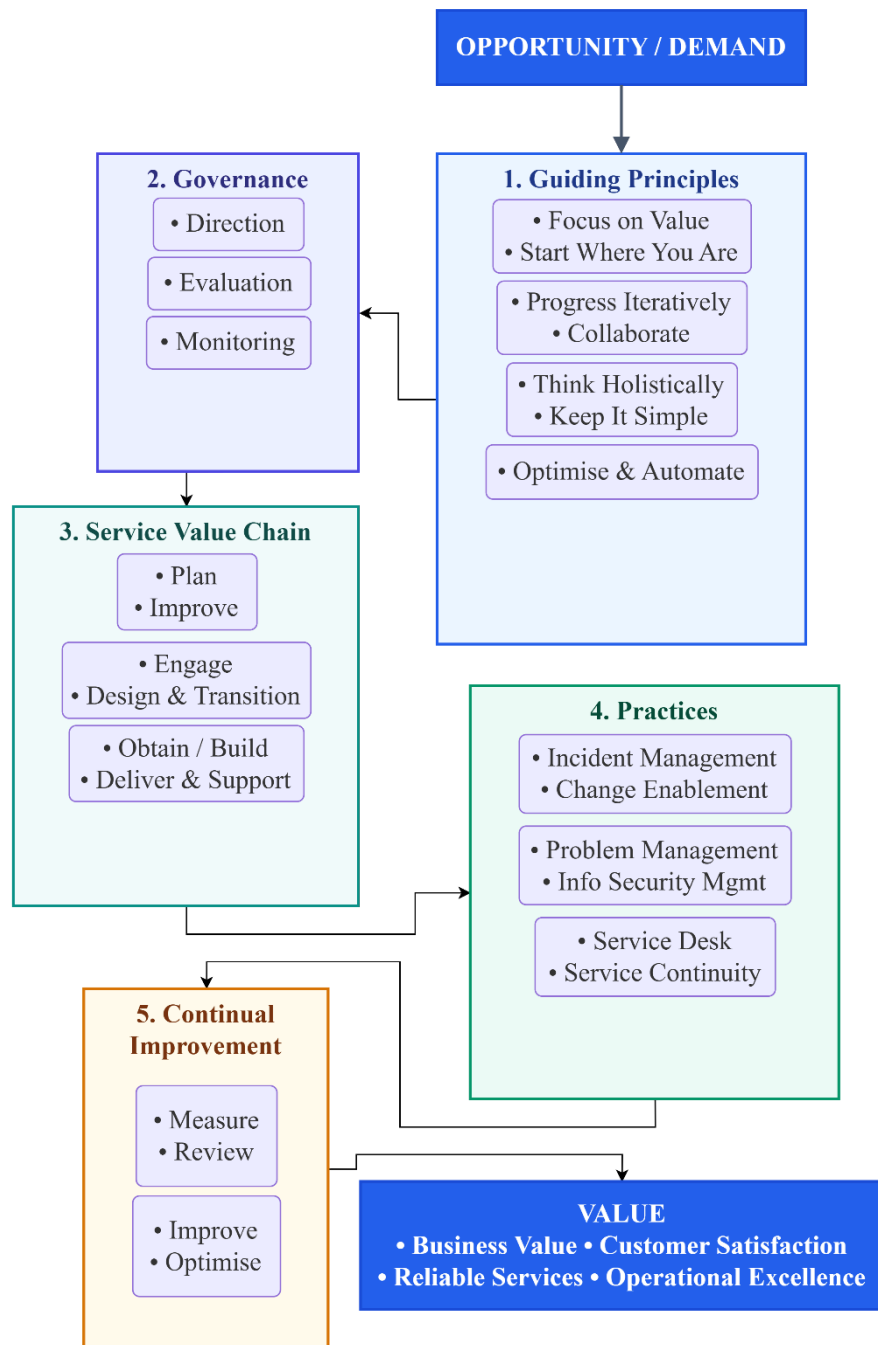


Figure 8: ITIL 4 Service Value System

(Source: Self-developed)

ITIL 4 is a global IT service management framework that is used in support of service delivery that uses practices like incident management change enablement problem management availability management continual improvement and more. The UK National Health Service (NHS) to improve service reliability by using ITIL principles which are

adopted by organisations efficiency [23]. The standardization of service processes improves the incident-handling process for business continuity and highlights that ITIL not cyber security governance as it focuses on service management [38]. ITIL 4 would enhance operational resilience, reduce service disruptions, and strengthen incident and change management processes in outsourced environments for everyone [14].

3.6 Zero Trust Security Model

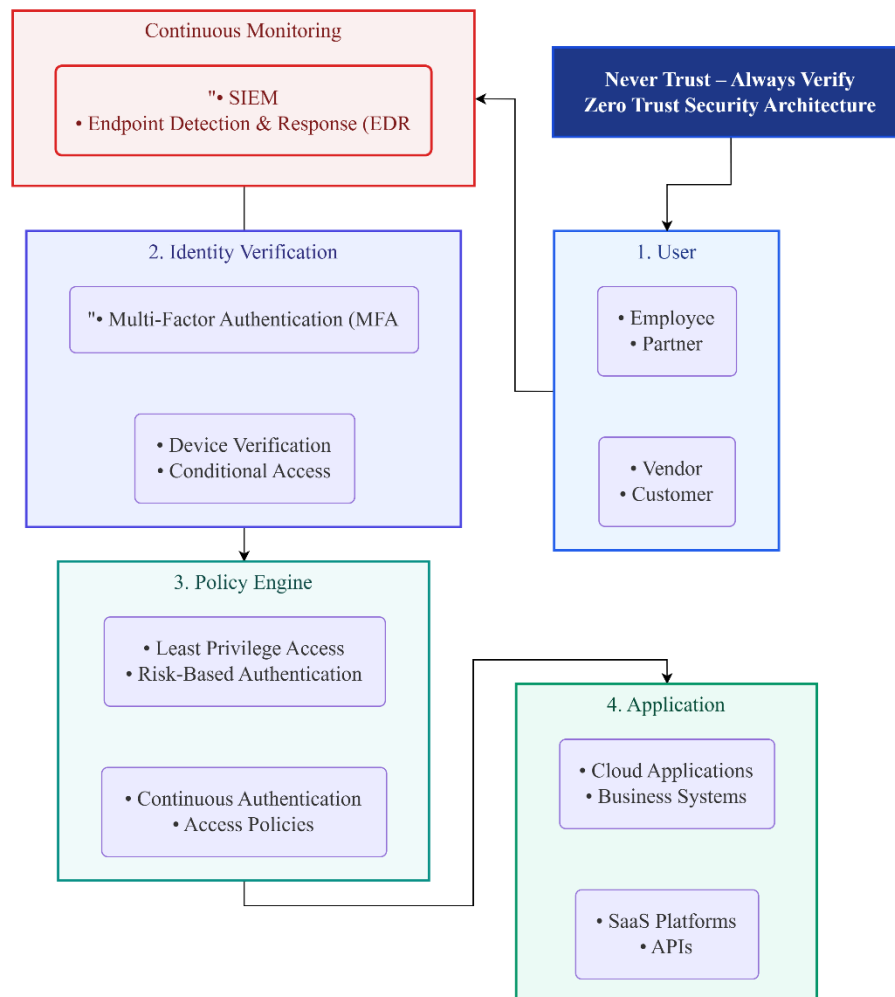


Figure 9: Zero Trust Model

(Source: Self-developed)

The zero trust security model developed by John Kindervag works on the principle of “Never Trust, Always Verify” [49]. Zero trust security enforces continuous authentication, least privilege access, verification of identity and micro-segmentation with every user regardless of location. Due to the growth of remote working, Google and other organisations switched to

the Beyond Corp Zero Trust architecture to secure its employees without a corporate network [16]. Although identity management technologies must be applied, Zero Trust considerably reduces insider threats and un-authorised access [50]. Zero-Trust has enhanced access control and identity verification to ensure the delivery of sensitive logistics data at ALL, which has a globally distributed workforce and unmanaged devices.

3.7 Shared Responsibility Model (Cloud)

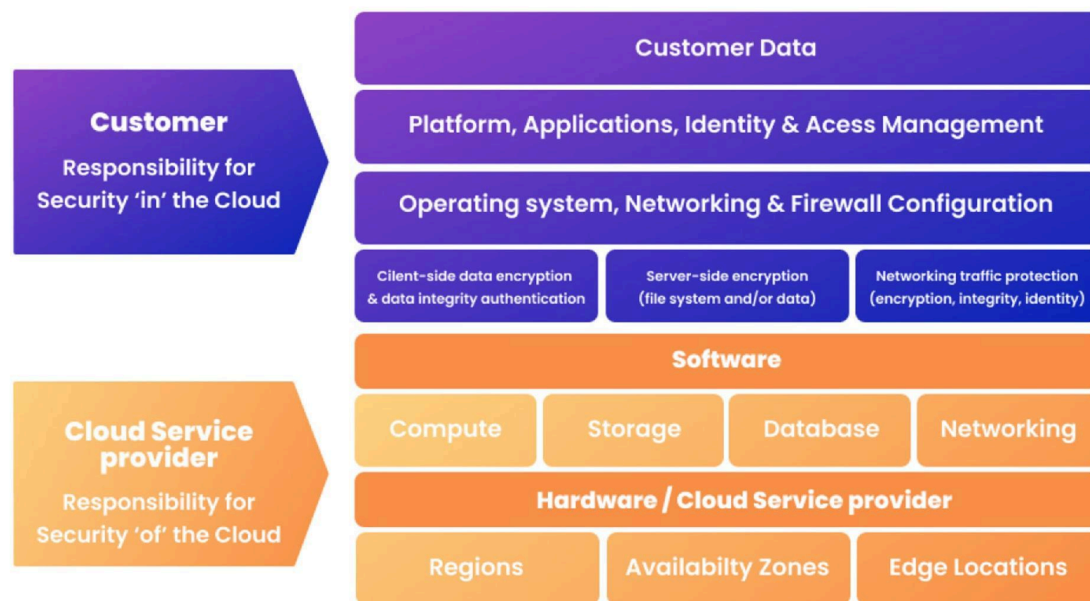


Figure 10: Cloud Security

(Source: SNYK, 2024)

The Shared Responsibility Model distinguishes between cloud provider and customer security obligations. Cloud service providers like Amazon Web Services (AWS), and Microsoft Azure secure the cloud infrastructure which includes physical facilities, networking and hardware with customers remaining responsible for accessing management, data protection, application security to access control. Not understanding these responsibilities is a key factor in data breaches involving exposed data storage services in the cloud [46]. IT infrastructure is outsourced to IaaS highlighting the 88% of AeroLink Logistics across SaaS vendors. The organization must adopt the Shared Responsibility Model which will clarify accountability, enhance vendor governance, and reduce the risk of cloud-related security events.

3.8 Comparative Evaluation

There is no singular framework that comprehensively covers ALL's requirements for governance, operations and compliance. The NIST CSF 2.0 offers full-fledged cyber risk management, while the ISO/IEC 27001 is a certified Information Security Management System and enables regulatory compliance [13]. The ITIL offers informative practices for IT services management [44] [21]. Zero Trust helps with identity-centric security issues around remote workers and the cloud [33]. Thus, the combined use of these frameworks will lead to greater organisational resilience than the use of either one alone. This strategy which combines hybrid helps enhance governance at All, reduce cyber risks and ensure ongoing compliance with regulations.

<i>Framework</i>	<i>Primary Strength</i>	<i>Limitation</i>	<i>Impact on ALL</i>
NIST CSF 2.0	risk management	organisational maturity	High
ISO/IEC 27001	ISMS certification	Certification	High
COBIT 2019	Strong governance	Extensive documentation	High
ITIL 4	Service management	Limited focus	Medium
Zero Trust Security Model	Strong protection,	High implementation cost	High

Table 2: Comparative Evaluation across Security Frameworks

(Source: Self-developed)

4 Design of an Integrated Security Governance Framework for AeroLink Logistics

4.1 Proposed Integrated Framework

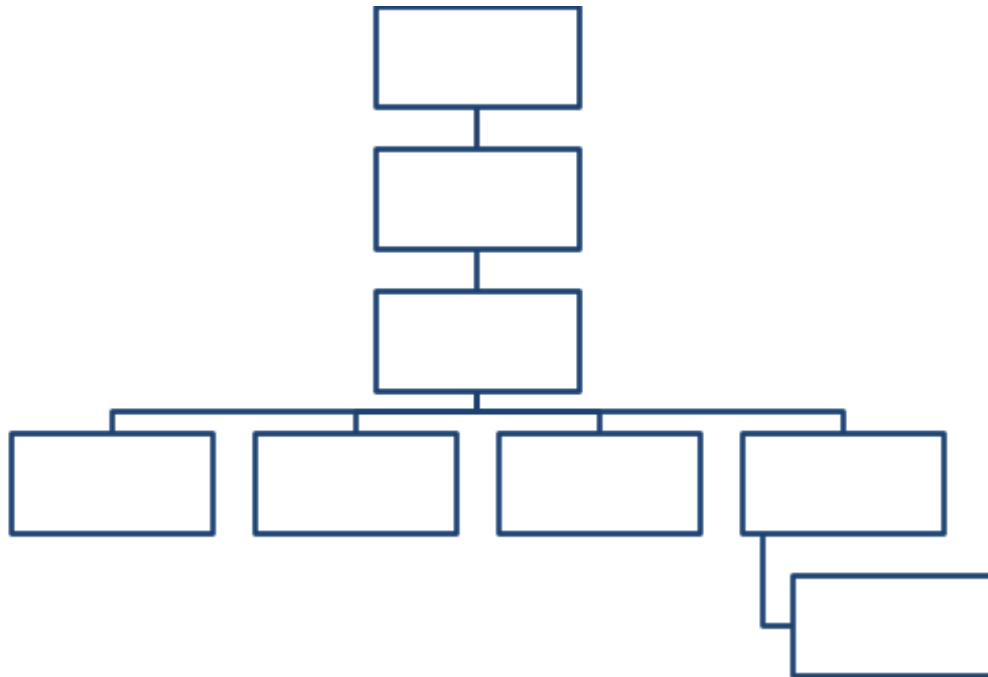


Figure 11: Security Governance Framework

(Source: Self-developed)

The framework establishes a governance structure to be followed in a top-down manner by the Board to provide strategic oversight. The Security Governance Committee, CISO, risk, compliance, operational and incident response functions will support. Constant monitoring will help achieve further improvements. In developing this—a comprehensive Cybersecurity and Risk Management framework, a specific methodology was adopted [39]. Rather than relying upon a single framework, ISO/IEC 27001 for ISMS, NIST CSF 2.0 for a cybersecurity risk management, COBIT 2019 for governance, Zero Trust for a persona or identity-centric security, and ITIL 4 for and service management has been integrated into the model [48]. Organisations like Microsoft and IBM use a similar system approach to enhance governance; strengthen resilience; and ensure regulatory compliance.

4.2 Governance Structure

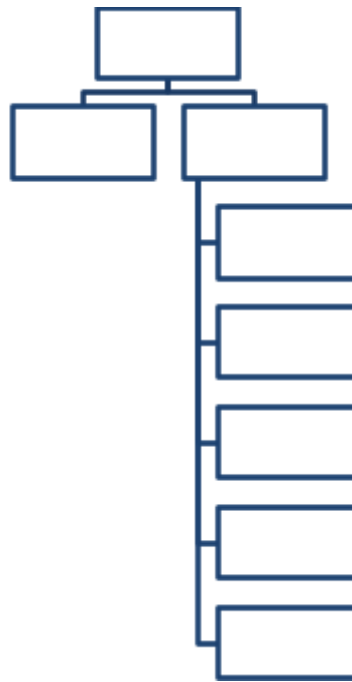


Figure 12: Organisation Chart

(Source: Self-developed)

The proposed governance structure for ALL clarifies responsibilities from the strategic level, through managerial and operational, to external stakeholders. CISO manages cybersecurity operational oversight and highlights the Board, which ensures governance oversight to CIO oversees technology strategy [45]. The SOC provides continuous monitoring for managing via legally-embedded service level agreements the DPO ensures compliance with the UK GDPR as a third parties [54]. Governance structures similar to those recommended in ISO/IEC 27001 and COBIT 2019, and which are widely employed by organisations such as the National Health Service (NHS), enhance accountability, regulatory compliance, and organisational resilience.

<i>Role</i>	<i>Primary Responsibility</i>
Board of Directors	Focused on governance
CIO	Strategy for digital transformation
CISO	Leadership

DPO	GDPR compliance
SOC	Continuous monitoring
Vendors	Security obligations

Table 3: Roles and Responsibilities of Governance

(Source: Self-developed)

4.3 Security Policies



Figure 13: Security Policy Flow

(Source: Self-developed)

Illustration 12 shows the hierarchical structure of governance policies, which are discussed in more detail, followed by Standards, procedures and operational guides. Every business needs to develop and implement security policy which should include acceptable use policy, password policy, data classification policy, encryption policy, remote working policy, mobile device security policy, and Bring Your Own Device (BYOD) policy [6]. These policies provide for secure remote access as per ISO/IEC 27001 Annex A controls and the UK National Cyber Security Centre (NCSC). Similar policy frameworks are in place at organisations like Barclays and HSBC to ensure security practices, comply with regulation and efficiently protect the organisation's information.

4.4 Risk Management Process

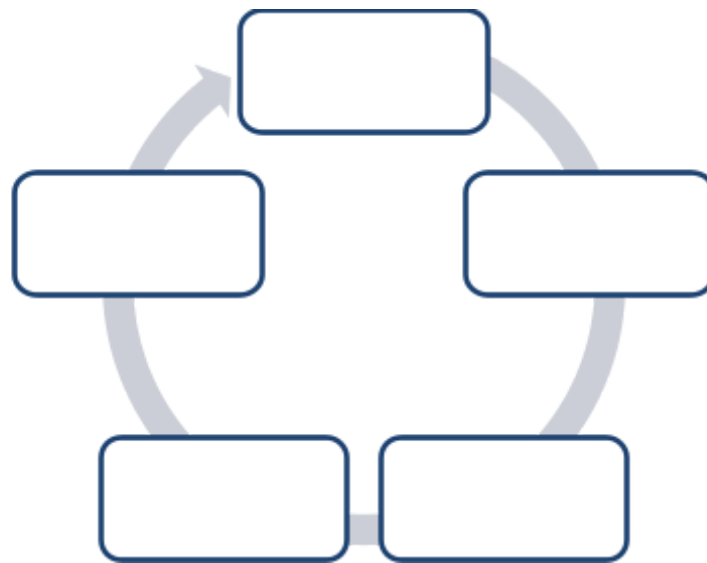


Figure 14: Risk Management Cycle

(Source: Self-developed)

As figure 13 shows, based on ISO/IEC 27005, the risk management cycle enables ALL to identify, assess, prioritise, treat and monitor cybersecurity risks [3]. Risk assessments must examine Cloud infrastructure, IoT devices, third-party suppliers, remote access and confidential customer data [3].

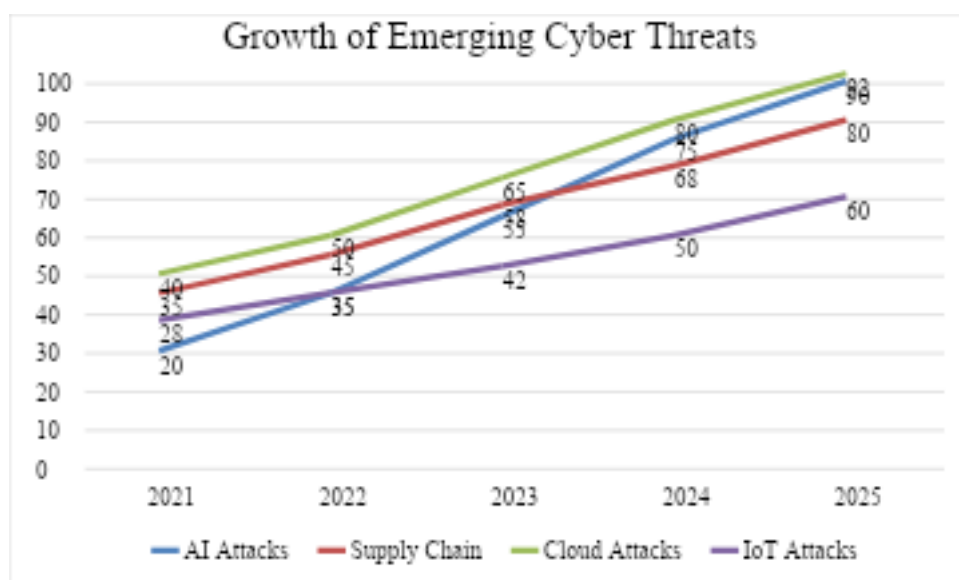


Figure 15: Cyber Threats

(Source: We Forum, 2025)

Continually monitoring all threats as they arise and controls remain effective. The adoption of ISO/IEC 27001 highlights the roles and responsibilities of the organisation which supports proactive decision-making in continual improvement [29].

4.5 Compliance Strategy

The Data Protection Act 2018 highlights different strands which include ISO/IEC 27001, the NIS Regulations, Cyber Essentials Plus, and PCI DSS for ALL's security programme which also comply with UK GDPR, [47]. Lower regulatory risk highlights the layered compliance system helps to achieve legal accountability. UK sectors use various frameworks to show resilience in these organisations working due to stakeholder confidence in ongoing compliance updates.

4.6 Protection Mechanisms

Depicted is a hypothetical example of a Defence-in-Depth architecture, as per the NIST document [51]. Microsoft Azure and AWS customers implement similar layered security architectures to minimise attack surfaces and improve organisational resilience.

4.7 Vendor and SLA Management

A vendor risk lifecycle begins with the supplier assessment and progresses through auditing, contractual governance, performance monitoring and continuous review. Given that ALL outsources around 88% of its IT infrastructure, vendor governance must be strong. The part of Service Level Agreements (SLAs) highlights the security requirements which highlight the standards with breach notification deadlines that indicate audit rights across compliance obligations [42]. Establishing key performance indicators (KPIs) reduces accountability in conducting regular third-party security assessments as supply chain risk [5]. The guidance of ISO/IEC 27036 highlights that organisations governance of third-party security following NIST Supply Chain Risk Management to adopt similar practices [40].

4.8 Incident Response

In accordance with the NIST Cybersecurity Framework, an incident response process was proposed. The process starts with preparation, followed by threat detection, containment, eradication and recovery, before lessons learned for better future resilience. Every organization should set up its own CSIRT with underlying SIEM technologies, detailed communication plans, and frequent simulation exercises. Organisations like the UK National

Cyber Security Centre (NCSC) recommend a structured process to deal with incidents to minimise the disruption of operations, reduce financial losses and improve organisational readiness against hackers [18].

4.9 Business Continuity

As outlined in Figure 18, the business continuity framework proposed contemplates that ALL must be able to conduct essential logistics operations in the event of cyber incidents and systems collapse. The establishment comprises a Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). They also incorporate cloud backup and conduct disaster recovery testing. These will be ISO 22301 Business Continuity Management compliant and are already being followed by cloud service providers with critical missions [17]. Constant testing enhancement for impending interruptions will help the organization sustain effectiveness and client satisfaction.

5 Critical Discussion: Continuous Updates to Regulations and Standards

Continuous updates are good practice as Cyber threats keep changing all the time with things, like ransomware attacks that use intelligence, new weaknesses that nobody knows about yet and problems that come from the supply chain. Regular updates help make sure that security methods work well against ways that hackers try to break in instead of just defending against old problems.

Emerging technologies have significantly expanded organizational attack surfaces like AI, IoT, and cloud computing, as well as anticipated quantum computing [13]. Cross-border data protection challenges are rising adoption of cloud-native architectures highlight the third-party platforms has posed more supply chain risks [34]. From the governance perspective it need to do as, ISO/IEC 27001:2022 recommends continual improvement of the ISMS framework through the PDCA cycle while the NIST CSF 2.0 recommends continuous governance, monitoring and risk management.

The NIS2 Directive has increased the cybersecurity requirements of some essential and important entities in Europe (such as hospitals, telecommunications providers), increasing supply chain security, governance accountability, and incident reporting requirements. Similarly, changes to UK GDPR guidance require organisations to keep re-assessing privacy controls as technology and processing change [19]. All organizations must integrate threat

intelligence, regulatory monitoring and periodic assessment of risks into governance processes to ensure compliance, strengthen organization resilience and address existing and emerging cyber threats.

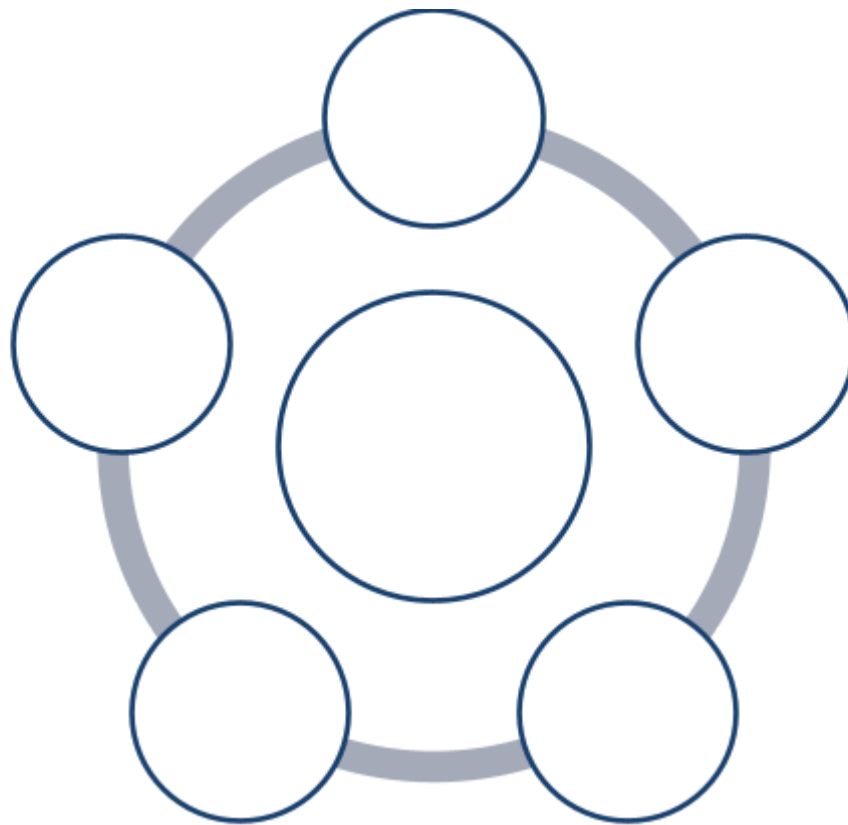


Figure 16: Continuous Compliance Improvement Cycle

(Source: Self-developed)

One-off compliance gives a snapshot of the security posture of the organisation and doesn't help with the dynamic nature of Cyber Threats. Adapting security controls that continuously evaluates risks verifies trust not just as a periodic compliance audit according to the Continuous Adaptive Risk and Trust Assessment (CARTA) model [1]. In 2024, the need for continuous monitoring in rapid recovery in a CrowdStrike software update incident that disrupted the services worldwide shows that vendors can expose organizations to operational risk [18].

6. Recommendations

The guidelines presented in ISO/IEC 27001 should form the basis of the organisation's Information Security Management System (ISMS) to create governance, risk and continual improvement (Humphreys, 2025).

Companies like HSBC maintain ISO/IEC 27001 certification to enhance information security and show compliance with regulations [43]. A zero-trust architecture that secures remote users and unmanaged devices should be implemented. A good example of this is Google's BeyondCorp which has successfully replaced the perimeter with identity. Due to ALL's massive outsourcings, vendor security audits must occur regularly.

Both Microsoft Azure and Amazon Web Services (AWS) have undertaken similar undertakings to evaluate their vendors all the time [53] [8]. Setting a Security Operations Centre (SOC) (24) will allow continuous monitoring and quicker response to incidents, similar to the operational models of the UK National Cyber Security Centre (NCSC) and major banks [41]. Training employees regularly on security awareness and conducting phishing simulations like

Barclays will greatly reduce the human aspect of cyber risk [11]. The UK GDPR, ISO/IEC 27001 in cyber are essentials which will promote continual improvement to enhance stakeholder confidence through effective governance [20].

7. Conclusion

This report appraises the leading information security framework and demonstrates the outcome of the integration of the framework to enhance the cyber security governance of AeroLink Logistics. According to the research, NIST CSF 2.0 along with ISO/IEC 27001, COBIT, ITIL 4 and Zero Trust Security model gives complementary capabilities for managing cyber risks, achieving business objectives and regulatory compliance. Drawing on these results, an integrated security governance framework was designed for diverse organisational oversight, risk assessment, protection mechanisms, vendor governance, incident response, and business continuity planning.

As the report further said, compliance must always be a continuous process given technology innovations, the emergence of new cyber threats and changing regulatory requirements. By applying continual improvement, carrying out periodic risk assessments, proactive governance and applying security standards which are recognized at the global level. AeroLink Logistics can significantly enhance its cyber-resilience protective information assets which are critical, maintain stakeholder or investor confidence and ensure continued compliance with regulations over the long term.

References

1. Akerele, J.I., Smart, D. and Leo, J., Data-Driven Governance Frameworks for Cyber Risk, Financial Security, and Digital Trust in Critical Infrastructure.
https://www.researchgate.net/profile/Elevane-M/publication/408495046_Data-Driven_Governance_Frameworks_for_Cyber_Risk_Financial_Security_and_Digital_Trust_in_Critical_Infrastructure_Author/links/6a4bba01d4da0457569ca388/Data-Driven-Governance-Frameworks-for-Cyber-Risk-Financial-Security-and-Digital-Trust-in-Critical-Infrastructure-Author.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. Almaayah, M. and Sulaiman, R.B., 2024. Cyber risk management in the Internet of Things: Frameworks, models, and best practices. *STAP Journal of Security Risk Management*, 2024(1), pp.3-23.
https://www.researchgate.net/profile/Rejwan-Bin-Sulaiman/publication/392957114_Cyber_Risk_Management_in_the_Internet_of_Things_Frameworks_Models_and_Best_Practices/links/696132655cc49c35ce7a4d3e/Cyber-Risk-Management-in-the-Internet-of-Things-Frameworks-Models-and-Best-Practices.pdf
4. Almarri, S., Issa, W., Keshk, M., Turnbull, B. and Moustafa, N., 2026. Cyberworthiness for Corporate Organisations: A Structured Review of Standards, Frameworks, and Future Directions. *Electronics*, 15(10), p.2133. <https://www.mdpi.com/2079-9292/15/10/2133>
5. Almohaimeed, M., Albalwy, F., Alharbi, R., Alqarni, A. and Aljohani, A., 2025. Developing a comprehensive cyber risk assessment framework for supply chains: insights into third-party vulnerabilities and security gaps. *Intell. Inf. Manage*, 17(3), pp.58-77.
https://www.researchgate.net/profile/Aisha-Alqarni-3/publication/397720422_Developing_a_Comprehensive_Cyber_Risk_Assessment_Framework_for_Supply_Chains_Insights_into_Third-Party_Vulnerabilities_and_Security_Gaps/links/692f250918a6405a30fa85a5/Developing-a-Comprehensive-Cyber-Risk-Assessment-Framework-for-Supply-Chains-Insights-into-Third-Party-Vulnerabilities-and-Security-Gaps.pdf

6. AlShalaan, M.R. and Fati, S.M., 2023. Enhancing organizational data security on employee-connected devices using BYOD policy. *Information*, 14(5), p.275.
<https://www.mdpi.com/2078-2489/14/5/275>
7. Amore, E., Dilger, T., Ploder, C., Bernsteiner, R. and Mezzenzana, M., 2023. Leverage the COBIT 2019 Design Toolkit in an SME Context: A Multiple Case Study. *KnE Social Sciences*, pp.73-101.
<https://knepublishing.com/index.php/KnE-Social/article/download/12636/20419>
8. Aslam, M., Khan Abbasi, M.A., Khalid, T., Shan, R.U., Ullah, S., Ahmad, T., Saeed, S., Alabbad, D.A. and Ahmad, R., 2022. Getting smarter about smart cities: Improving data security and privacy through compliance. *Sensors*, 22(23), p.9338.
<https://www.mdpi.com/1424-8220/22/23/9338>
9. AWS Amazon (2025) *Simplify third-party software risk assessments*. Available form: <https://aws.amazon.com/marketplace/features/vendor-insights/> Accessed on 03.08.2026
10. Barclays (2025) *External Supplier Control Obligation*. Available from: <https://home.barclays/content/dam/home-barclays/documents/who-we-are/our-suppliers/uk/Information%20and%20Cyber%20Security%20SCO%20v11.0.pdf> Accessed on 03.08.2025
11. Barclays Corporate (2025) *Are your cyber defences secure?* Available form: <https://www.barclayscorporate.com/insights/fraud-protection/cyber-threat-landscape/> Accessed on 03.08.2026
12. BBC (2025) *British Airways fined £20m over data breach*. Available from: <https://www.bbc.com/news/technology-54568784> Accessed on 03.08.2025
13. Benny Thomas, A., 2025. Framework for Improving Cybersecurity in Cloud based VoIP provider.
https://www.utupub.fi/bitstream/handle/10024/182211/BennyThomas_Alan_Thesis.pdf?sequence=4
14. 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+would+enhance+operational+resilience,+reduce+service+disruptions,+and+strengthen+incident+and+change+management+processes+in+outsourced+environments+for+everyone&ots=phmLo7_w0s&sig=WYulrsBdSyzigOJdzHLgiY10x5k

15. Chen, H. and Hai, Y., 2024. Exploring the critical success factors of information security management: a mixed-method approach. *Information & Computer Security*, 32(5), pp.545-572.

https://www.researchgate.net/profile/Hao-Chen-50/publication/377626669_Exploring_the_critical_success_factors_of_information_security_management_a_mixed-method_approach/links/676729e4117f340ec3d1a4c5/Exploring-the-critical-success-factors-of-information-security-management-a-mixed-method-approach.pdf

16. Cloud Google (2025) *What is Beyond Corp?* Available form:

<https://cloud.google.com/beyondcorp> Accessed on 03.08.2025

17. Crask, J., 2024. *Business continuity management: A practical guide to organizational resilience and ISO 22301*. Kogan Page Publishers.

https://books.google.com/books?hl=en&lr=&id=O98EEQAAQBAJ&oi=fnd&pg=PR1&dq=+ISO+22301+Business+Continuity+Management+compliant+and+are+already+being+followed+by+cloud+service+providers+with+critical+missions&ots=JfGmt13avq&sig=4b_NGbIDpiP4nrYejGneJ599IVM

18. Crowd Strike (2026) *CROWDSTRIKE 2026 GLOBAL THREAT REPORT*. Available form:

https://go.crowdstrike.com/2026-global-threat-report.html?utm_campaign=thih&utm_content=crwd-saia-eur-uki-en-psp-x-wht-gtr-tct_x_x_x-x-x&utm_medium=sem&utm_source=google&utm_term=cyber%20threats&utm_language=en-gb&cq_cmp=12208318263&cq_plac=&gad_source=1&gad_campaignid=12208318263&gbraid=0AAAAAC-K3YQV48aByS0ltDZQnDGYCUowq&gclid=Cj0KCQjw-MDTBhCgARIsAKAkdlS0jWtpRk-u-5-wZxXUkaKwlp9jzFepgz6KwE8JTdmQ5VpPP-OtXM4aAt0XEALw_wcB. Accessed on 03.08. 2026

19. Edwards, J. and Weaver, G., 2024. *The cybersecurity guide to governance, risk, and compliance*. John Wiley & Sons.

<https://books.google.com/books?hl=en&lr=&id=Y2b8EAAAQBAJ&oi=fnd&pg=PP1&dq=U+GDPR,+ISO/IEC+27001,+Cyber+Essentials+Plus+will+promote+continual+improvement>

[t+and+enhance+stakeholder+confidence+through+effective+governance&ots=DXUx6IKS8j&sig=Ukzh-Vcrt3l9P3YsPKXrsPM2N6o](https://books.google.com/books?hl=en&lr=&id=JysbEQAAQBAJ&oi=fnd&pg=PR19&dq=NIST+Cybersecurity+Framework+CSF+2.0+has+six+core+functions+such+as+Govern,+Identify,+Protect,+Detect,+Respond,+and+Recover+that+helps+an+organisation+to+manage+the+risk&ots=DXUx6IKS8j&sig=Ukzh-Vcrt3l9P3YsPKXrsPM2N6o)

20. 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+Cybersecurity+Framework+CSF+2.0+has+six+core+functions+such+as+Govern,+Identify,+Protect,+Detect,+Respond,+and+Recover+that+helps+an+organisation+to+manage+the+risk&ots=bNNL2zWn8m&sig=n1WqHrw5JpH9MUzXNWZf8fNebXE>
21. Ejairu, U., Aderamo, A.T., Olisakwe, H.C., Esiri, A.E., Adanma, U.M. and Solomon, N.O., 2024. Eco-friendly wastewater treatment technologies (concept): Conceptualizing advanced, sustainable wastewater treatment designs for industrial and municipal applications. *Comprehensive research and reviews in Engineering and Technology*, 2(1), pp.83-104.
<https://crrjournals.com/crret/sites/default/files/CRRET-2024-0063.pdf>
22. Faruq, M.O., 2025. A meta-analysis of cybersecurity framework integration in GRC platforms: Evidence from US enterprise audits. *Journal of Sustainable Development and Policy*, 1(01), pp.224-249. <https://jsdp-journal.org/index.php/jsdp/article/download/10/10>
23. Furusa, S.S. and Phahlane, M., 2026. Antecedents, Decisions, and Outcomes for ICT Governance Adoption in the African Public Sector: A Systematic Review Based on McClelland Theory and ADO Framework. *Computers*, 15(8), p.476.
<https://www.mdpi.com/2073-431X/15/8/476>
24. Gracy, S.S., 2025. A global analysis of data breaches from 2004 to 2024. *arXiv preprint arXiv:2502.05205*. <https://arxiv.org/pdf/2502.05205>
25. Grigaliūnas, Š., Schmidt, M., Brūzgienė, R., Smyrli, P., Andreou, S. and Lopata, A., 2024. Holistic information security management and compliance framework. *Electronics*, 13(19), p.3955. <https://www.mdpi.com/2079-9292/13/19/3955>
26. Hasan, A., Shrestha, A. and Jha, K.N., 2024. *Construction company management*. Taylor & Francis.
<https://www.researchgate.net/profile/Constantinos-Challoumis-Konstantinos-Challoumes/pub>

[lication/389002038_Management_of_Enterprises_in_the_Greek_Economy/links/67b0a318645ef274a481e7f7/Management-of-Enterprises-in-the-Greek-Economy.pdf](https://www.researchgate.net/publication/389002038_Management_of_Enterprises_in_the_Greek_Economy/links/67b0a318645ef274a481e7f7/Management-of-Enterprises-in-the-Greek-Economy.pdf)

27. Hasan, M. and Faruq, M.O., 2025. AI-augmented risk detection in cybersecurity compliance: A GRC-based evaluation in healthcare and financial systems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), pp.313-342.

<https://global.asrcconference.com/index.php/asrc/article/download/15/16>

28. HSBC (2026) *Trust in Technology*. Available from:

<https://www.hsbc.com/-/files/hsbc/media/media-release/2017/170609-updated-trust-in-technology-final-report.pdf> Accessed on 03.08.2025

29. 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=organisations+implementing+ISO/IEC+27001+supports+proactive+decision-making+and+continual+improvement&ots=qAM41YFYhS&sig=WDXNZcE17FDoOiqhg-NNj_RTosg

30. 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=nes+presented+in+ISO/IEC+27001+should+form+the+basis+of+the+organisation%E2%80%99s+Information+Security+Management+System+\(ISMS\)&ots=qAM41XN_IO&sig=5eweP_oRW0kD8ITS0G5YodB59OrE](https://books.google.com/books?hl=en&lr=&id=5s_BEQAAQBAJ&oi=fnd&pg=PR13&dq=nes+presented+in+ISO/IEC+27001+should+form+the+basis+of+the+organisation%E2%80%99s+Information+Security+Management+System+(ISMS)&ots=qAM41XN_IO&sig=5eweP_oRW0kD8ITS0G5YodB59OrE)

31. 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=Standards+ISO/IEC+27001+are+recognized+in+the+world+for+establishing+an+Information+Security+Management+System+\(ISMS\)&ots=qAM41XMVnU&sig=kUmzY7IMD5Hpnq7xxi6Gf3uUfKI](https://books.google.com/books?hl=en&lr=&id=5s_BEQAAQBAJ&oi=fnd&pg=PR13&dq=Standards+ISO/IEC+27001+are+recognized+in+the+world+for+establishing+an+Information+Security+Management+System+(ISMS)&ots=qAM41XMVnU&sig=kUmzY7IMD5Hpnq7xxi6Gf3uUfKI)

32. 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=I

SO/IEC+27001+is+a+great+framework+for+establishing+an+advanced+security+manageme
nt+system&ots=qAM41XMZjV&sig=ZG5CKXJfi8etQ1QQT4waC_JmCSI

33. Joe, D., 2025. Challenges and Best Practices in Deploying Zero Trust Security Frameworks for Cloud-Based Remote Work Infrastructure.

https://www.researchgate.net/profile/Kehinde-Akingbade-2/publication/404883843_Challenges_and_Best_Practices_in_Deploying_Zero_Trust_Security_Frameworks_for_Cloud-Based_Remote_Work_Infrastructure/links/6a064cc4e93d461915961de0/Challenges-and-Best-Practices-in-Deploying-Zero-Trust-Security-Frameworks-for-Cloud-Based-Remote-Work-Infrastructure.pdf

34. Kethu, S.S., 2020. AI and IoT-driven CRM with cloud computing: Intelligent frameworks and empirical models for banking industry applications. *International Journal of Modern Electronics and Communication Engineering (IJMECE)*, 8(1), p.54.

https://www.researchgate.net/profile/Sai-Kethu/publication/396930736_AI_and_IoT-Driven_CRM_with_Cloud_Computing_Intelligent_Frameworks_and_Empirical_Models_for_Banking_Industry_Applications/links/68ff44497d9a4d4e870cf283/AI-and-IoT-Driven-CRM-with-Cloud-Computing-Intelligent-Frameworks-and-Empirical-Models-for-Banking-Industry-Applications.pdf

35. Kуттенбергер, F., 2026. A framework for the economic and simultaneously implementation of the ISO/IEC 27001 standard and the European Union's NIS2 Directive in renewable and conventional power plants. *International Journal of Critical Infrastructure Protection*, p.100863. <https://www.sciencedirect.com/science/article/pii/S1874548226000351>

36. Malatji, M., 2023, January. Management of enterprise cyber security: A review of ISO/IEC 27001: 2022. In *2023 International conference on cyber management and engineering (CyMaEn)* (pp. 117-122). IEEE.

<https://www.johanolausson.com/management.pdf>

37. Malgieri, G., 2023. *Vulnerability and data protection law*. Oxford University Press.

<https://books.google.com/books?hl=en&lr=&id=caO3EAAQBAJ&oi=fnd&pg=PP1&dq=UK+GDPR,+the+Data+Protection+Act+2018+and+other+relevant+laws&ots=0K-L4lf2y-&sig=fcRK44Rh8uRt1Hr3hhMXKWTr78s>

38. 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>
39. Melaku, H.M., 2023. Context-based and adaptive cybersecurity risk management framework. *Risks*, 11(6), p.101. <https://www.mdpi.com/2227-9091/11/6/101>
40. 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* 2025, 5, 33 [online] <https://www.mdpi.com/2305-6703/5/4/33>
41. NCSC (2025) *Building a Security Operations Centre (SOC)*. Available form: <https://www.ncsc.gov.uk/collection/building-a-security-operations-centre> Accessed on 03.08.2026
42. 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>
43. Nurani, N. and Legowo, N., 2026. Assessing Information Security Risk Exposure During the Transition from ISO/IEC 27001: 2013 to ISO/IEC 27001: 2022 in a Banking Institution. *Information*, 17(7), p.692. <https://www.mdpi.com/2078-2489/17/7/692>
44. Otkhozoria, N., Petriashvili, L., Zhvania, T. and Lortkipanidze, N., 2024. The Critical Role of Information Technology Service Management Using ITIL Best Practices to Improve Business Management. *Works of GTU*, 2(532), pp.171-176.
<https://www.academia.edu/download/120414169/1512-0996-2024-2-171-176.pdf>
45. 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
46. Pimenta Rodrigues, G.A., Marques Serrano, A.L., Lopes Espiñeira Lemos, A.N., Canedo, E.D., Mendonça, F.L.L.D., de Oliveira Albuquerque, R., Sandoval Orozco, A.L. and García Villalba, L.J., 2024. Understanding data breach from a global perspective: Incident

visualization and data protection law review. *Data*, 9(2), p.27.

<https://www.mdpi.com/2306-5729/9/2/27>

47. Riurean, S., Fiță, N.D., Păsculescu, D. and Slușariuc, R., 2025. Securing photovoltaic systems as critical infrastructure: A multi-layered assessment of risk, safety, and cybersecurity. *Sustainability*, 17(10), p.4397. <https://www.mdpi.com/2071-1050/17/10/4397>

48. RRSg (2024) *The PECB academy in your language: 132 official certifications with real specialisation in cybersecurity and GRC*. Available form:

https://www.rrsg.eu/?gad_source=1&gad_campaignid=24006540928&gbraid=0AAAABEJkPeCRRknP3M2gBqdM3-gmrtKzy&gclid=Cj0KCQjw-MDTBhCgARIsAKAkdlTZIfmMWrbJ4bNFZrXJ2SiCCyuvgaWK2stlEu90Op_7ghyF_Vd7oKEaAnMPEALw_wcB Accessed on 03.08.2026

49. Shekhar, P.C., 2022. Never Trust, Always Verify: Zero Trust Security Testing Framework. <https://philarchive.org/archive/CHANTA-46>

50. Shelby, J., 2026. Cybersecurity Risk Assessment for CubeSat Missions: Adapting Established Frameworks for Resource-Constrained Environments. *arXiv preprint arXiv:2604.00303*.

<https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/51809/202695.pdf?sequence=2&isAlloWed=y>

51. Singh, H., 2024. Strengthening endpoint security to reduce attack vectors in distributed work environments. *Available at SSRN 5267844*.

<https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5267844>

52. Statista (2025) Infrastructure as a Service (IaaS) - statistics & facts. Available from:

<https://www.statista.com/topics/2739/cloud-infrastructure-as-a-service/?srsltid=AfmBOorr1lYGQ7dqNHL83UE7VoxzTERhJuYGs4Zm4-psOBOL0OpZZ5LH> Accessed on 03.08.2025

53. Telefonica Tech (2026) 5 Signs Your Microsoft Azure Environment Needs a Review. Available form:

[https://telefonicatech.uk/articles/5-signs-your-microsoft-azure-environment-needs-a-review/?utm_term=microsoft%20azure&utm_campaign=Cloud:+Azure+Estate+Assessment+Blog+\(Awareness\)&utm_source=adwords&utm_medium=ppc&utm_id=24083435651&hsa_acc=90](https://telefonicatech.uk/articles/5-signs-your-microsoft-azure-environment-needs-a-review/?utm_term=microsoft%20azure&utm_campaign=Cloud:+Azure+Estate+Assessment+Blog+(Awareness)&utm_source=adwords&utm_medium=ppc&utm_id=24083435651&hsa_acc=90)

68982291&hsa_cam=24083435651&hsa_grp=195992820622&hsa_ad=818777583763&hsa_src=g&hsa_tgt=kwd-10524847590&hsa_kw=microsoft%20azure&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gad_source=1&gad_campaignid=24083435651&gbraid=0AAAAA-ZxFba63w_AHla38nPFI12UTRcvI&gclid=Cj0KCOjw-MDTBhCgARIsAKAkdIQ3q9RnDzb4vthOBaq2iX0IGoEogzCSDDKDrK-BWvBbFmct-OdJarYaApNhEALw_wcB Accessed on 03.08.2026

54. ΠΟΥΤΑΚΙΑΔΟΥ, Α., General Data Protection Regulation (GDPR) compliance and its impact on private companies' operations.

https://www.academia.edu/download/122516899/Paper7_2025April4.pdf

