



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

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: Poshiya Janvi Vivekkumar

Student ID: 2543705

Abstract

The fast integration of cloud computing, artificial intelligence (AI), IoT technologies, and outsourced IT operations has caused cyber security risks and governance challenges to increase considerably. This report will analyse the cybersecurity and governance risks faced by AeroLink Logistics (ALL), a multinational logistics company with data breaches and no coherent security governance framework. The report will provide an evaluation of some well-known security frameworks, namely the NIST Cybersecurity Framework (CSF) 2.0, ISO/IEC 27001 and ISO/IEC 27002, COBIT 2019, ITIL 4, Zero Trust Security Model, and Shared Responsibility Model for cloud computing. Leveraging the strengths of all these models, a holistic security governance model can be designed in order to improve risk management, regulatory compliance, vendor governance, access management, incident management, and business continuity. In addition to this, this report highlights the significance of continuous updating of security regulations and standards due to the emergence of new technologies and cyber threats.

Table of Contents

1. Introduction.....	4
1.1 Background.....	4
1.2 Problem Statement.....	4
1.3 Aim.....	5
1.4 Objectives.....	5
1.5 Report Structure.....	6
2. Case Scenario Analysis and Assumptions.....	6
2.1 Current Security Challenges.....	6
2.2 Assumptions.....	7
3. Critical Review of Security Frameworks and Models.....	8
3.1 NIST Cybersecurity Framework (CSF) 2.0.....	10
3.2 ISO/IEC 27001 and ISO/IEC 27002.....	11
3.3 COBIT 2019.....	12
3.4 ITIL 4.....	13
3.5 Zero Trust Security Model.....	14
3.6 Shared Responsibility Model (Cloud).....	15
3.7 Comparative Evaluation.....	16
4. Proposed Integrated Security Governance Framework for AeroLink Logistics.....	17
4.1 Proposed Integrated Security Governance Model.....	17
4.2 Governance Structure.....	18
4.3 Risk Management Framework.....	20
4.4 Security Policies.....	21
4.5 Protection Mechanisms.....	22
4.6 Vendor Governance.....	23
4.7 Compliance Framework.....	25
4.8 Incident Response.....	26
4.9 Business Continuity.....	27
5. Critical Discussion: Why Continuous Updates to Regulations and Standards Matter.....	28
6. Conclusion and Recommendations.....	29
Reference.....	30

1. Introduction

1.1 Background

The use of digital technologies, including cloud computing, artificial intelligence (AI), and the Internet of Things (IoT), has become essential for the current business processes that enable businesses to communicate, automate, predict, and connect worldwide. At the same time, the adoption of remote work systems and outsourcing of IT functions has made organizations more flexible but complicated the process of information security management.

1.2 Problem Statement

The multinational logistics and supply chain company such as AeroLink Logistics (ALL) is facing difficulties because of its strong dependence on cloud solutions, Internet of Things (IoT) tracking systems, AI analytics, as well as on external IaaS and SaaS providers. However, regardless of these developments in technology, ALL has experienced multiple data breaches related to customer PII and revealed serious deficiencies in such areas as governance, risk management, vendor management, and standard compliance such as GDPR and ISO/IEC 27001.

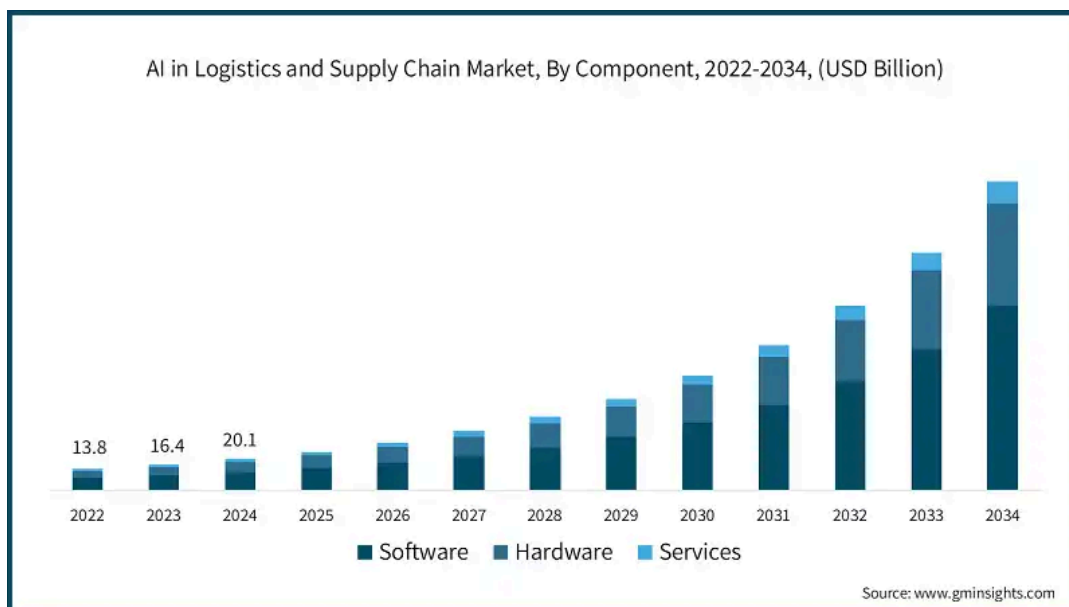


Figure 1: AI in Logistics and Supply Chain Market Analysis

(Source: [24])

According to the report of the global AI in logistics and supply chain market, the market was estimated at £14.96 billion (USD 20.1 billion) in 2024. The forecast is that the CAGR of the market from 2025 to 2034 will be 25.9% [24]. The major drivers for such growth include growing demand for visibility, routing optimization, and warehouse automation.

1.3 Aim

The aim of this report is to create an integrated information security governance strategy which will solve the problems of security, governance, and compliance faced by AeroLink Logistics.

1.4 Objectives

- To critically evaluate established information security frameworks and governance models.
- To assess the information security, governance, and compliance challenges.
- To develop a holistic security governance model for the organisation to cater for its security, risk management, vendor management, and compliance needs.
- To elaborate on the need for continually revising security policies and compliance rules.

1.5 Report Structure

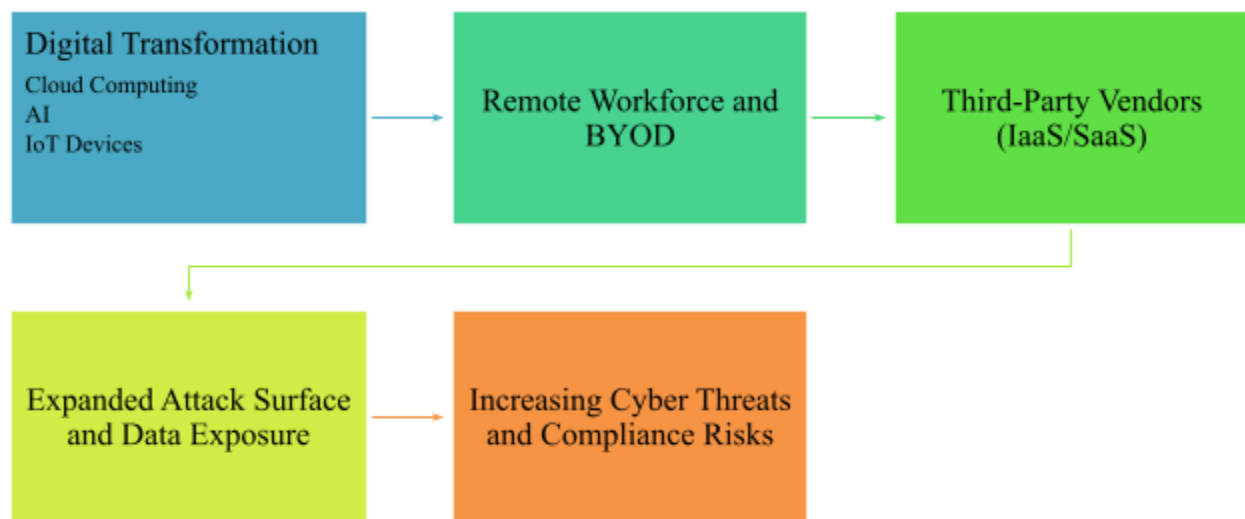


Figure 2: Digital Transformation and Expanding Cyber Attack Surface

(Source: Self-developed)

This research paper will critically analyze the existing security frameworks/models, the formulation of a proper security governance framework, and the need for the relevance of updating security policies/standards due to technological developments and new threats.

2. Case Scenario Analysis and Assumptions

2.1 Current Security Challenges

AeroLink Logistics (ALL) exists within an interwoven digital ecosystem that relies significantly on the use of cloud computing, internet of things, artificial intelligence, and third-party vendors. While technological innovations have ensured that the operations of the organisation have become more efficient, it has also meant that cyber threats have grown for ALL [16]. This is due to the absence of a full-fledged cybersecurity governance structure, effective risk management practices, proper vendor management, and compliance with information security standards.

Current Problem	Business Impact
No unified security governance	Lack of accountability and lack of consistency in decision-making
Heavy cloud dependency	Increase in third-party and vendor risk
Remote workforce and unmanaged devices	Increased risk to endpoints
Lack of ISO/IEC 27001 compliance	More regulations and legal repercussions
Weak incident response capability	Delayed detection, containment, and recovery
Customer PII breaches	Non-compliance with GDPR
No formal business continuity planning	Increased disruptions during incidents

Table 1: Current Security Challenges

(Source: Self-developed)

2.2 Assumptions

Based on the assumptions made, AeroLink Logistics is an international company with more than 65000 employees and relies on IT infrastructure through cloud-based services IaaS and SaaS, as well as 1350 logistic facilities [2]. The company deals with processing personal data of its customers who are from the UK and European Union countries. Therefore, AeroLink Logistics has to adhere to the following standards such as UK GDPR, EU GDPR, ISO/IEC 27001, NIS2, and Cyber Essentials Plus. It is also assumed that AeroLink Logistics has a medium to large corporate security budget and a low maturity level in information security governance [3].

According to the case scenario, the current security maturity assessment of AeroLink Logistics shows several weaknesses in the above areas.



Figure 3: Current Security Maturity Assessment

(Source: Self-developed)

3. Critical Review of Security Frameworks and Models

With the increased adoption of cloud computing, IoT, and AI, and outsourcing IT solutions by businesses, there needs to be an information security framework to improve governance, solve information security and cybersecurity issues, and comply with legal requirements [45]. However, despite the existence of various internationally acclaimed information security frameworks, each of them caters to some aspect of information security and governance [33]. As a result, instead of using one framework, organisations with advanced digital technology infrastructure, such as AeroLink Logistics (ALL) that use a combined framework.

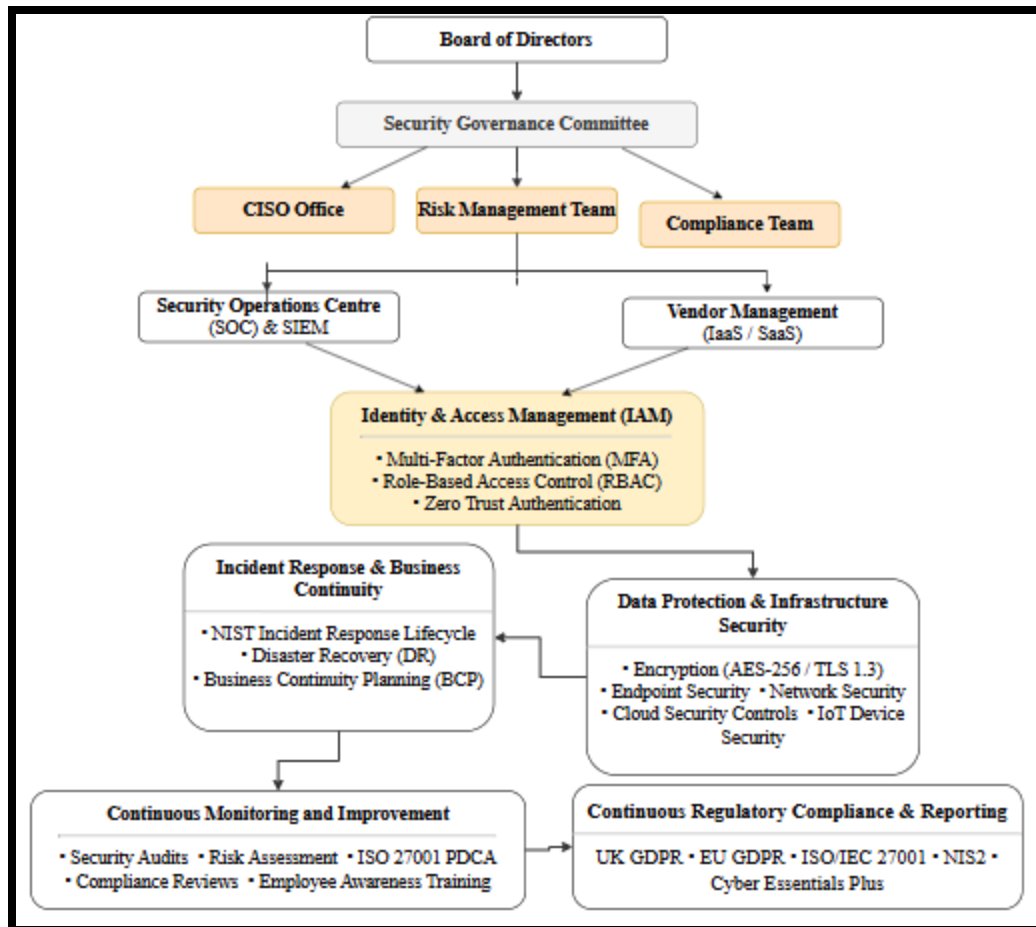


Figure 4: Integrated Security Governance Framework

(Source: Self-developed)

3.1 NIST Cybersecurity Framework (CSF) 2.0

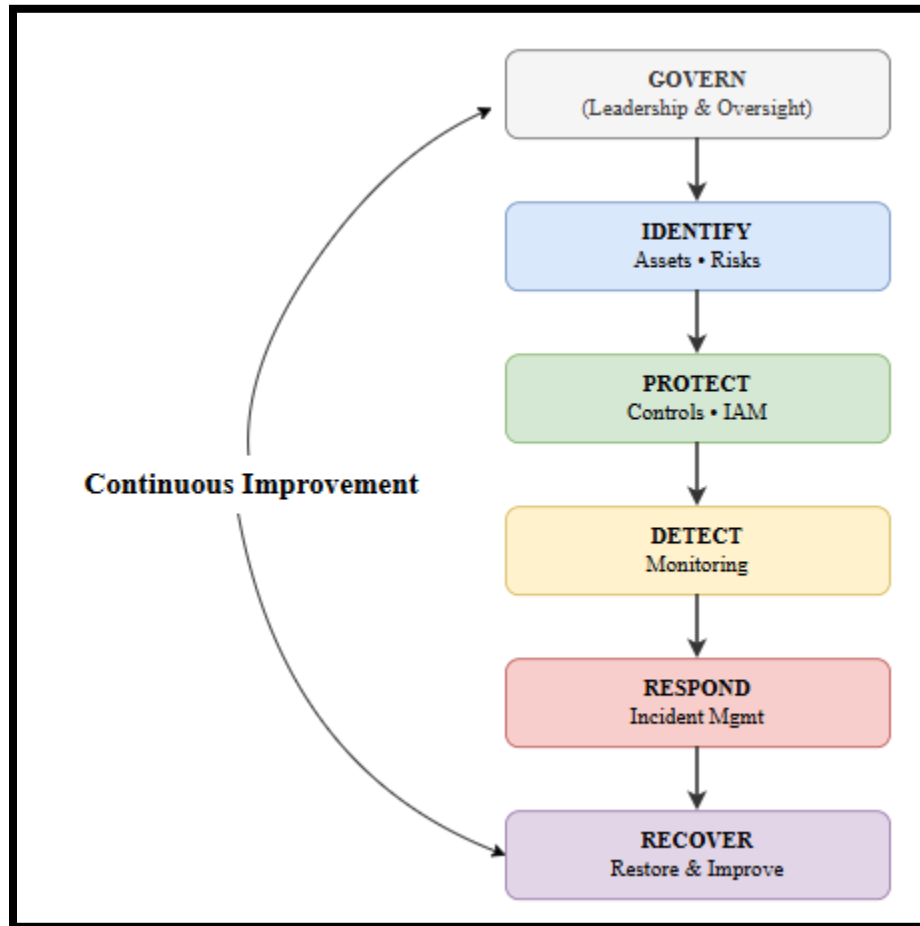


Figure 5: NIST Cybersecurity Framework

(Source: Self-developed)

The NIST Cybersecurity Framework (CSF) 2.0 provides an adaptable and risk-based approach for the management of cybersecurity using six primary functions [42]. The elements include govern, identify, protect, detect, respond, and recover, and they help organizations to counter cyber threats. The element of govern is useful as it helps to increase the involvement of management in cybersecurity [36]. As opposed to compliance-oriented frameworks, the NIST framework is more flexible and more suitable for cloud-driven and technology-heavy organisations. It does not give any implementation controls but rather needs to be supplemented by other standards.

3.2 ISO/IEC 27001 and ISO/IEC 27002

ISO/IEC 27001 provides an established ISMS approach based on risk management practices, while ISO/IEC 27002 describes guidelines for security practices implementation [17].

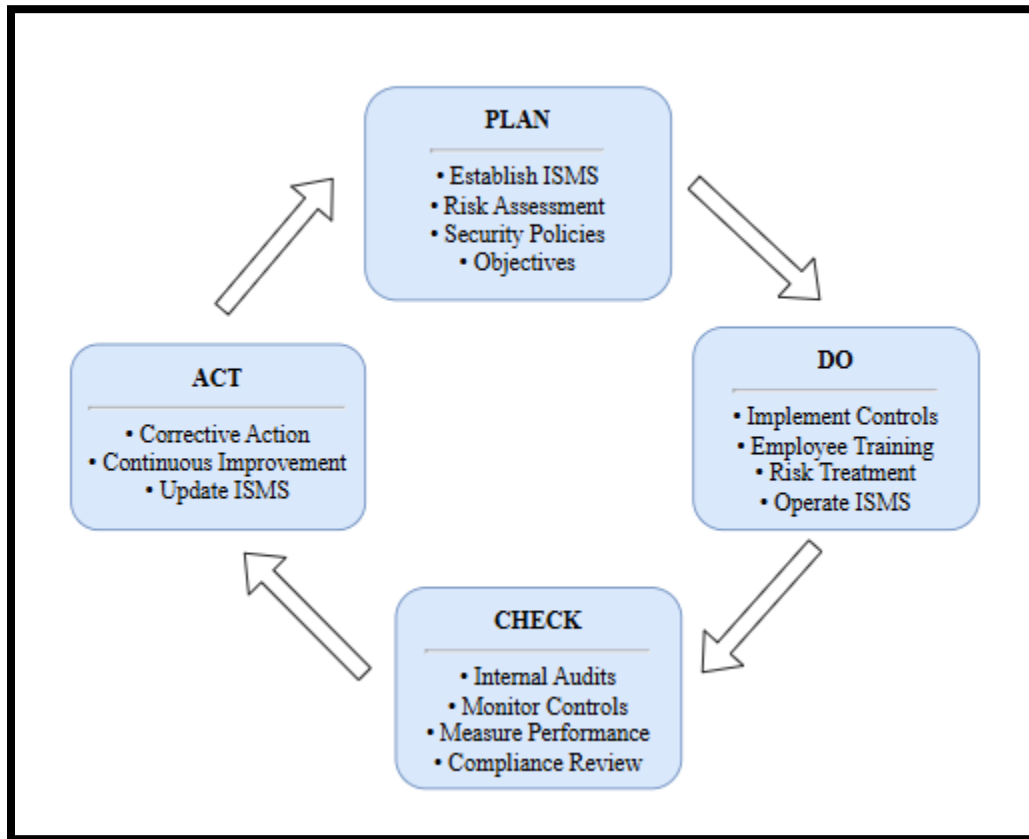


Figure 5: PDCA Cycle of ISO/IEC 27001 Information Security Management System (ISMS)

(Source: Self-developed)

This information security framework follows the principles of PDCA and focuses on continuous improvement and governance. The difference from NIST is that ISO 27001 has some certification procedures to demonstrate commitment to the legislation and information security [28]. However, the implementation of ISO 27001 requires much more effort and money than \$70,000 (£52090.50) [43]. In the case of ALL, ISO 27001 will bring governance, better information security controls, and UK GDPR compliance.

3.3 COBIT 2019

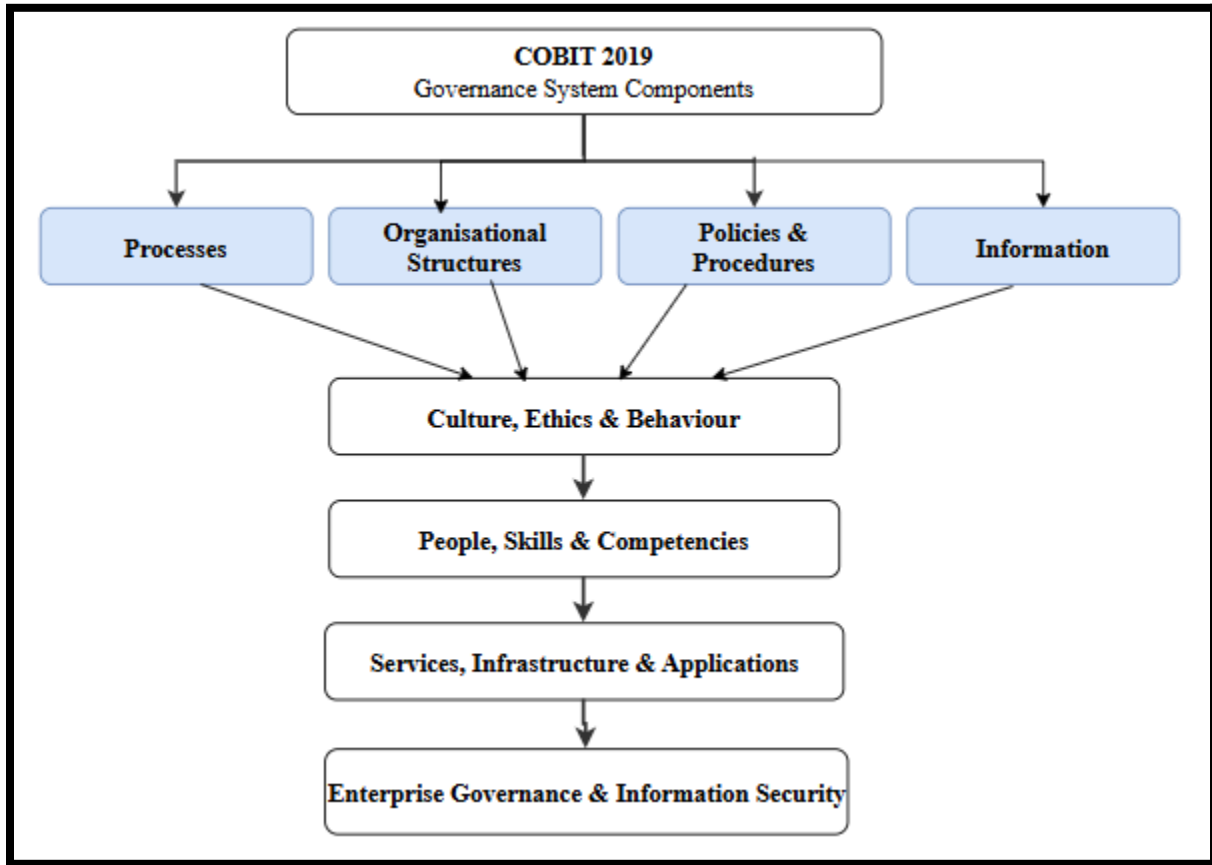


Figure 5: COBIT 2019 Governance System

(Source: Self-developed)

The COBIT 2019 framework has a broader scope than cybersecurity as it presents a governing system to maintain alignment of the organisation's information systems [36]. The governance and management goals outlined in the COBIT 2019 framework guarantee executives the necessary overview of governance and performance. Moreover, it helps in making optimal utilisation of resources as well as risk governance [46]. In contrast to ISO 27001, the COBIT 2019 model creates business value, not information security [52]. It may be difficult to incorporate, as a wide range of the COBIT framework may produce adoption difficulties due to organisational governance maturity.

3.4 ITIL 4

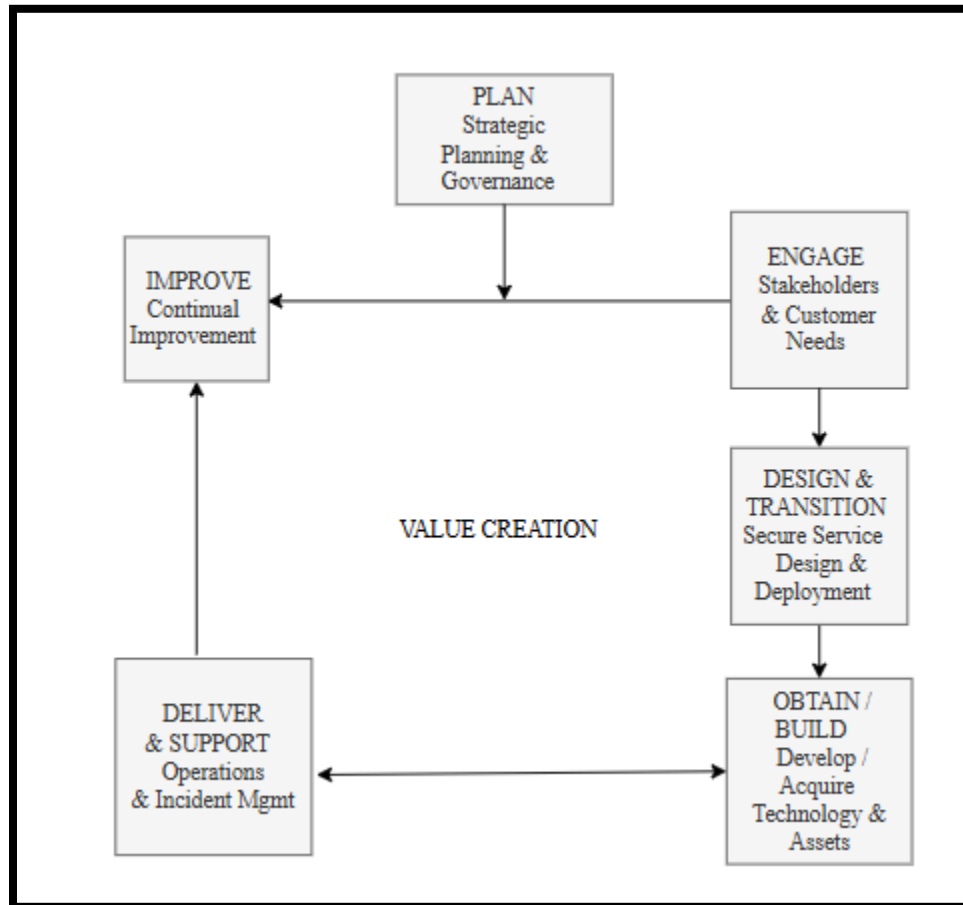


Figure 7: ITIL 4 Service Value Chain

(Source: Self-developed)

By replacing ITIL v3 and ITIL Practitioner, ITIL 4 provides digital change solutions due to an increased interest in digitalization [9]. ITSM also provides a system of continuous improvement by means of the Service Value Chain of ITIL 4, which is focused on the good design of service, incident management, problem management, change management, and operation management [26]. Hence, ITSM helps provide resiliency, availability, and continuous improvement, but ITIL cannot provide a cybersecurity solution [7]. Regarding AeroLink Logistics, ITIL will assist in improving incident management, reducing service disruptions, and managing changes in cloud logistics services. Hence, ITIL should act as a supplement to other security frameworks.

3.5 Zero Trust Security Model

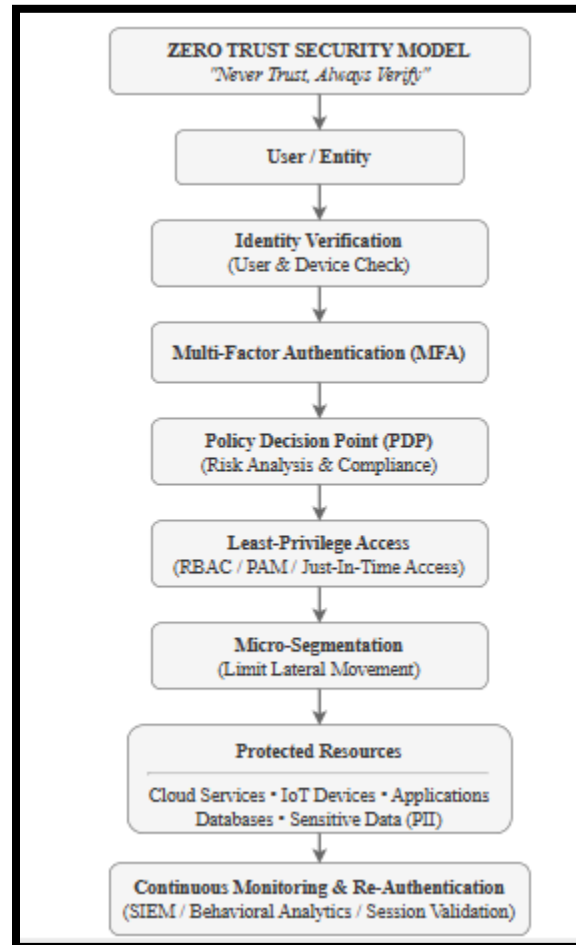


Figure 8: Zero Trust Security Model

(Source: Self-developed)

Zero Trust Security Model is becoming increasingly important for businesses where there are remote employees and cloud computing [27]. Zero Trust framework works on the principle of “never trust, always verify” and requires continuous authentication, least privilege access, identity verification, and micro-segmentation before giving access to the resources of an organization [10]. Unlike the perimeter-based security framework, Zero Trust knows that threats can come not only from the external environment but also from within [30]. Even though zero trust architecture requires investments in Identity and Access Management systems, it reduces the risks of any unauthorized access and lateral movements. Taking into account that ALL will

be using unmanaged remote devices and third-party access, the Zero Trust framework would be a safe architectural choice for ALL.

3.6 Shared Responsibility Model (Cloud)

Since AeroLink Logistics has its IT resources managed externally in terms of IaaS and SaaS, knowledge of the Shared Responsibility Model becomes vital. In essence, the cloud service provider has the responsibility of securing the cloud environment infrastructure, which includes physical locations, network, and hardware [23]. In addition, the customer is responsible for securing the applications, identities of users, data, access management, and regulatory compliance. Also, a lack of knowledge of responsibilities often leads to cloud misconfiguration and data leaks [49]. It means that ALL has to define SLAs, perform vendor risk assessments, and maintain security monitoring practices.

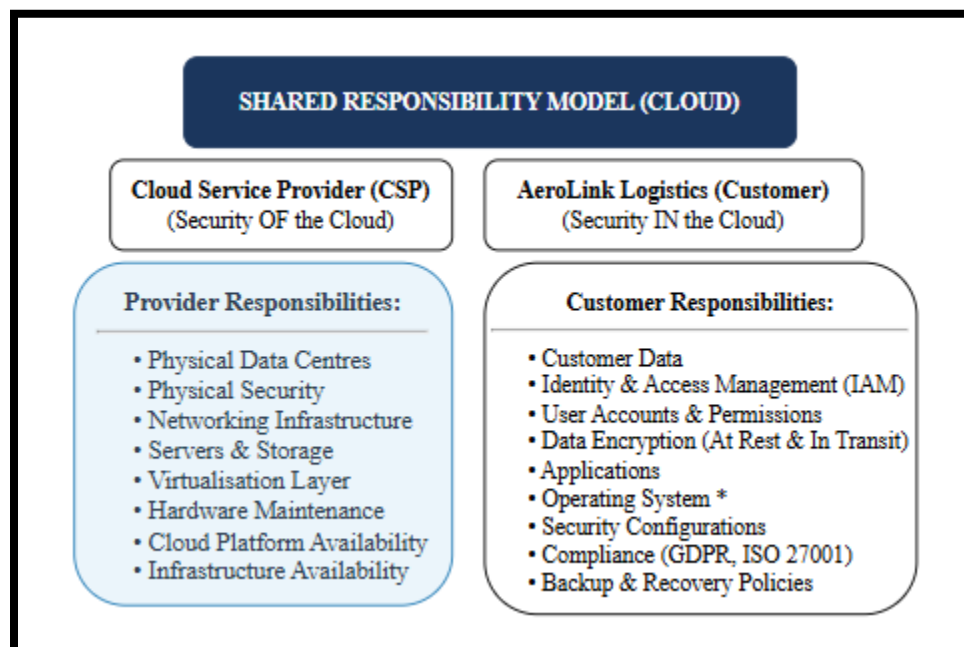


Figure 9: Shared Responsibility Model (Cloud)

(Source: Self-developed)

3.7 Comparative Evaluation

The mentioned frameworks target the unique needs of the organisations. The NIST CSF offers comprehensive risk management for cybersecurity. ISO/IEC 27001 is a framework for governance and certification of compliance, whereas COBIT adds to governance and executive oversight [8]. ITIL improves service management, whereas Zero Trust offers security for the distributed digital environment [14]. Finally, the Shared Responsibility Model is focused on cloud security governance. Therefore, all these frameworks are supplementary and not competing.

Framework	Governance	Compliance	Cloud Security	Risk Management	Vendor Management	Suitability for ALL
NIST CSF 2.0	High	Medium	High	High	Medium	Excellent
ISO/IEC 27001	High	High	High	High	Medium	Excellent
COBIT 2019	Excellent	High	Medium	High	High	Excellent
ITIL 4	Medium	Medium	Medium	Low	Medium	Good
Zero Trust	Low	Medium	Excellent	High	High	Excellent

Table 2: Comparative Evaluation

(Source: Self-developed)

More importantly, none of the models alone is able to provide the comprehensive approach needed to deal with the highly intricate security environment within which AeroLink Logistics operates. This includes the use of cloud computing technology, remote work, IoT devices, AI,

outsourcing, and strict regulatory requirements. NIST performs well in cybersecurity operations, ISO/IEC 27001 offers a good governance and compliance framework, and COBIT boosts enterprise governance. Similarly, ITIL improves service operations, while Zero Trust brings improvements in access management. Thus, a security governance framework that integrates all these complementary models is the best solution.

4. Proposed Integrated Security Governance Framework for AeroLink Logistics

4.1 Proposed Integrated Security Governance Model

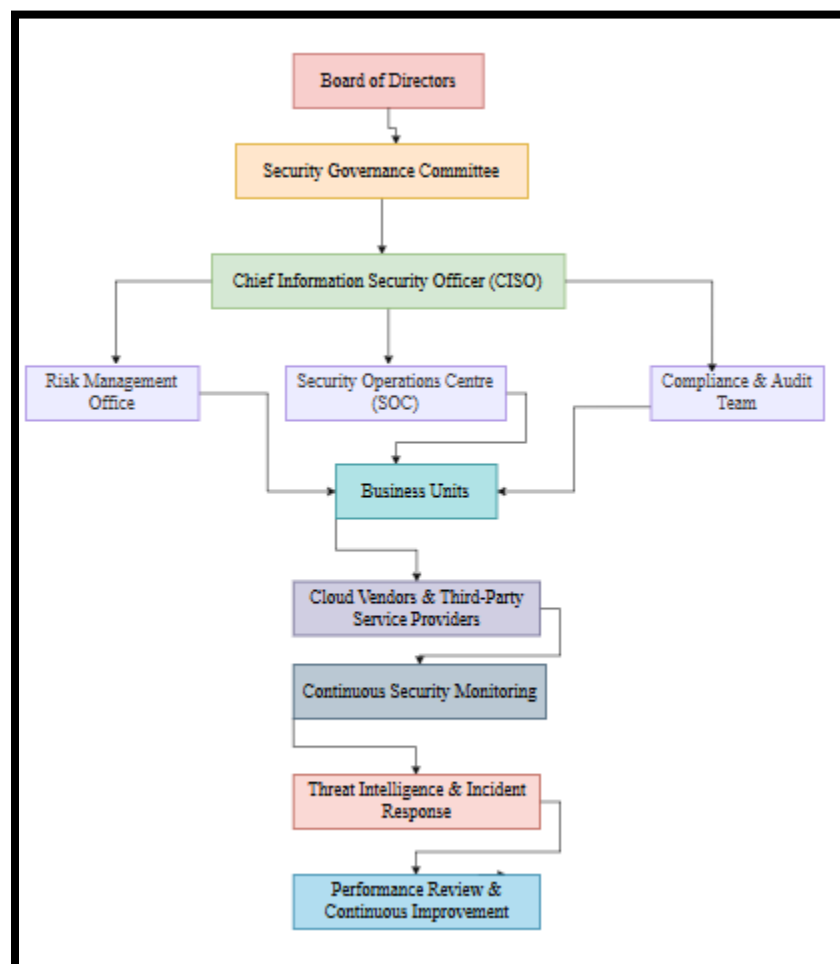


Figure 10: Integrated Security Governance Framework

(Source: Self-developed)

The Integrated Security Governance Framework proposes a governance framework that integrates the governance principles of ISO/IEC 27001, NIST Cybersecurity Framework (CSF 2.0), COBIT 2019 and ITIL 4 into one model for AeroLink Logistics (ALL).

Oversight responsibilities rest with the Board and Security Governance Committee. Chief Information Security Officer (CISO) helps to secure wider enterprise compliance [29] . Compliance Team, Business Units and Cloud Vendors are responsible in the Risk Management Office, Security Operations Centre (SOC) to get operational tasks. Across the IT environment of organisations, it helps to detect any threat and regulatory compliance to gain real-time visibility [15]. By continuous monitoring, constant improvement and organisational resilience are supported against the cyber threats.

4.2 Governance Structure

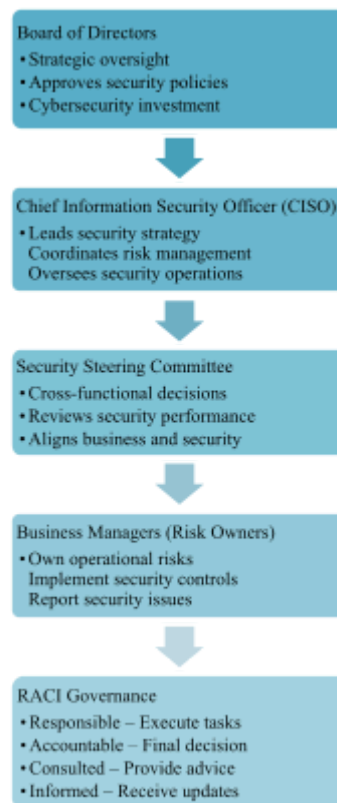


Figure 11: Organisation Structure

(Source: Self-developed)

Accountability is ensured by the organizational setup which helps to gain information security throughout AeroLink Logistics (ALL). The Board of Directors supervises the investments made in cybersecurity [34]. Approves all the security policies in place. A CISO translates strategic objectives into the operational security programme, and coordinates the risk management activities in an organisation. A committee helps in decision-making on behalf of the entire organization across functions [32]. Relevant business managers take on risk ownership using a RACI (Responsible, Accountable, Consulted and Informed) model to clarify roles and responsibilities, which improves governance transparency, supports regulatory compliance and strengthens organisational accountability *[refers to Appendix-A]*.

4.3 Risk Management Framework

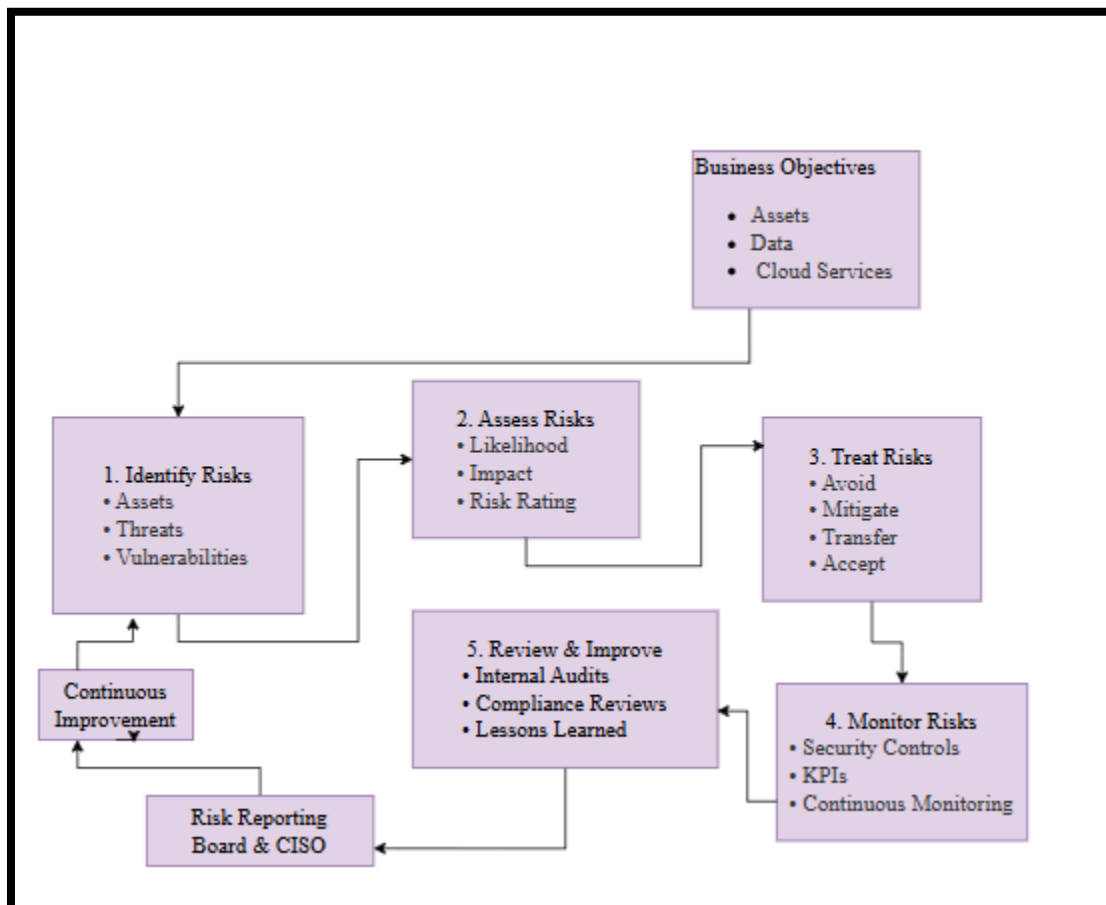


Figure 12: Integrated Risk Management Cycle for AeroLink Logistics

(Source: Self-developed)

AeroLink Logistics should set up a structured Risk Management Framework as per ISO 31000 and based on the NIST Risk Management Framework (RMF) for systematic identification, assessment and mitigation of cyber risks. ISO 31000 presents principles for governance of risk with the enterprise [39]. The NIST RMF has structured guidance as it is implementing security controls and managing risk [19]. The framework starts by identifying the assets, threats and vulnerabilities within the organisation, followed by the risk assessment of the likelihood and impact. After this, including necessary treatment measures to reduce risks. Ongoing monitoring and periodic assessment of the framework ensures compliance with prevailing laws and adaptability to the dynamic business [35].

4.4 Security Policies

Policy	Purpose	Owner	Review Frequency
Acceptable Use	System usage rules	IT Manager	Annual
Password Policy	Strong passwords & MFA	CISO	6 Months
Remote Working	Secure remote access	IT Security	Annual
BYOD	Secure personal devices	IT Security	Annual
Cloud Security	Protect cloud services	Cloud Manager	6 Months
Data Classification	Classify sensitive data	Data Owner	Annual
Incident Response	Manage security incidents	SOC Manager	Quarterly

Encryption	Protect data at rest & transit	CISO	Annual
------------	--------------------------------	------	--------

Table 3: Security Policies

(Source: Self-developed)

AeroLink Logistics (ALL) should develop effective security policies to protect the organisation's information assets and comply with regulations. An Acceptable Use Policy should describe what an acceptable use of organisational systems and devices looks like. A strong password and the use of multi-factor authentication (MFA) are defined through a Password Policy [37]. From unmanaged devices, Bring Your Own Device policies and remote working initiatives can help to ensure security access throughout the endpoint protection and Zero Trust principles [50]. Policies on cloud security and data classification should protect the cloud's data and sensitive data. Policies on Incident Response and Encryption will ensure speedy management of incidents and maintain confidentiality, integrity and availability of data across the organisation [44].

4.5 Protection Mechanisms

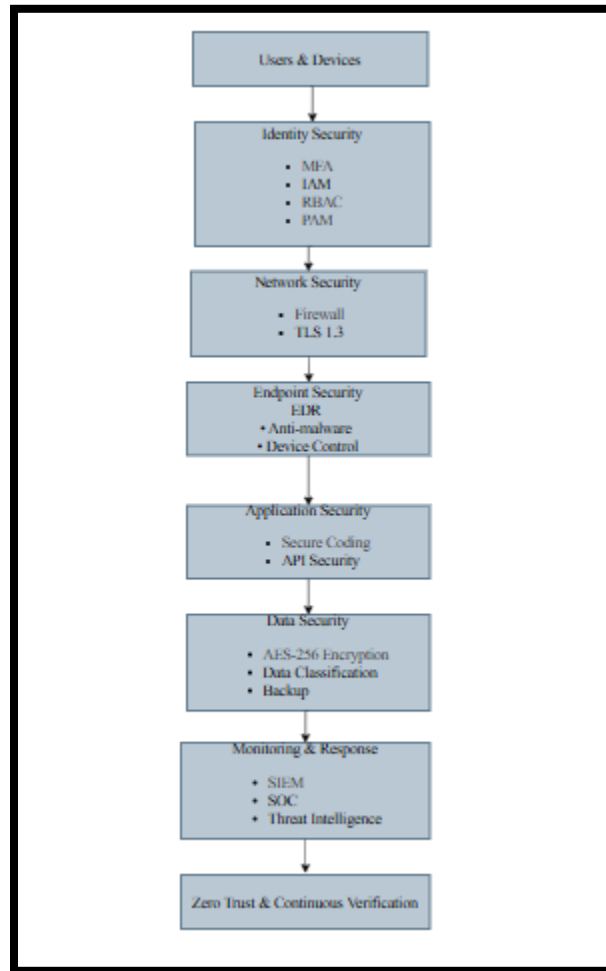


Figure 13: Layered Defence (Defence in Depth) Model for AeroLink Logistics

(Source: Self-developed)

To reduce the cyber risk to AeroLink Logistics (ALL), the company has to implement a layered defence strategy based on Defence in Depth principle [18]. Strengthen identity security and restrict unauthorized access using Multi-Factor Authentication (MFA), Identity and Access Management (IAM), Role-Based Access Control (RBAC) and Privileged Access Management (PAM). Sensitive data should implement AES-256 encryption on data at rest and TLS 1.3 on data in transit [11]. Endpoint Detection and Response (EDR) systems, Security Information and Event Management (SIEM) systems and a Security Operations Centre (SOC) should ensure continuous threat monitoring while a Zero Trust architecture ensures that no one is trusted by default [53].

4.6 Vendor Governance

Evaluation Criteria	Key Requirements
Risk Assessment	• Identify security risks • Risk rating
ISO Certification	• ISO/IEC 27001 certified • Compliance evidence
Third-party Audit	• Independent audit • Annual review
SLA Compliance	• Security targets • Incident response time
KPIs	• Availability • Patching • Performance
Security Controls	• MFA • Encryption • Access control
Penalties	• SLA breach

	• Financial penalties
Continuous Monitoring	• Performance review • Security monitoring

Table 4: Vendor Evaluation Matrix

(Source: Self-developed)

Essentially, vendor governance is required because AeroLink Logistics (ALL) outsources about 88 per cent of its IT infrastructure. Before onboarding, a comprehensive vendor governance program should include risk assessments, regular security audits and compliance with different standards, such as ISO/IEC 27001 [22]. SLAs is helping in security responsibilities, incident reporting timelines and performance expectations [1]. To gain non-compliance and security breaches, the vendor performance should be monitored through key Performance Indicators (KPIs) and penalties *[refer to Appendix B]*. To keep pace with the latest security standards, mitigate supply chain risks, vendors are continuously monitored and routinely evaluated for supporting regulatory compliance across the service lifecycle [4].

4.7 Compliance Framework

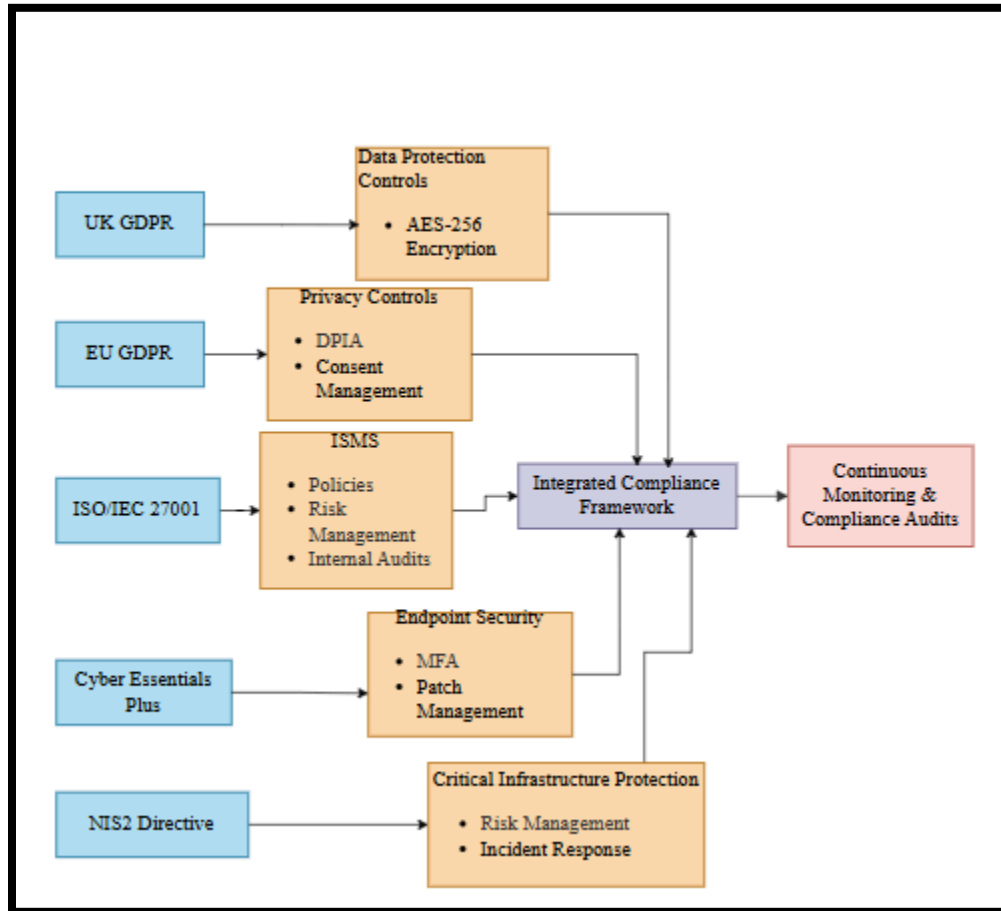


Figure 14: Integrated Compliance Framework

(Source: Self-developed)

It is proposed that AeroLink Logistics (ALL) adopt a compliance framework that matches security controls with applicable legal and regulatory requirements. Failing to comply with a large number of rules and regulations can lead to serious consequences [25]. Being up to date with all the requirements is a must. The impact of legislation on organisations ensures compliance by conducting compliance audits, monitoring policies and procedures, reviewing legislation on a regular basis [13].

4.8 Incident Response

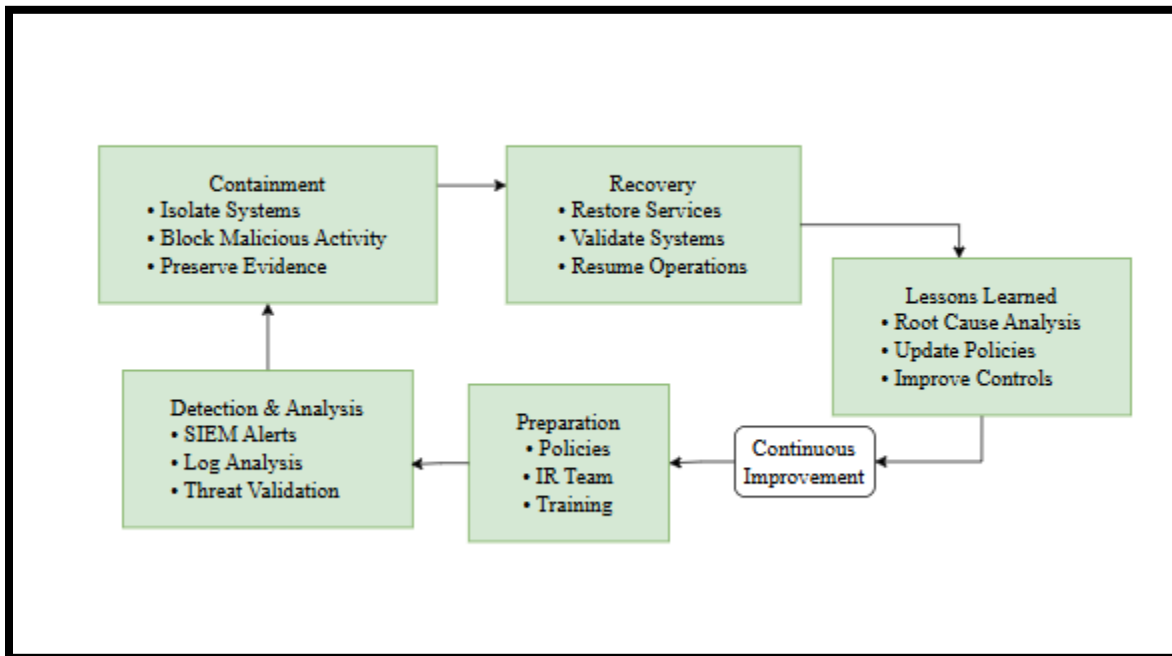


Figure 15: NIST Incident Response Process

(Source: Self-developed)

The NIST Incident Response Framework should be followed by AeroLink Logistics (ALL) which ensures a good response to cyber incidents. The Preparation process involves developing policies, response teams and communication plans [12]. Security tools such as SIEM and EDR help in detection by identifying and analysing potential threats. Devices are isolated to prevent further damage which highlights the reduction that ensures any affected systems [47]. Reviewing the incident by updating security controls highlights the Lessons Learned process helps to reduce cyber threats by improving response procedures.

4.9 Business Continuity

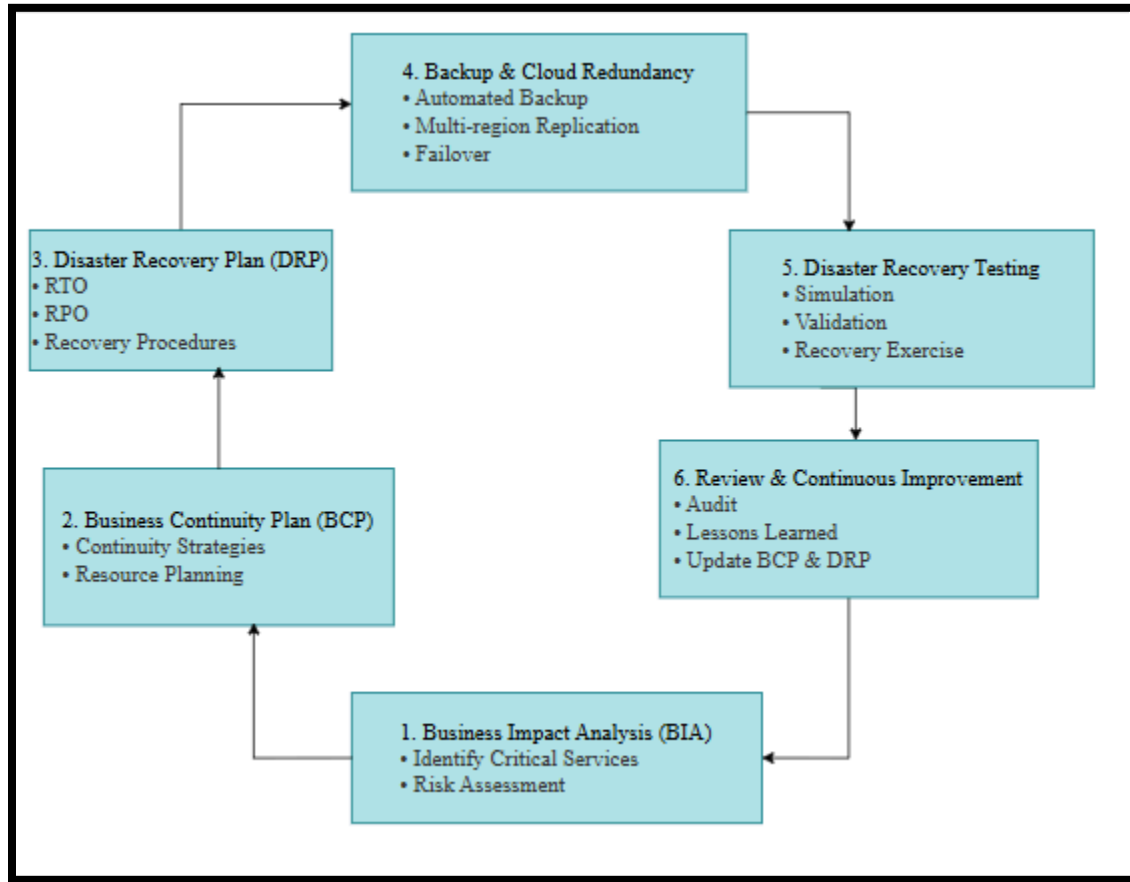


Figure 16: Business Continuity Cycle

(Source: Self-developed)

To gain across the competitive market with the key logistics operations,

AeroLink Logistics (ALL) needs to build a reliable business continuity plan (BCP) and disaster recovery plan (DRP) during a cyber-attack [6]. The BCP must allow essential functions as the DRP is going to ensure the restoration of the IT systems and data. Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) help to minimize disruption and the rate of data loss [20]. The organisational resilience after disruptive events highlight the data back-ups across the cloud redundancy spread over regions which highlight the scheduled disaster recovery testing must reinforce to ensure the quick restoration services [21].

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

ALL requires continuous updates to cybersecurity regulations in combination with the standards because its utilisations of the cloud computing, AI, IoT and ultimately the third-party services continuously change its cyber-risk exposure. Besides that, the company needs to update several things which includes security policies, compliance requirements as well as the controls to address the emerging threats while preventing the regulatory gaps. This can be achieved through the help of the periodic risk assessments, compliance audits, regulatory reviews and employee training, ensuring ALL remains resilient, compliant and responsive to evolving cybersecurity risks.

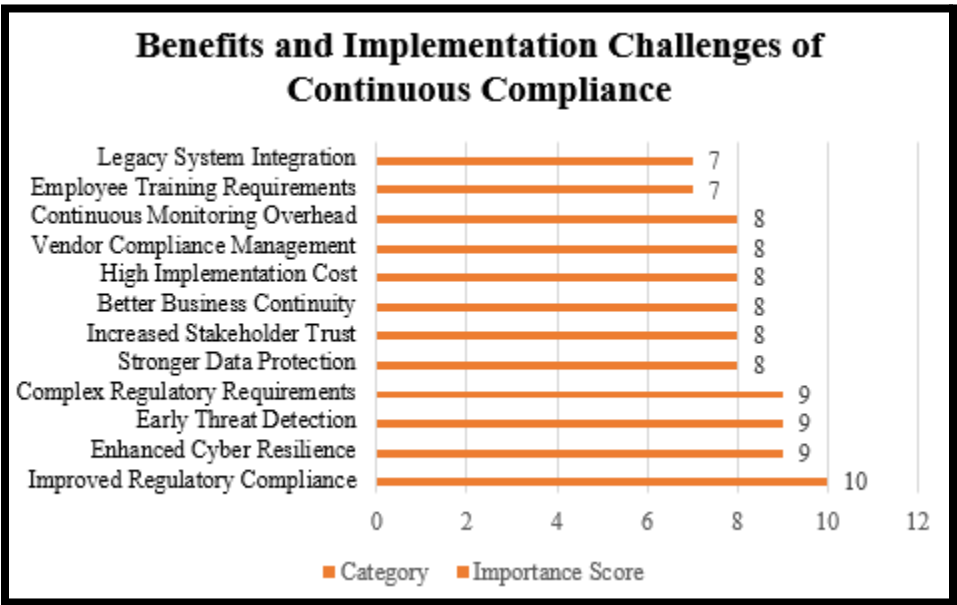


Figure 17: Benefits and Implementation Challenges of Continuous Compliance

(Source: Self-developed)

To provide necessitating continuous updates, digital technologies have disrupted the cybersecurity landscape by regulations and security standards within organizations with

requirements [51]. The airport may bounce back quicker by drawing more strength and staying connected with the global supply chain [31].

The attack surface, ransomware campaigns can be reduced by the software supply chain as it is increasingly exploiting vulnerabilities with the third-party services as artificial intelligence (AI), Internet of Things (IoT) devices and cloud computing have expanded. Quantum computing endangers conventional algorithms across the organizations which start preparing for post-quantum cryptography to raise the effect [5].

The event management with regular audits offers a number of strategic benefits which helps to identify constant monitoring. The organisation from time to time by improving regulatory compliance can also strengthen the resilience of mitigating security risks [38].

Ongoing compliance is ensuring resource-intensive and frequent regulatory updates which requires investment, expertise and continuous training of employees [40]. Along with multiple third-party vendors, new compliance requirements are implemented across complex cloud environments which can lead to increased operational complexity and compliance costs [48].

6. Conclusion and Recommendations

Conclusion

The NIST Cybersecurity Framework, ISO/IEC 27001, COBIT 2019, and ITIL were investigated through report writing in accordance with Oliver Wyman's requirements. An Integrated Security Governance Framework (ISGF) integrates governance, risk management compliance and monitoring to enhance organisation resilience. Good governance and clearly defined roles, as well as proactive risk management, contribute to security maturity. Furthermore, ongoing compliance allows organizations to deal with emerging cyber and technology threats, as well as changing international regulatory requirements.

Recommendations

The implementation of an Information Security Management System that meets ISO/IEC 27001 should be a priority for AeroLink Logistics, as should taking on a Zero Trust architecture and

conducting quarterly compliance audits [38]. IBM's Cost of a Data Breach Report 2025 observes that using AI-driven security and automation to assist the detection optimise the data security [41].

Reference

1. Abhange, A., 2025. Dynamic SLA & Alert System. *Available at SSRN 6523958*. <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=6523958>
2. Aerolink Global Logistics, (2025), *Connect Your Business To A World Of Possibilities*. Available from <https://aerolinkgloballogistics.com/#:~:text=AeroLink%20Global%20Logistics%20has%20been,and%20reliable%20air%20cargo%20solutions> Accessed on 04.08.2026.
3. Aerolink, (2026), *Security & Resilience*. Available from <https://aerolink.dev/security> Accessed on 04.08.2026.
4. 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>
5. Alim, S. and Bodade, N., 2026. Quantum Computing Threats to Modern Cryptography: Readiness Assessment and Post-Quantum Security Framework. https://assets-eu.researchsquare.com/files/rs-10120845/v1_covered_6aa8f3e1-b87f-46ab-9290-bf7a0eabe283.pdf
6. Aliya, H. and Nicola, H., 2024. Enhancing Corporate Resilience: A Comprehensive Disaster Recovery Plan for Ensuring Business Continuity in the Age of IoT Security. https://www.researchgate.net/profile/Henrietta-Nicola/publication/387502238_Enhancing_Corporate_Resilience_A_Comprehensive_Disaster_Recovery_Plan_for_Ensuring_Business_Continuity_in_the_Age_of_IoT_Security/links/6771140ac1b0135465feda0c/Enhancing-Corporate-Resilience-A-Comprehensive-Disaster-Recovery-Plan-for-Ensuring-Business-Continuity-in-the-Age-of-IoT-Security.pdf

7. Al-Janabi, S., Jabbar, H. and Syms, F., 2024. Cybersecurity transformation: cyber-resilient IT project management framework. *Digital*, 4(4), pp.866-897. <https://www.mdpi.com/2673-6470/4/4/43>
8. Alrehili, A.A. and Alhazmi, O.H., 2023, September. ISO/IEC 27001 standard: Analytical and comparative overview. In *International Conference on Advances in Data-driven Computing and Intelligent Systems* (pp. 143-156). Singapore: Springer Nature Singapore. https://link.springer.com/chapter/10.1007/978-981-99-9524-0_12
9. Anand, A., (2026), *ITIL 4 Explained: Framework, Practices, and Key Change*. Available from <https://itsm.tools/itil-4-explained/> Accessed on 04.08.2026.
10. Arora, A., 2025. Analyzing Best Practices and Strategies for Encrypting Data at Rest (Stored) and Data in Transit (Transmitted) in Cloud Environments. *Available at SSRN 5268190*. <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5268190>
11. Arora, A., 2025. Zero Trust Architecture: Revolutionizing Cybersecurity for Modern Digital Environments. *Available at SSRN 5268151*. <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5268151>
12. Barcaui, A. and Monat, A., 2023. Who is better in project planning? Generative artificial intelligence or project managers?. *Project Leadership and Society*, 4, p.100101. <https://www.sciencedirect.com/science/article/pii/S2666721523000224>
13. Bolanle, M., Ikre, W. and Olabiyi, W., 2024. Adhering to regulatory requirements and industry standards. *Ladoke Akintola University of Technology*. https://www.researchgate.net/profile/Mercy-Bolanle/publication/383400510_Adhering_to_regulatory_requirements_and_industry_standards/links/66cb20c2920e05672e4e2f66/Adhering-to-regulatory-requirements-and-industry-standards.pdf
14. 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>

15. Damodaram, R., 2025. Adaptive Cloud Cybersecurity Architectures for Real-Time Threat Detection and Compliance Monitoring. *International Journal of Science, Research and Technology*, 8(6), pp.15369-15379. <http://www.ijrsrat.com/index.php/ijrsrat/article/download/147/140>
16. De Azambuja, A.J.G., Plesker, C., Schützer, K., Anderl, R., Schleich, B. and Almeida, V.R., 2023. Artificial intelligence-based cyber security in the context of industry 4.0—a survey. *Electronics*, 12(8), p.1920. <https://www.mdpi.com/2079-9292/12/8/1920>
17. DNV, (2026), *ISO 27001 vs ISO 27002: A Comparison*. Available from <https://www.dnv.com/assurance/articles/iso-27001-vs-iso-27002-the-key-differences/> Accessed on 04.08.2026.
18. Ee, S., O'Brien, J., Williams, Z., El-Dakhakhni, A., Aird, M. and Lintz, A., 2024. Adapting cybersecurity frameworks to manage frontier AI risks: A defense-in-depth approach. *arXiv preprint arXiv:2408.07933*. <https://arxiv.org/pdf/2408.07933>
19. Efe, A., 2023. A comparison of key risk management frameworks: coso-erm, nist rmf, iso 31.000, cobit. *Denetim ve Güvence Hizmetleri Dergisi*, 3(2), pp.185-205. <https://dergipark.org.tr/en/download/article-file/3120080>
20. Ejiobi, J.C., 2022. Aligning Recovery Objectives With Organizational Capabilities. <https://scholar.dsu.edu/cgi/viewcontent.cgi?article=1381&context=theses>
21. Farooq, J. and Zhu, Q., 2025. Cyber resilience in next-generation networks: Threat landscape, theoretical foundations, and design paradigms. *arXiv preprint arXiv:2512.22721*. <https://arxiv.org/pdf/2512.22721>
22. Faruq, M.O., 2024. Vendor risk management in cloud-centric architectures: A systematic review of soc 2, Fedramp, and ISO 27001 practices. *International Journal of Business and Economics Insights*, 4(1), pp.01-32. <https://ijbei-journal.org/index.php/ijbei/article/download/2/2>
23. Fernandes, D.A., Soares, L.F., Gomes, J.V., Freire, M.M. and Inácio, P.R., 2014. Security issues in cloud environments: a survey. *International journal of information security*,

13(2), pp.113-170.
<https://www.researchgate.net/profile/Salam-Ismaeel/post/Does-anyone-know-of-security-issues-in-cloud-computing/attachment/59d61de479197b807797be9c/AS%3A273824770134018%401442296320398/download/Security+issues+in+cloud+environments+a+survey.pdf>

24. Global Market Insights, (2025), *AI in Logistics and Supply Chain Market Size & Share 2025 - 2034*. Available from <https://www.gminsights.com/industry-analysis/ai-in-logistics-and-supply-chain-market>. Accessed on 04.08.2026.
25. Habbal, A., Ali, M.K. and Abuzaraida, M.A., 2024. Artificial Intelligence Trust, risk and security management (AI trism): Frameworks, applications, challenges and future research directions. *Expert Systems with Applications*, 240, p.122442. https://www.academia.edu/download/107426902/1_s2.0_S0957417423029445_main.pdf
26. 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>
27. IMB, (2026), *What is zero trust?*. Available from <https://www.ibm.com/think/topics/zero-trust> Accessed on 04.08.2026.
28. ISO, (2022), *ISO/IEC 27001:2022*. Available from <https://www.iso.org/standard/27001#:~:text=General%20information> Accessed on 04.08.2026.
29. Jones, L.A., 2023. Aligning Risk Perspectives Between the Chief Risk Officer and the Chief Information Security Officer. In *Real-World Solutions for Diversity, Strategic Change, and Organizational Development: Perspectives in Healthcare, Education, Business, and Technology* (pp. 153-172). IGI Global Scientific Publishing. https://www.academia.edu/download/124989618/Aligning_Risk_Perspectives_Between_the_Chief_Risk_Officer_and_the_Chief_Information_Security_Officer.pdf

30. Kang, H., Liu, G., Wang, Q., Meng, L. and Liu, J., 2023. Theory and application of zero trust security: A brief survey. *Entropy*, 25(12), p.1595. <https://www.mdpi.com/1099-4300/25/12/1595>
31. Kazda, A., Badanik, B. and Serrano, F., 2022. Pandemic vs. post-pandemic airport operations: hard impact, slow recovery. *Aerospace*, 9(12), p.810. <https://www.mdpi.com/2226-4310/9/12/810>
32. Kumar, S., 2024. Strategic decision making and strategic decision practices in intelligent organizations: A review. *International Journal of Business and Management Research*, 12(2), pp.31-39. https://www.academia.edu/download/116914964/ijbmr_120202.pdf
33. Lomas, E., 2020. Information governance and cybersecurity: Framework for securing and managing information effectively and ethically. *Cybersecurity for Information Professionals: Concepts and Applications*, pp.109-131. https://discovery.ucl.ac.uk/id/eprint/10072825/1/Information_governance_and_cybersecurity_elomas_Accepted2019.pdf
34. Lowry, M.R., Vance, A. and Vance, M.D., 2026. Inexpert supervision: Field evidence on boards' oversight of cybersecurity. *Management Science*, 72(2), pp.783-804. <https://pubsonline.informs.org/doi/full/10.1287/mnsc.2023.04147>
35. 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>
36. Mohammed, A., 2023. SOC Audits in Action: Best Practices for Strengthening Threat Detection and Ensuring Compliance. *Baltic Journal of Engineering and Technology*, 2(1), pp.62-69. https://www.academia.edu/download/121532980/SOC_Audits_in_Action_Best_Practices_for_Strengthening_Threat_Detection_and_Ensuring_Compliance.pdf
37. Mohammed, A.H.Y., Dziyauddin, R.A. and Latiff, L.A., 2023. Current multi-factor of authentication: Approaches, requirements, attacks and challenges. *International Journal*

of *Advanced Computer Science and Applications*, 14(1).
https://www.researchgate.net/profile/Ali-Mohammed-172/publication/367987835_Current_Multi-factor_of_Authentication_Approaches_Requirements_Attacks_and_Challenges/links/673857b968de5e5a307829c7/Current-Multi-factor-of-Authentication-Approaches-Requirements-Attacks-and-Challenges.pdf

38. Mosso, J., 2025. Information security assurance: Building justified confidence and public trust. https://blacklabel.nz/wp-content/uploads/2025/12/Assurance_Enterprise_2025.pdf
39. Musa, H.A.H., 2026. ISO 31000, REGULATORY COMPLIANCE, AND ENTERPRISE RISK MANAGEMENT EFFECTIVENESS: EVIDENCE FROM SAUDI INSURANCE COMPANIES UNDER A TRANSITIONING SUPERVISORY REGIME. https://www.researchgate.net/profile/Hamed-Mosa/publication/401374031_ISO_31000_REGULATORY_COMPLIANCE_AND_ENTERPRISE_RISK_MANAGEMENT_EFFECTIVENESS_EVIDENCE_FROM_SAUDI_INSURANCE_COMPANIES_UNDER_A_TRANSITIONING_SUPERVISORY_REGIME/links/69a3bc5743ad5e30a853ff89/ISO-31000-REGULATORY-COMPLIANCE-AND-ENTERPRISE-RISK-MANAGEMENT-EFFECTIVENESS-EVIDENCE-FROM-SAUDI-INSURANCE-COMPANIES-UNDER-A-TRANSITIONING-SUPERVISORY-REGIME.pdf
40. Mustafaa, B. and Lleshia, S., 2024. The impact of lifelong learning and investments in employee development on employee productivity and performance. *Multidisciplinary Research Journal*, pp.1-15.
<https://www.academia.edu/download/117919306/e2024175.pdf>
41. Nikunj, D., 2025. Rising threats and next-generation defenses in cybersecurity. *International Journal of Trend in Scientific Research and Development*, 9(5), pp.531-537.
<http://eprints.umsida.ac.id/16414/1/ijtsrd97555.pdf>
42. NIST, (2024), *The NIST Cybersecurity Framework (CSF) 2.0*. Available from <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> Accessed on 04.08.2026.

43. Novelvista, (2025), *ISO/IEC 27001:2022*. Available from <https://assets.novelvista.com/resources/pdf/blogs/other/Global-ISO-27001-Cost-Comparison-Report.pdf> Accessed on 04.08.2026.
44. Okusi, O., Obiakor, I.J. and Adeloye, F.C., 2025. Designing resilient data risk management protocols for regulatory compliance and cyber incident response. *International Journal of Advance Research Publication and Reviews*, 2(7), pp.45-70. https://www.researchgate.net/profile/Fadekemi-Adeloye/publication/401371186_Designing_Resilient_Data_Risk_Management_Protocols_for_Regulatory_Compliance_and_Cyber_Incident_Response/links/69a3829c003023747db2d0de/Designing-Resilient-Data-Risk-Management-Protocols-for-Regulatory-Compliance-and-Cyber-Incident-Response.pdf
45. Pham, M.T. and Nguyen, L.H., 2023. A Comparative Review of Cybersecurity Standards and Frameworks: Supporting Information Assurance in Government and Industry Systems. *Transactions on Machine Learning, Artificial Intelligence, and Advanced Intelligent Systems*, 13(8), pp.1-15. <http://monteinstitute.com/index.php/TMLAIAIS/article/download/2023-AUGUST-04/11>
46. PMI, (2012), *COBIT and project management*. Available from <https://www.pmi.org/learning/library/control-objectives-information-related-technology-6007> Accessed on 04.08.2026.
47. Pradhan, P.L., 2026. An Overview of EDR Serviceability for Security Information and Event Management (SIEM). *Journal of Information Assurance and Security*, 21(2), pp.52-88. <https://reference-global.com/download/article/10.2478/ias-2026-0004.pdf>
48. Rapolu, U.K., 2024. Developing Custom Software Solutions for Compliance in Multi-Cloud Environments. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT Yapedumenu: Indospace Publications*, 8(1), pp.1-7. https://www.academia.edu/download/125332381/15_Developing_Custom_Software_Solutions_for_Compliance_in_Multi_Cloud_Environments.pdf

49. Salih, B.M. and Mohammad, O.K.J., 2024. Cloud data leakage, security, privacy issues and challenges. *Procedia Computer Science*, 242, pp.592-601. <https://www.sciencedirect.com/science/article/pii/S1877050924018325/pdf?md5=611ff01fc5c9275fe75807a09dbb4bcf&pid=1-s2.0-S1877050924018325-main.pdf>
50. Singh, H., 2022, November. The importance of cybersecurity frameworks and constant audits for identifying gaps, meeting regulatory and compliance standards. In *Meeting Regulatory and Compliance Standards (November 10, 2022)*. <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5267862>
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. Utomo, D., Wijaya, M., Suzanna, S., Efendi, E. and Sagala, N.T.M., 2022. Leveraging COBIT 2019 to implement IT governance in SME context: A case study of higher education in campus A. *CommIT (Communication and Information Technology) Journal*, 16(2), pp.129-141. <https://www.academia.edu/download/95997912/4569.pdf>
53. Yadav, J., An Integrated Framework for Enhancing Enterprise Cybersecurity: Leveraging AI, Zero Trust Architecture, And Siem to Overcome. <https://journal.mysocialbliss.com/wp-content/uploads/2025/03/AN-INTEGRATED-FRAMEWORK-FOR-ENHANCING-ENTERPRISE-CYBERSECURITY.-1.pdf>

