



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

Module:

ACCA7028 Data Security, Governance and Compliance

MSc Cybersecurity and Digital Forensics

University of Wales Trinity Saint David

AKASH NATUBHAI LUHARIYA

STUDENT ID: 2535266

Submission: 12th August 2026

TABLE OF CONTENTS

Abstract

1. Introduction

2. Assumptions

3. Background of AeroLink Logistics

4. Research into Security Frameworks and Models

4.1 NIST Cybersecurity Framework (CSF) 2.0

4.2 ISO/IEC 27001:2022 and the 27000 Series

4.3 COBIT 2019

4.4 ITIL 4

4.5 Positioning the Frameworks

5. Proposed Security, Governance and Compliance Design for ALL

5.1 Governance and Strategic Planning

5.2 Information Security Management and Compliance

5.3 Risk Management and Operational Security

5.4 Vendor Management and Continuity of Services

5.5 Zero Trust Security and Employee Awareness

5.6 Integration and Critical Evaluation of the Proposed Framework

6. Critical Discussion: The Importance of Maintaining Continuous Updates to Regulations and Security Standards

7. Conclusion

References

ABSTRACT

While the adoption of cloud computing, Artificial Intelligence (AI) and Internet of Things (IoT) technologies have improved the efficiency of logistics activities, it also presents several cybersecurity and compliance risks. This report analyses the problems that ALL encounters in terms of cybersecurity, which include data breach and poor governance. This report will also evaluate four well-known cybersecurity frameworks, including the NIST Cybersecurity Framework (CSF) 2.0, ISO/IEC 27001:2022, COBIT 2019, and ITIL 4. Considering these frameworks, a hybrid Security Governance Framework will be recommended.

1. INTRODUCTION

Innovations in cloud computing, AI and IoT have had a considerable impact on the evolution of the logistics industry, resulting in increasing operational efficiency, real-time tracking and decision making based on available information. Unfortunately, the development of digitalized processes and interconnection of computer systems makes organizations more vulnerable to cybersecurity risks such as data breach, ransomware attacks, unauthorized access to data and many others (NIST, 2024; ENISA, 2024). Information security governance is crucial nowadays when companies heavily rely on cloud service providers and telecommuting systems.

AeroLink Logistics (ALL) is an example of a multinational company facing these issues because of the heavy use of cloud IaaS, SaaS, IoT tracking devices and AI analytics. There were multiple data breaches at ALL concerning clients' data and lack of any security governance framework, risk management and implementation of security regulations such as ISO/IEC 27001 and GDPR.

This report aims to analyse four internationally recognized security governance frameworks (NIST Cybersecurity Framework 2.0, ISO/IEC 27001:2022, COBIT 2019 and ITIL 4) and propose a combined Security Governance Framework for ALL. In addition, the importance of updates of regulations and standards will be discussed (ISO, 2022; ISACA, 2019).

2. ASSUMPTIONS

The recommendations included in the current report rely on a set of assumptions about AeroLink Logistics (ALL) to make sure that the proposed security governance framework is pragmatic and matches the conditions described in the case scenario. Considering that there are only a few organisational details provided in the scenario, the assumptions serve as the basis for the analysis and further formulation of the strategies related to security, governance and compliance.

First, it is assumed that ALL is a large multinational company, having enough financial and human capital to adopt internationally recognised security frameworks such as ISO/IEC 27001, NIST CSF 2.0, COBIT 2019 and ITIL 4. The second assumption is that the company is going to continue using cloud-based Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), IoT-enabled tracking and AI-powered analytics as the main elements of its operations. Thus, the suggested security controls are aimed at providing protection for the cloud-based and digitally connected environment (NIST, 2024; Cloud Security Alliance, 2024).

The assumption is also made that ALL the processes involving PII of customers in various countries need to be considered and hence will have to follow international laws such as GDPR along with recognized standards of information security like ISO/IEC 27001:2022 (ISO, 2022). Lastly, it is also assumed that there will be willingness on the part of the management to improve on the cybersecurity governance, and they will support continuous risk assessments, security awareness among employees, vendor management and compliance audits.

3. BACKGROUND OF AEROLINK LOGISTICS

ALL is a multinational supply chain and logistics company providing real-time shipment tracking and warehousing and distribution solutions to its customers worldwide. To increase operational efficiency and customer satisfaction, ALL has implemented cloud computing, Internet of Things (IoT) sensors, and AI-based analytics into its operations. About 88% of ALL's IT environment consists of Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS) providers. As a result, the organisation can operate in a flexible and scalable manner. However, such high level of dependency on cloud services poses serious security risks associated with cloud misconfigurations, supply chain attacks, and other third-party security risks (Cloud Security Alliance, 2024; NIST, 2024).

There are several major information security issues faced by ALL, according to the provided case scenario. First, employees, suppliers, and partners of the organisation use remote access to its systems from multiple geographically distributed locations using unmanaged devices, which expands the attack surface of the organisation and increases the likelihood of unauthorised access to sensitive corporate assets. Moreover, there have been many data breaches at ALL, which involve thefts of customer Personally Identifiable Information (PII) and shipment data. It means that the company lacks strong identity and access management, proper encryption, and cybersecurity monitoring. Additionally, the company does not have any coherent security governance framework, proper risk management procedures, and regular compliance assessment against international standards such as ISO/IEC 27001 and GDPR (ISO, 2022; ENISA, 2024).

4. RESEARCH INTO SECURITY FRAMEWORKS AND MODELS

Rapidly growing use of cloud computing technology, Artificial Intelligence (AI), Internet of Things (IoT) technologies and remote work have radically changed business operations. Although the use of such technology leads to increased efficiency and innovation, it also raises security threats by increasing an organisation's attack surface and causing regulatory and governance complications. Consequently, more companies adopt internationally recognised security frameworks that enable efficient governance, management of cyber risks, regulatory compliance and organisational resilience (NIST, 2024; ENISA, 2024). The following section will review four internationally recognised security frameworks: NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 and ITIL 4 in relation to AeroLink Logistics (ALL).

4.1 NIST Cybersecurity Framework (CSF) 2.0

The NIST Cybersecurity Framework (CSF) 2.0 is a widely recognized risk-based framework that assists organisations in identifying, assessing, and managing cybersecurity risks. It incorporates six core functions Govern, Identify, Protect, Detect, Respond, and Recover – offering organisations a comprehensive approach for cybersecurity management (NIST, 2024). Unlike prescriptive standards, NIST CSF is adaptable and can be applied to organisations of different scales and industries.

Figure 1: NIST Cybersecurity Framework (CSF) 2.0 Core Functions

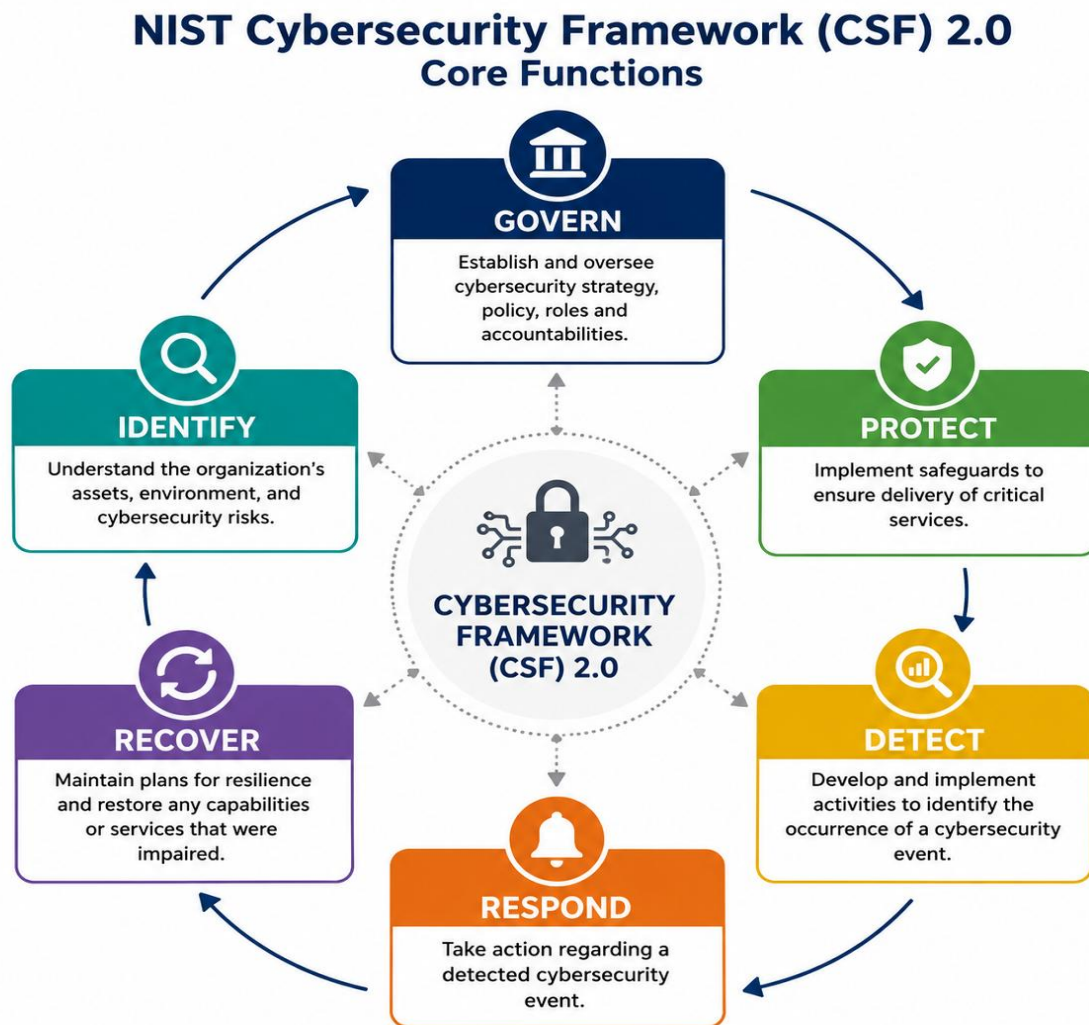


Figure 1. *NIST Cybersecurity Framework (CSF) 2.0 Core Functions* (Adapted from NIST, 2024).

The CSF is highly relevant to AeroLink Logistics as it caters to the needs of cloud security, Internet-of-Things (IoT) ecosystems and third-party risk management. The Govern function defines governance of cybersecurity practices and assigns responsibilities for them. In addition, the Protect and Detect functions improve access control, encryption and continuous monitoring of IT security. Besides, the Respond and Recover functions allow organisations to mitigate the consequences of cyber incidents by means of proper incident response and disaster recovery procedures. Nevertheless, even though the framework is comprehensive, it cannot be certified, implying that organisations should design their own implementation procedures (McIntosh et al., 2024).

4.2 ISO/IEC 27001:2022

The ISO/IEC 27001:2022 standard establishes the international framework for Information Security Management Systems (ISMS). It offers a comprehensive methodology to establish, implement, maintain, and continually improve information security using a risk-based

approach (ISO, 2022). It obligates organisations to identify information assets, evaluate security risks, and apply adequate controls based on documented policies and regular audits.

One of the major advantages of ISO/IEC 27001 is the internationally recognised certification that confirms the organisation's readiness to secure information assets and comply with regulatory requirements. For AeroLink Logistics, the framework can help to systematically improve its governance and protect its customer personally identifiable information (PII), which is important from the standpoint of GDPR compliance. Moreover, its continual improvement model allows responding to changing cyber threats adequately. However, the implementation of the framework may be resource-intensive due to its extensive documentation, regular internal audit, and continual management involvement. Thus, it is usually used in combination with other frameworks to pursue governance goals (Kitsios, Chatzidimitriou and Kamariotou, 2023).

4.3 COBIT 2019

The framework COBIT 2019 designed by ISACA pays attention to enterprise governance of information and technology, not operational cybersecurity controls. This framework connects IT activities with the strategic needs of a business via governance principles, performance measurement and accountability (ISACA, 2019). In this way, it allows for managing IT strategically and controlling risks effectively.

Regarding AeroLink Logistics, the implementation of COBIT 2019 will allow overcoming organizational weaknesses in terms of governance highlighted in the case study, which involve unclear security responsibilities and fragmented decision-making. With COBIT 2019, organizations can build up appropriate governance structure and consider cybersecurity when developing business strategy. Yet, COBIT does not give recommendations regarding technical aspects of implementing cybersecurity controls. That is why scholars suggest combining COBIT 2019 with other frameworks, such as NIST CSF and ISO/IEC 27001 (Almarzooqi and Alshamsi, 2023).

4.4 ITIL 4

Information Technology Infrastructure Library (ITIL) 4 is an internationally accepted framework for IT Service Management (ITSM). Contrary to the NIST CSF and ISO/IEC 27001, ITIL is geared towards ensuring dependable, efficient and constantly improving IT services through incident management, change enablement, problem management, and service continuity practices (AXELOS, 2019).

ITIL 4 assists AeroLink Logistics in improving the reliability of cloud-based logistics systems by increasing service availability and minimizing downtimes in cases of cyber-attacks. The framework also improves supplier management which makes it useful for organizations that depend largely on cloud-based service providers. Its continual improvement approach helps organizations evaluate service delivery and learn from cyber incidents. However, ITIL 4 was not developed to be a cybersecurity framework; hence it does not have technical controls against cyber threats. Rather, the framework works best in conjunction with cybersecurity and governance frameworks (AXELOS, 2019).

4.5 Positioning the Frameworks

Though all the frameworks mentioned above play a role in information security, they have different purposes and ways to implement them. The NIST CSF is concentrated on operations and cybersecurity, ISO/IEC 27001 represents certifiable Information Security Management System, COBIT 2019 improves strategic governance and responsibility of executives, and finally, ITIL 4 facilitates service management and operational continuity. It is evident that there is no framework that covers all aspects of governance, compliance, operations and service management concerning cybersecurity. Therefore, companies use a combination of several frameworks to get cybersecurity governance comprehensively (McIntosh et al., 2024).

The suggested combination for AeroLink Logistics would be a combination of all four frameworks mentioned above, namely COBIT 2019, ISO/IEC 27001, NIST CSF, and ITIL 4, which will ensure the necessary governance and security management, compliance, cybersecurity operations, and service management.

Table 1: Comparison of Security Frameworks

Framework	Primary Focus	Strengths	Limitations
NIST CSF 2.0	Cybersecurity risk management	Flexible, risk-based approach, incident response, resilience	No formal certification
ISO/IEC 27001:2022	Information Security Management System (ISMS)	International certification, governance, compliance	Resource-intensive implementation
COBIT 2019	Enterprise IT governance	Strategic alignment, accountability, performance measurement	Limited operational security guidance
ITIL 4	IT service management	Incident management, continual improvement, service continuity	Limited cybersecurity controls

5. PROPOSED SECURITY GOVERNANCE FRAMEWORK FOR AEROLINK LOGISTICS

As it was seen from the literature review, a single security framework cannot fully cover all aspects of the governance and operational security issues faced by AeroLink Logistics (ALL). The firm operates in an increasingly digitized environment, which includes cloud computing, Internet of Things (IoT) technologies, artificial intelligence (AI), third party outsourcing and remote working. That is why a hybrid Security Governance Framework will be proposed through the integration of the best features of COBIT 2019, ISO/IEC 27001:2022, NIST CSF 2.0 and ITIL 4 frameworks.

Figure 2: Proposed Integrated Security Governance Framework

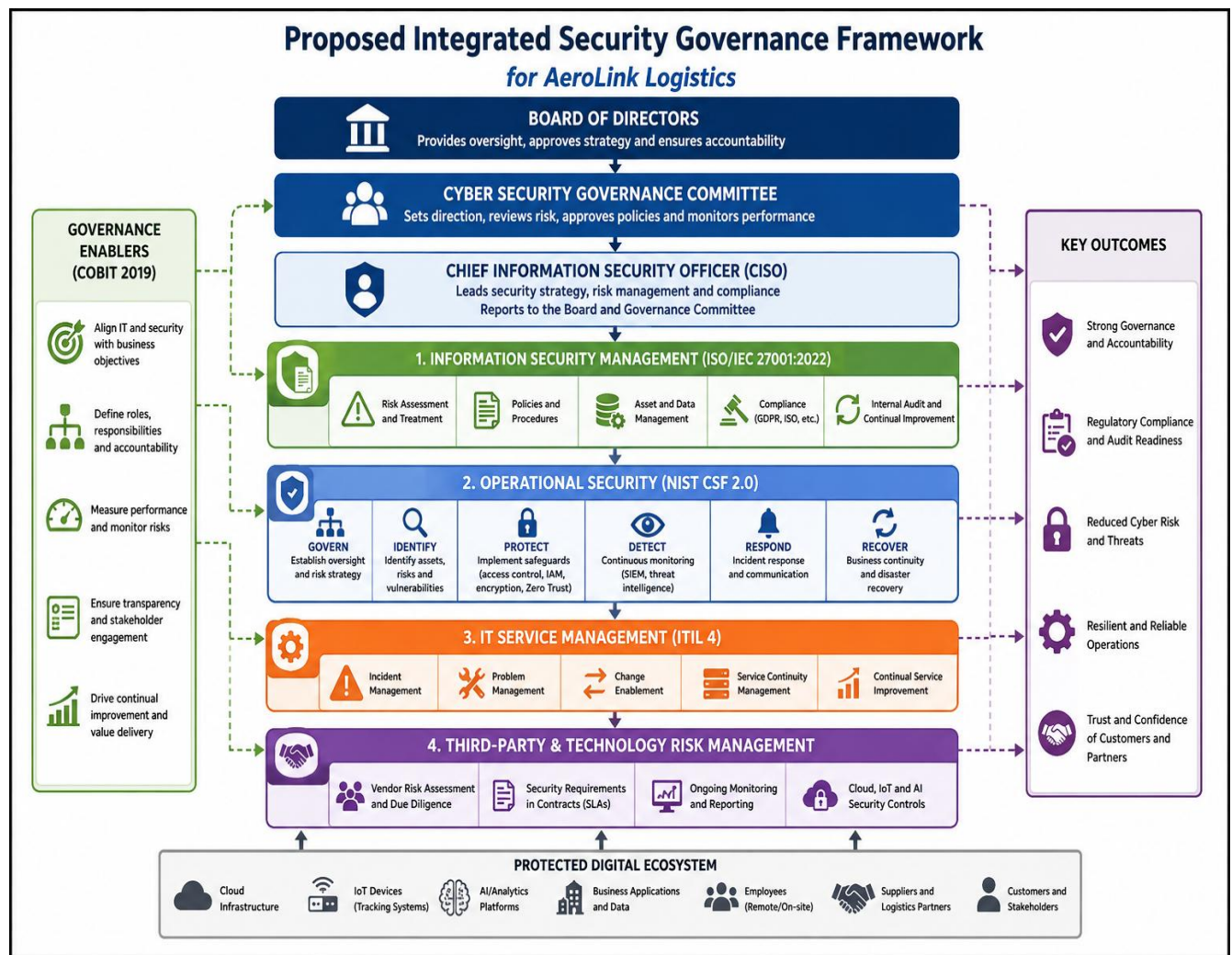


Figure 2. Proposed Hybrid Security Governance Framework for AeroLink Logistics (Adapted from ISACA, 2019; ISO, 2022; NIST, 2024 and AXELOS, 2019).

5.1 Governance and Strategic Leadership

According to the proposed structure, governance is the top-most aspect since cybersecurity requires strategic leadership instead of technology-based measures only. According to the COBIT 2019 framework, ALL needs to form a Cyber Security Governance Committee, which will determine cybersecurity goals, monitor cyber risk, and ensure that information security is consistent with the organization's strategy (ISACA, 2019). A Chief Information Security Officer (CISO) should oversee cybersecurity efforts and report directly to senior management. Governance aspects can be further enhanced with a RACI matrix.

5.2 Information Security Management and Compliance

The second layer of the model is based on ISO/IEC 27001:2022 standards that give a systematic approach to Information Security Management System (ISMS). ALL must have policies on security in areas such as data classification, acceptable use, password management, encryption, remote access and incident handling. Risk assessments will help identify any vulnerabilities in cloud platforms, AI and Internet of Things. Internal audit will ensure compliance with the ISO/IEC 27001 and GDPR standards (ISO, 2022). The

introduction of the ISMS system will help the organization continually improve by reviewing and taking corrective actions.

5.3 Risk Management and Operational Security

The operational cybersecurity strategy must be employed with the use of six functions in NIST Cybersecurity Framework (CSF) 2.0 (NIST, 2024): Govern, Identify, Protect, Detect, Respond, and Recover. ALL should identify the critical assets, such as cloud infrastructure, customer databases, and tracking devices. The protection functions should be based on Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), encryption of sensitive information and network segmentation. Continuous monitoring via SIEM systems will allow to detect any suspicious activity quickly. The incident response strategy needs to outline the roles and responsibilities during cybersecurity attacks.

5.4 Vendor Management and Continuity of Services

Since 88% of ALL's IT infrastructure is outsourced, vendor management becomes an important issue. All cloud providers and technology partners must undergo security assessment before the approval of the contract and be subject to recognized standards such as ISO/IEC 27001 (Cloud Security Alliance, 2024). Service Level Agreements (SLAs) must specify security responsibilities, requirements for incident reporting, encryption standards and auditing.

The ITIL 4 framework supports this strategy by enhancing service management with structured incident management, problem management, change enablement and continual service improvement (AXELOS, 2019). Regular testing of BCP and DRP will ensure that vital logistics services can operate in case of cyber incidents and minimize disruption.

5.5 Zero Trust Security and Employee Awareness

As employees, suppliers, and logistics partners work in a remote environment accessing organisational systems from unmanaged devices, the proposed solution follows a Zero Trust Architecture (ZTA) following the principle of “Never Trust, Always Verify” (NIST, 2024). Every access must be continuously authenticated and authorised irrespective of the location or type of devices that employees use to access the system. IAM should have multi-factor authentication, least privilege and privileged account management.

Technical controls will be ineffective without employee awareness of cybersecurity issues. Therefore, ALL must provide mandatory training for their employees to create a culture of awareness regarding cybersecurity issues. The training must include information about phishing attacks, password protection, remote working practices, and data protection.

5.6 Integration and Critical Evaluation of the Proposed Framework

The principal strength of the proposed model is the clear separation of responsibilities between the four frameworks. COBIT 2019 addresses why and who should govern cybersecurity; ISO/IEC 27001 addresses how information security should be managed systematically; NIST CSF 2.0 addresses how cyber risks should be identified, protected, detected, responded to and recovered from; and ITIL 4 addresses how secure and resilient IT services should be managed and continually improved.

This integration reduces the weaknesses associated with relying on a single framework. However, adopting four frameworks simultaneously creates a potential governance problem: duplicated controls, excessive documentation, conflicting responsibilities, and increased implementation costs. ALL should therefore avoid creating four separate compliance programmers. Instead, common controls should be mapped across the frameworks and managed through a single governance structure and integrated risk register.

Table 2: Key Components of the Proposed Security Governance Framework

Security Area	Framework / Proposed Solution	Critical Purpose	Expected Outcome
Governance	COBIT 2019, Cybersecurity Governance Committee and CISO	Establish accountability and align cybersecurity with business objectives	Stronger strategic oversight and decision making
Information Security	ISO/IEC 27001:2022 ISMS	Establish systematic risk management and continual improvement	Consistent security management and assurance
Cyber Risk	NIST CSF 2.0	Identify, protect, detect, respond, and recover from cyber risks	Improved operational risk management
Identity and Access	Zero Trust, MFA, RBAC and privileged access management	Apply continuous verification and least privilege	Reduced unauthorized access and lateral movement
Third-Party Security	Supplier assessments, contractual controls, and SLA monitoring	Control risks introduced by outsourced services	Improved supply chain security
IT Service Management	ITIL 4 incident, problem, and change management practices	Integrate security with day-to-day service operations	More controlled and resilient IT services
Business Continuity	BCP/DRP testing and recovery objectives	Maintain or restore critical logistics operations	Reduced operational disruption
Human Security	Mandatory awareness training and phishing simulations	Reduce employee related security risks	Improved security behavior and incident reporting
Assurance and Improvement	Internal audit, KPIs, KRIs and continual review	Measure whether controls remain effective	Evidence-based security improvement

In-text citations: (ISACA, 2019; ISO, 2022; NIST, 2024; AXELOS, 2019; Cloud Security Alliance, 2024; ENISA, 2024).

5. CRITICAL DISCUSSION: THE IMPORTANCE OF MAINTAINING CONTINUOUS UPDATES TO REGULATIONS AND SECURITY STANDARDS

As more companies move towards the use of cloud computing, Artificial Intelligence (AI), IoT technologies, and remote work, cybersecurity threats have changed rapidly. In turn, it becomes crucial to maintain continuously updated security regulations, governance framework, and industry standards to protect organisational resources, maintain legal compliance, and preserve customers' trust. Thus, for an outsourcing company like AeroLink Logistics (ALL) that is heavily dependent on cloud services and IoT-based logistics systems, outdated security controls might pose a serious threat of customer information theft through cyberattacks and disruptions (NIST, 2024; ENISA, 2024).

The first reason for continuously updating security standards is the appearance of new cyber threats that exploit cloud environments, supply chains, and remote access systems through such tactics as ransomware, phishing, and malware attacks. Such updates allow companies to identify weaknesses and enhance their overall cyber resilience. Implementation of new security measures such as Multi-Factor Authentication (MFA), Zero Trust Architecture, and continuous security monitoring can provide additional security to the organisation (Cloud Security Alliance, 2024).

In addition, continuous updates are necessary to maintain regulatory compliance. Companies that work internationally should comply with constantly changing legislation such as General Data Protection Regulation (GDPR) and relevant international standards such as ISO/IEC 27001:2022. Regular audits, policy reviews, and risk assessments will help the company to identify security weaknesses and process personal and business data properly. Non-compliance with GDPR or ISO standards can lead to heavy penalties and loss of customer trust (ISO, 2022).

However, such updates require financial and human investments and management commitment. Nevertheless, such updates will improve the company's resilience, reduce cyber risks and help to achieve business continuity. Therefore, AeroLink Logistics should create a culture of continuous updates by reviewing its governance framework, security controls, and compliance practices (McIntosh et al., 2024).

CONCLUSION

The growing use of cloud computing, Artificial Intelligence (AI) and Internet of Things (IoT) technologies, as well as outsourcing of digital services makes information security governance an important strategic issue for contemporary organizations. AeroLink Logistics (ALL) is a typical example which proves that poor security governance, inefficient risk management and insufficient regulation compliance may result in higher chances of having breaches, interruptions in operations and reputational losses. Consequently, a comprehensive approach to cybersecurity needs to be implemented by ALL to protect critical information resources and maintain trust (NIST, 2024; ENISA, 2024).

This report has critically analyzed four globally recognized security frameworks – NIST Cybersecurity Framework (CSF) 2.0, ISO/IEC 27001:2022, COBIT 2019 and ITIL 4 and found out that none of the frameworks alone is enough to meet all the security and governance needs of ALL. As a result, a hybrid Security Governance Framework which includes strategic governance, information security management, operational cybersecurity controls and service management was suggested (ISO, 2022; ISACA, 2019)

REFERENCES

Almarzooqi, A. and Alshamsi, A. (2023) ‘Information security governance in the banking sector: A systematic literature review’, *IEEE Access*, 11, pp. 45678–45692.

AXELOS (2019) *ITIL Foundation: ITIL 4 Edition*. London: TSO.

Cloud Security Alliance (2024) *Security Guidance for Critical Areas of Focus in Cloud Computing*. Available at: <https://cloudsecurityalliance.org> (Accessed: 3 August 2026).

ENISA (2024) *ENISA Threat Landscape 2024*. Luxembourg: European Union Agency for Cybersecurity. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> (Accessed: 3 August 2026).

European Parliament and Council (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. *Official Journal of the European Union*, L119, pp. 1–88.

IBM Security (2025) *Cost of a Data Breach Report 2025*. Armonk, NY: IBM Corporation. Available at: <https://www.ibm.com/reports/data-breach> (Accessed: 3 August 2026).

International Organization for Standardization (ISO) (2022) *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements*. Geneva: ISO.

ISACA (2019) *COBIT 2019 Framework: Governance and Management Objectives*. Schaumburg, IL: ISACA.

Kitsios, F., Chatzidimitriou, E. and Kamariotou, M. (2023) ‘The ISO/IEC 27001 information security management standard: How organisations extract value from information security management systems’, *Sustainability*, 15(7), pp. 1–24.

Lokare, A., Bankar, S. and Mhaske, P. (2025) ‘Integrating cybersecurity frameworks into IT security: A comprehensive analysis of threat mitigation strategies and adaptive technologies’, *arXiv*. Available at: <https://arxiv.org/abs/2502.00651> (Accessed: 3 August 2026).

McIntosh, T.R., Susnjak, T., Liu, T., Watters, P. and Halgamuge, M. (2024) ‘From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks and regulatory compliance in commercialising large language models’, *Computers & Security*, 145, 103998.

National Institute of Standards and Technology (NIST) (2024) *Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD: U.S. Department of Commerce. Available at: <https://www.nist.gov/cyberframework> (Accessed: 3 August 2026).

National Institute of Standards and Technology (NIST) (2024) *Special Publication 800-207A: Zero Trust Architecture*. Gaithersburg, MD: U.S. Department of Commerce.

PwC (2025) *Global Digital Trust Insights 2025*. London: PricewaterhouseCoopers. Available at: <https://www.pwc.com/gx/en/issues/cybersecurity.html> (Accessed: 3 August 2026).

Verizon (2025) *2025 Data Breach Investigations Report*. New York: Verizon. Available at: <https://www.verizon.com/business/resources/reports/dbir> (Accessed: 3 August 2026).