



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

Data Security, Governance and
Compliance at AeroLink Logistics: A
Hybrid GRC Framework for the
Outsourced Supply Chain

Name: Dipkumar Hemantkumar patel

Student Id: 2535265

Course: MSc Cybersecurity and Digital Forensics

Module: Data security, governance and Compliance

University: University of Wales, Trinity Saint David

Table of Contents

1. Abstract	3
1. Introduction	3
2. assumptions	4
3. Research into Security Frameworks and Models.....	4
3.1 ISO/IEC 27000 series	4
3.2 NIST Cybersecurity Framework 2.0	5
3.3 COBIT 2019	5
3.4 ITIL 4	5
3.5 Comparative evaluation	5
4. A Security, Governance and Compliance Design for Aero-Link Logistics.....	6
4.1 Design rationale and overview.....	6
4.2 Governance and strategic planning.....	7
4.3 Risk management and assessment	7
4.4 Security policies and procedures	8
4.5 Protection mechanisms and access controls	8
4.6 Vendor and SLA management.....	9
4.7 Contingency and business continuity planning.....	9
4.8 Compliance, law and ethics.....	9
4.9 Implementation roadmap	10
5. Why Continuous Updating of Regulations and Standards is Good Practice	10
6. Conclusion	11
7. References.....	11

Abstract

AeroLink Logistics (ALL), a global supply chain firm, has quickly embraced cloud services, IoT tracking and machine and data analytics. Its security governance, nevertheless, did not develop as quickly. The repeated leakage of shipment information and customer personally identifiable information (PII) has emerged frequently in the news. Since 2016, 88% of its infrastructure is outsourced. This exposes ALL, its customers and stakeholders to serious security, financial and regulatory risks.

In this paper, we assess the strengths, weaknesses and applicability of four widely recognised frameworks: ISO27000 series, NIST CSF 2.0, COBIT 2019 and ITIL 4, for the ALLsector's cyber resilience. We propose a hybridised approach based on our assessment to bolster the ALLsector's cyber resilience. The governance framework used is COBIT 2019. ISO/IEC 27001:2022 is used for information security management. Similarly, NIST CSF 2.0 is used for practical cybersecurity risk management. Underpinning the approach are zero-trust security, vendor management, GDPR compliance and ISO 22301 business continuity.

Instead of a common framework, the report contends that ALL requires an integrated and risk-based approach. As technology and cyber threats continue to evolve, it is also important to regularly review standards and regulations to be effective.

1. Introduction

The digital transformation has made new kinds of security threats. According to ENISA (2024), while cloud platforms, IoT devices, and AI systems boost efficiency, these systems also increase the number of systems, users, suppliers and access points to protect. According to IBM Security (2024), the global average cost of a data breach reached USD 4.88 million in 2024, with serious financial impacts. According to the European Parliament and Council (2016), the fines for serious violations, under the GDPR, can be 4% of total global annual turnover.

Thus, AeroLink Logistics (ALL) illustrates this. Approximately 88% of its IT infrastructure is outsourced while remote access from various unmanaged devices is used in numerous locations. The organization has also suffered breaches of shipping data and customer PII. At present, ALL does not possess a centralised risk management system or an auditing policy. As a result, there are weaknesses in vendor accountability, encryption, incident response and business continuity.

This report critically assesses the ISO/IEC 27000, the NIST CSF 2.0, open-source COBIT 2019, and ITIL 4 Frameworks, comparing their strengths and weaknesses against the specific requirements of ALL. From this analysis, a hybrid framework was proposed using COBIT 2019 for governance, ISO/IEC 27001:2022 for security management and NIST CSF 2.0 for operational cybersecurity risk management. Supporting measures encompass zero-trust access, vendor management, adherence to GDPR, and ISO 22301.

With upgrades to systems and security codes, and new developments to monitor, the White Paper's report calls for continuous reviews.

2. Assumptions

The following assumptions frame the analysis and design so that the recommendations can be interpreted in context:

- Scale and structure: ALL employs approximately 4,000 staff across Europe, North America and Asia-Pacific, with an internal IT function of around 120 but no dedicated security team, CISO or Data Protection Officer (DPO).
- Regulatory exposure: ALL processes personal data of EU and UK data subjects, so the EU GDPR and UK GDPR/Data Protection Act 2018 apply. It acts as a data controller for customer PII and as a processor for some client shipment data. Several major clients are themselves in scope of NIS2 or DORA and flow contractual security requirements down to logistics suppliers.
- Technology estate: core platforms (transport and warehouse management, ERP, IoT telemetry, AI analytics) run on major public cloud IaaS/SaaS providers; identity is managed through a hybrid directory service, but multi-factor authentication (MFA) is inconsistently enforced.

3. Research into Security Frameworks and Models

No single framework covers governance, management and operational control equally well; each embodies a different philosophy of how security should be organised (Loft et al., 2022). Four candidates relevant to ALL are examined below.

3.1 ISO/IEC 27000 series

The ISO/IEC 27000 series is based on ISO/IEC 27001:2022 which specifies the requirements for an Information Security Management System (ISMS): a risk-based, ongoing management system based on Plan-Do-Check-Act logic (ISO/IEC, 2022a). Its Annex A lists 93 controls across 4 themes (organisational, people, physical, technological) in detail in ISO/IEC 27002. ISO/IEC 27005 gives guidance on risk management. ISO/IEC 27017/27018 extend the controls to cloud services and PII in public clouds directly relevant to ALL's outsourced estate. Certifiability is the key element. Certification by an independent body offers reassurance to clients and regulators. Empirical work indicates that certification is associated with tangible performance benefits and not merely symbolic (Podrecca et al., 2022). However, the standard does not dictate how an organisation must achieve it.

3.2 NIST Cybersecurity Framework 2.0

The NIST CSF 2.0 is a voluntary, outcome-based framework that groups cybersecurity into six functions: Govern, Identify, Protect, Detect, Respond and Recover (NIST, 2024). The 2024 revision is important for ALL in two ways. Firstly, the new Govern function elevates risk governance, roles and policy to a first-class concern. Secondly, the expanded Cybersecurity Supply Chain Risk Management category (GV.SC) requires suppliers to be known, prioritised by criticality, and bound by contractual security requirements. This is a near-exact description of ALL's vendor problem. The CSF can be seen as a practical roadmap tool as it allows an organisation to describe its current and target postures through Implementation Tiers and Profiles.

3.3 COBIT 2019

COBIT 2019 is ISACA's framework for governance of enterprise information and technology. Its key difference between governance objectives (Evaluate, Direct, Monitor EDM) and management objectives (APO, BAI, DSS, MEA domains) directly addresses ALL's confusion on who is accountable for security (ISACA, 2018). Goals cascade translates enterprise goals down to technology and governance goals, making sure that investments in security are justified by their business value. Design factors personalize the governance system to the context. The problem with COBIT is its weight: it is a governance meta-framework, not a set of implementable security controls, and adopting it fully can be overwhelming for an organisation with low maturity at ALL.

3.4 ITIL 4

ITIL 4 is a service management framework that is based on the Service Value System and 34 practices such as information security management, supplier management, service level management, incident management and service continuity management (AXELOS, 2019). For a company that sources 88% of its IT as external services, ITIL's supplier and SLA management practices are mature, operational mechanisms to define, measure and enforce service commitments.

3.5 Comparative evaluation

Table 1: Comparative evaluation of candidate frameworks for ALL

Framework	Primary focus	Key strengths for ALL	Limitations
ISO/IEC 27001:2022	Certifiable ISMS; risk-based control baseline	Independent assurance to clients; systematic risk treatment; cloud/PII extensions (27017/27018)	Specifies what, not how; certification cost; risk of audit-driven adoption

Framework	Primary focus	Key strengths for ALL	Limitations
NIST CSF 2.0	Outcome-based cyber risk management	Free; common language; Govern function and supply-chain category (GV.SC); Tiers/Profiles support a maturity roadmap	Not certifiable; no management-system requirements
COBIT 2019	Enterprise governance of information and technology	Clarifies board accountability (EDM); goals cascade links security to business value	Heavyweight for low-maturity organisations; not control-level
ITIL 4	IT service management	Mature supplier, SLA, incident and continuity practices for an outsourced estate	Security peripheral; process overhead

The comparison shows the frameworks are complementary rather than competing: COBIT answers who governs and why, ISO/IEC 27001 answers how security is managed and evidenced, the CSF answers what outcomes operations must achieve, and ITIL disciplines the service relationships through which most of ALL's IT is actually delivered. This complementarity reinforced by the informative mappings NIST publishes between the CSF and ISO/IEC 27001 justifies the hybrid design in Section 4 rather than the wholesale adoption of any single framework.

4. A Security, Governance and Compliance Design for Aero Link Logistics

4.1 Design rationale and overview

The proposed design uses a four-layer hybrid model. COBIT 2019 provides the governance layer, defining board-level responsibility and accountability. ISO/IEC 27001:2022 forms the management layer through a certifiable Information Security Management System (ISMS), providing assurance to clients and stakeholders. NIST CSF 2.0 supports the operational layer by organising key cybersecurity activities, including protection, detection and response. The final assurance layer focuses on GDPR, client SLAs and business continuity requirements.

Table 2: Layered target architecture for ALL

Layer	Framework anchor	Purpose	Key artefacts
Govern	COBIT 2019 (EDM); CSF 2.0 Govern	Set direction, risk appetite and accountability	Security strategy; risk appetite statement; board risk dashboard
Manage	ISO/IEC 27001:2022 ISMS	Certifiable management system, policy and risk treatment	ISMS scope; Statement of Applicability; risk register; internal audit programme
Operate	CSF Protect/Detect/Respond/Recover; ISO/IEC 27002; NIST SP 800-207	Technical and procedural controls	Zero-trust access; encryption; SOC monitoring; incident response and recovery runbooks
Assure	GDPR/UK GDPR; ISO 22301; client SLAs	Legal, contractual and resilience conformance	DPIAs; records of processing; vendor assessments; BC/DR test evidence

4.2 Governance and strategic planning

The first corrective action is organisational. A Chief Information Security Officer (CISO) should be appointed, reporting to the CEO with a direct line to a newly formed Board Risk Committee, which exercises the COBIT EDM objectives: evaluating security proposals, directing strategy and monitoring performance against a small set of board-level indicators. An Information Security Steering Committee (ISSC), chaired by the CISO with representation from operations, legal, HR, procurement and regional business units, resolves the current lack of interdepartmental coordination and owns cross-functional decisions such as vendor onboarding and policy exceptions. A DPO is appointed in line with GDPR Article 37, given the scale of PII and location-tracking processing

4.3 Risk management and assessment

A single, centralised risk management process aligned to ISO/IEC 27005 replaces the current fragmented practice: establish context, identify, analyse and evaluate risks against the board-approved appetite, then treat, monitor and review on a quarterly cycle (ISO/IEC, 2022b). All risks are held in one register owned by the CISO, with named risk owners in the business. The target maturity is CSF Tier 3 (risk-informed, repeatable) within three years. Table 3 illustrates the initial assessment of ALL's most material risks.

Table 3: Extract of the initial risk register (L = likelihood, I = impact)

Risk	L	I	Rating	Primary treatment
Credential compromise via unmanaged remote devices	High	High	Critical	Zero-trust access, universal MFA, device posture checks
Breach at third-party IaaS/SaaS vendor	Medium	High	High	Vendor tiering, contractual controls, continuous assurance (4.6)
Cloud storage misconfiguration exposing PII	High	High	Critical	Hardened baselines, cloud security posture management, DLP
IoT tracking sensor tampering or spoofing	Medium	Medium	Medium	Network segmentation, device identity, signed firmware
GDPR non-compliance (no audit trail, late breach notification)	High	High	Critical	Compliance programme, DPIAs, 72-hour notification workflow (4.8)

4.4 Security policies and procedures

Policy is structured as a three-tier hierarchy. An Enterprise Information Security Policy, approved by the board, states intent, scope and accountability. Issue-specific policies operationalise it: acceptable use, access control, bring-your-own-device, data classification and handling cryptography, vendor security, secure development and incident response. System-specific standards and procedures (for example, cloud configuration baselines and IoT hardening standards) translate policy into verifiable technical settings. Every policy has an owner, a review cycle of at most twelve months, and a compliance measure, and is reinforced by role-based security awareness training critical given that the breach history is credential-driven.

4.5 Protection mechanisms and access controls

With ALL's workforce, suppliers and partners connecting from unmanaged devices and across time zones, a perimeter-based model is not practical. The design therefore implements a zero-trust architecture, where no user, device or network location is implicitly trusted and every access request is authenticated, authorised and continuously evaluated (Rose et al., 2020). Zero trust is well suited to the very cloud-heavy, boundary-less estates that ALL operates in (Syed et al., 2022). Specifically: identity is the control plane, all users require phishing-resistant MFA and conditional access policies evaluate device health prior to granting access; least privilege and privileged access management mitigate administrative accounts; the IoT sensor network is isolated from corporate IT with device-level identity; data is encrypted in transit (TLS 1.3) and at rest (AES-256) with customer-

controlled keys for the most sensitive client data; data loss prevention tracks PII egress; and a 24/7 security operations capability aggregates cloud, identity and IoT telemetry into a SIEM for detection and response.

4.6 Vendor and SLA management

With 88% of infrastructure outsourced, ALL's security is largely inherited, so vendor governance is treated as a core control rather than a procurement afterthought, in line with CSF 2.0 GV.SC (NIST, 2024) and ITIL 4 supplier management practice (AXELOS, 2019). Vendors are tiered by criticality and data sensitivity; onboarding requires due diligence evidence such as ISO/IEC 27001 certification or SOC 2 Type II reports; and contracts embed GDPR Article 28 processor terms breach notification within 24 hours, right-to-audit clauses, data residency commitments and exit/portability provisions.

4.7 Contingency and business continuity planning

Resilience is built on a business impact analysis that identifies ALL's critical services – real-time tracking, warehouse orchestration, client portals and establishes recovery time and recovery point objectives for each. A business continuity management system aligned to ISO 22301 delivers governance for continuity plans, alternative processing arrangements and supplier failover, exercised at least annually including joint tests with critical vendors (ISO, 2019). Incident response is based on the NIST incident handling lifecycle of preparation, detection and analysis, containment, eradication and recovery, and post-incident learning. The process is undertaken by a formally chartered response team with retained forensic support. They use the immutable copies in a 3-2-1 pattern to fight ransomware. The GDPR 72-hour breach notification duty is baked into the incident workflow, so legal assessment starts at detection, not post-recovery.

4.8 Compliance, law and ethics

The compliance programme operationalises the GDPR principles of lawfulness, purpose limitation, data minimisation, integrity and confidentiality and accountability (European Parliament and Council, 2016). All PII flows have records of processing activities. Data protection impact assessments are required for high-risk processing, notably the AI-led analytics and IoT location tracking, which raise ethical issues of workforce surveillance and algorithmic bias that transcend legal minima. Cross-border transfers are made pursuant to standard contractual clauses or the UK international data transfer agreement. The AI analytics portfolio is screened against the risk-based obligations of the EU AI Act to proactively build in the requirements for transparency and oversight by humans, rather than retrofit them (European Parliament and Council, 2024).

4.9 Implementation roadmap

Table 4: Three-phase implementation roadmap

Phase	Objectives	Key deliverables
0-6 months (Foundations)	Establish governance and stop the bleeding	CISO, ISSC and DPO appointed; risk appetite and register; enterprise policy; universal MFA; cloud misconfiguration remediation
6-18 months (Implementation)	Build the ISMS and modernise controls	ISO/IEC 27001 ISMS with Statement of Applicability; zero-trust rollout; vendor re-contracting and tiering; incident response and BC plans tested; awareness programme
18-36 months (Assurance)	Certify, measure, improve	ISO/IEC 27001 certification; ISO 22301 alignment; CSF Tier 3 achieved; continuous audit and board reporting cycle

5. Why Continuous Updating of Regulations and Standards is Good Practice

Standards and regulations are snapshots of consensus, while threats and technologies are moving targets. ENISA's threat landscape analysis shows sustained escalation in ransomware, supply chain compromise and AI-enabled attacks (ENISA, 2024); an organisation that freezes its compliance posture at a past version of a standard is, in effect, defending yesterday's threat model. The standards themselves demonstrate this. ISO/IEC 27001's 2022 revision restructured Annex A and introduced controls for threat intelligence, cloud service security and data loss prevention precisely because the 2013 catalogue no longer reflected practice, and certified organisations were required to transition or lose certification (ISO/IEC, 2022a). Likewise, NIST added the Govern function and expanded supply chain risk management in CSF 2.0 after a decade of breaches showed that technical controls fail without governance (NIST, 2024). For ALL, whose breach history is rooted in exactly these areas, tracking such updates is not bureaucracy it is how lessons learned across the whole economy reach an individual firm

6. Conclusion

AeroLink Logistics' difficulties are not primarily technological but organisational: capable cloud IoT and AI platforms operate without direction, accountability or assurance. This report has shown that the established frameworks each solve a different part of that problem, and has therefore proposed a layered hybrid: COBIT 2019 to give the board genuine governance of security; ISO/IEC 27001:2022 to institutionalise a certifiable, risk-based management system; NIST CSF 2.0 to structure operational outcomes and, through its supply chain category, to discipline an estate that is 88% outsourced; and GDPR-aligned compliance, zero-trust protection and ISO 22301 continuity to close the specific gaps exposed by ALL's breaches. Delivered over a three-year roadmap with explicit assumptions about budget, scale and maturity, the design converts security from a source of recurring crisis into a demonstrable business capability. Sustaining it requires the discipline argued for in Section 5: continuous, risk-prioritised alignment with evolving standards and regulation, so that ALL's security posture ages with the threat landscape rather than against it.

References

AXELOS (2019) ITIL Foundation: ITIL 4 Edition. London: The Stationery Office.

Culot, G., Nassimbeni, G., Podrecca, M. and Sartor, M. (2021) 'The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda', *The TQM Journal*, 33(7).

ENISA (2024) ENISA Threat Landscape 2024. Athens: European Union Agency for Cybersecurity.

European Parliament and Council (2016) Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). *Official Journal of the European Union*, L119.

European Parliament and Council (2024) Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*.

IBM Security (2024) Cost of a Data Breach Report 2024. Armonk, NY: IBM Corporation.

ISACA (2018) COBIT 2019 Framework: Introduction and Methodology. Schaumburg, IL: ISACA.

ISO (2019) ISO 22301:2019 Security and resilience Business continuity management systems Requirements. Geneva: International Organization for Standardization.

ISO/IEC (2022a) ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection Information security management systems Requirements. Geneva: International Organization for Standardization.d

ISO/IEC (2022b) ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection Guidance on managing information security risks. Geneva: International Organization for Standardization.

Loft, P., He, Y., Yevseyeva, I. and Wagner, I. (2022) 'CAESAR8: An agile enterprise architecture approach to managing information security risks', *Computers & Security*, 122, 102877.

NIST (2024) The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). Gaithersburg, MD: National Institute of Standards and Technology.

Podrecca, M., Culot, G., Nassimbeni, G. and Sartor, M. (2022) 'Information security and value creation: the performance implications of ISO/IEC 27001', *Computers in Industry*, 142.

Rose, S., Borchert, O., Mitchell, S. and Connelly, K. (2020) Zero Trust Architecture (NIST Special Publication 800-207). Gaithersburg, MD: National Institute of Standards and Technology.

Syed, N.F., Shah, S.W., Shaghghi, A., Anwar, A., Baig, Z. and Doss, R. (2022) 'Zero Trust Architecture (ZTA): a comprehensive survey', *IEEE Access*, 10.