



DATA SECURITY, GOVERNANCE AND COMPLIANCE

ETHICAL HACKINGStrengthening Data Security, Governance and Compliance at AeroLink Logistics: A Critical Evaluation and Integrated Framework for Cloud, IoT and Third-Party



2505249-SANJAY KUMAR UNKILI

UNIVERSITY OF WALES TRINITY SAINT DAVID - Wales Institute of Science and Arts –
School of Applied Computing

Abstract

Cloud services, the Internet of Things (IoT) tracking and artificial intelligence have led to AeroLink Logistics (ALL) growth and outsourcing about 88% of its information technology environment. The model facilitates global operations, but has also resulted in fragmented accountability, uncontrolled access to remote, dependence on suppliers and recurring shipment information, as well as personally identifiable information. In this report, an in-depth comparison and contrast of ISO/IEC 27001 and 27002, NIST Cybersecurity Framework 2.0, COBIT 2019 and ITIL 4 are critically examined. It then suggests an AeroLink Integrated Security Governance and Compliance model which is an amalgamation of board governance, a risk-based information security management system, operational controls, supplier assurance, incident response and business continuity. The model puts security of identity, security of cloud shared-responsibility controls, IoT authentication, privacy accountability and quantifiable service-level obligations to the forefront. It is suggested to have a three-year action plan over a year and a half. The report ends with the conclusion that legal and threat and standards monitoring should be a continuous process but the updates should be controlled via risk-based change management to prevent repetitive controls, policy weariness and operational interference.

Keywords: cybersecurity governance, ISO/IEC 27001, NIST CSF 2.0, COBIT 2019, ITIL 4, cloud security, IoT security, supplier risk, GDPR

Table of Contents

Abstract	1
1. Introduction	3
2. Organisational Context and Assumptions	3
3. Critical Evaluation of Frameworks	4
4. AeroLink Integrated Security Governance and Compliance Model.....	7
4.1 Governance, Risk and Privacy Accountability	7
4.2 Identity, IoT, Cloud, Data and AI Controls	10
4.3 Vendor and Service-Level Governance	11
4.4 Incident Response and Business Continuity	12
5. Continuous Updating of Regulations and Standards	13
6. Implementation Roadmap and Performance Measurement	14
7. Conclusion	15
References	16
Appendix A. Framework-to-Design Mapping	18

1. Introduction

AeroLink Logistics is a global logistics company that relies on real-time monitoring, cloud computing, artificial intelligence and a vast network of partnerships. The employees, suppliers and logistics partners interact across time zones and in many cases, the unmanaged devices are used. It is mentioned in the case that the unauthorised individuals have got access to the customer PII and shipment data, and security ownership, audit, encryption, incident response and continuity plans have not been developed yet. The conditions ensure the problem is broader than technical defence: ALL does not have an enterprise-wide process on how risk is accepted, how to hold suppliers responsible and how to keep a record of compliance.

There are three purposes of the report. First, it considers the well-known security, governance and service-management frameworks instead of considering any of the models as an overall solution. Second, it works on a customised governing and control structure of ALL. Thirdly, it evaluates the reasons why regulations and standards must be re-evaluated with changes in technology and threats. The design is risk-based, as a good framework has to turn business goals, and legal obligations and dependencies of operations into prioritized controls and quantifiable assurance.

2. Organisational Context and Assumptions

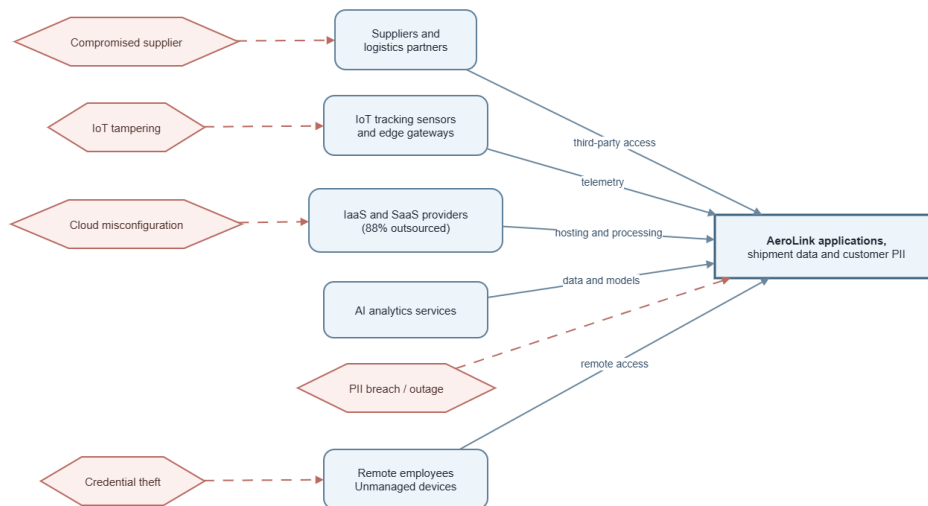


Figure 1: Current Attack Surface and Principal Threat Paths

There are five risk concentrations that are linked in the attack surface in Figure 1. Third party and remote identities are able to access internal applications without a trustworthy device assurance. IoT sensors can be either physically unprotected, computationally limited and hard to update. Services on cloud and AI spread data out among the providers and sub-processors. Outsourcing as well minimizes the immediate monitoring of configuration, logs, recoverability and

administrator action. Lastly, the lack of a good coordination can lead to confusion as to who should detect, contain, report and learn an incident.

Table 1: Design Assumptions

Assumption Area	Working Assumption
Regulatory scope	ALL serves EEA and UK customers and processes relevant PII as controller, exact national legal scope requires counsel.
Technology	Several IaaS and SaaS providers host critical services, central IAM, SIEM and supplier-risk tooling are not yet mature.
Resources	A board-sponsored eighteen-month programme and specialist support can be funded.
Operations and contracts	Shipment tracking and warehouse integrations require high availability and tested recovery, critical contracts can be amended at renewal or through risk-driven negotiation.

The design presupposes that ALL customers in the European Economic Area and the United Kingdom, PII is a controller, there are multiple global IaaS and SaaS providers, and it can afford an eighteen-month improvement programme. It also presupposes the absence of any central identity, security monitoring, or supplier-risk platform, and its maturity. The treatment of NIS2 obligations as potentially applicable is where it has been left to the national implementation and the classification of the type of services of the organisation that subject an entity to an obligation, rather than merely stating that the organisation is covered by the law. The suggested controls are thus not the official guidelines but rather a scale of the official legal advice.

3. Critical Evaluation of Frameworks

The choice of a framework depends on the needs of an organisation, as there are variations in standards and frameworks based on the purpose, details, and assurance value. Taherdoost (2022) states that one model might not be able to meet all the business needs, and complementary standards can be effective to enhance implementation [14]. This directly applies to ALL, and their weaknesses are in governance, privacy, operational security, supplier management and service continuity.

The foundation of the management system should be in the ISO/IEC 27001:2022. It also involves an organisation to design, adopt, manage and continuously enhance an information security management system (ISMS) with risk-based decisions [8]. Its power is auditable governance: the following can produce defensible evidence: scope, policies, risk treatment, competence, internal audit and management review. But it does not dictate an overall technical architecture and certification may turn into a paperwork process unless the effectiveness of controls is demonstrated. The ISO/IEC 27002:2022 provides implementation guidance, involving organisational, people, physical and technological controls but it is not a separately certifiable standard, it is guidance [9].

NIST CSF 2.0 would be more helpful in sorting out the results of operations. Its GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER capabilities are applicable in cloud, mobile, IoT and AI environments and Profiles can compare the present and the desired capability [11]. The new GOVERN feature will be useful to ALL, as it puts the supply-chain risk, policy, responsibilities and oversight in the centre-stage. However, the CSF outlines the desired results, not steps of implementation that must be followed, thus it needs to have supportive control standards and responsible owners.

Table 2: Comparative Framework Evaluation

Framework	Primary Purpose	Strength for ALL	Principal Limitation	Role in Proposed Model
COBIT 2019	Enterprise governance, decision rights and performance	Strong board alignment and tailored objectives	Too high-level for technical control design	Governance and assurance layer
ISO/IEC 27001/27002	Risk-based ISMS and control guidance	Auditable, certifiable management system	Can become compliance-led without effectiveness testing	ISMS foundation and control catalogue
NIST CSF 2.0	Cybersecurity outcomes and	Current/Target Profiles, strong	Non-prescriptive, requires supporting	Operational risk structure

Framework	Primary Purpose	Strength for ALL	Principal Limitation	Role in Proposed Model
	maturity communication	governance and supply-chain focus	controls	
ITIL 4	Service management and continual improvement	Useful for incident, change, supplier and SLA processes	Service quality does not prove security	Operational service discipline
CSA CCM	Cloud assurance and shared responsibility	Provider questionnaire and cross-framework mappings	Cloud-specific, not an enterprise governance system	Cloud control overlay

COBIT 2019 ought to bridge the gap between cybersecurity and enterprise goals and board decisions. It has a central model, which has forty governance and management objectives that can be optimised to organisational priorities [6]. COBIT is thus practical in making decisions, performance reporting and assurance, nonetheless, is too high-level to make an encryption, access or IoT choice. It is accompanied by ITIL 4 on service level in terms of incident, change, supplier, service-level and continual-improvement practices [13]. Operational discipline can be enhanced with the help of ITIL, but the sole presence of the targets of service availability cannot indicate the security of personal data or privileged access.

Integration and not competition is the right way to go. COBIT is the governor, ISO is the creator of the ISMS, NIST is the organizer of cybersecurity performance, ITIL regulates the work of the service, and the Cloud Controls Matrix (CSSA) Cloud Controls Matrix (CCM) provides cloud-specific added-value shared-responsibility and provider-assessment information. The existing CCM has 197 objectives on 17 domains and provides the Consensus Assessments Initiative Questionnaire to make sure the providers are assured [3].

4. AeroLink Integrated Security Governance and Compliance Model

4.1 Governance, Risk and Privacy Accountability

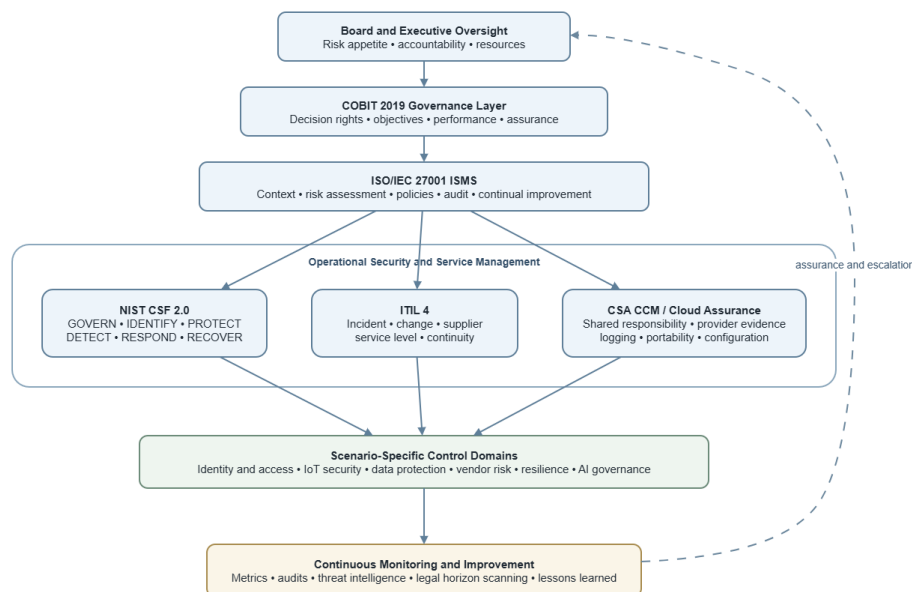


Figure 2: AeroLink Integrated Security Governance and Compliance Model

The suggested AeroLink Integrated Security Governance and Compliance model is shown in figure 2. Approving risk appetite, review material cyber and privacy risk, and getting quarterly assurance should be approved by the board. The security programme ought to be owned by a Chief Information Security Officer (CISO), whereas the privacy requirements must be left to a Data Protection Officer or other privacy lead. The operations, legal, procurement, human resources, enterprise risk and internal audit should be a part of a cross functional Security, Risk and Compliance Committee. This rights the ambiguity that currently exists by splitting the ownership, execution, consultation and independent assurance.

The committee ought to have a restrained policy framework encompassing information security, access, remote working and cloud utilization, Internet of Things, information classification and encryption, acceptable use, supplier security, incident reaction, data continuity and retention. All the policies are supposed to indicate the owner of the policy, its audience, prerequisite requirements, exceptions, evidence and review trigger. Policy then should be transformed into steps of operation which can be repeated. This is a distinction: a wide policy might need minimum privilege, whereas an access-review process will need to specify systems, reviewers, evidence, time-to-escalate and time-to-complete. Exceptions ought to be time based, risk based and must be visible to the executive in charge. The security awareness must be role-based, and

more training of the administrators, developers, procurement staff and incident decision-makers should be provided instead of a single, generic, annual, module.

Table 3: Governance RACI Matrix (A = Accountable, R = Responsible, C = Consulted, I = Informed)

Activity	Board	CISO	IT / SOC	DPO / Legal	Procurement	Vendor
Approve security strategy and risk appetite	A	R	C	C	I	I
Maintain risk register and CSF Profiles	I	A/R	R	C	C	I
Approve privacy impact assessments	I	C	C	A/R	I	C
Assess and contract critical suppliers	I	A	C	C	R	C
Detect, contain and recover from incidents	I	A	R	C	I	R/C
Provide independent control assurance	C	C	I	C	I	I

The ninety days initial should lay down a business asset, inventory of data and supplier. Every critical service is to have a business owner, data classification, purpose of recovery, lawful-processing foundation, technology dependencies and named risk owner. These facts should be translated into prioritised improvement plan and not a generic checklist by NIST CSF Current and Target Profiles. Risk acceptance should not be at the tolerance level and must have an expiry date which should be approved by the executive. Evidence testing by internal audit should be independent, and persistent overdue action challenged by the board.

The concept of privacy governance should be incorporated in the processes. The privacy and security impact assessment of new AI analytics, tracking uses and transfers across countries

should be done prior to release. The procedures of breaches should provide the ability to quickly evaluate and keep evidence and contact with controllers, processors and supervisory authorities. The EDPB (2023) clarifies that in the case of controllers, they should inform a competent authority within the 72-hour period in which a personal data breach is likely to cause harm and in the case of processors, they are required to inform the controller within the shortest time [5]. ALL should then invite suppliers to notify them much before the legal time frame and then it will be able to investigate and make decisions.

Table 4: Priority Risk Register

Risk	Likelihood	Impact	Priority	Principal Treatment	Owner
Unmanaged remote access	High	High	Critical	MFA, conditional access, restricted sessions, endpoint assurance	CISO
PII disclosure through cloud or SaaS	Medium	Very high	Critical	Classification, encryption, DLP, configuration monitoring, DPIA	DPO / Data Owner
Compromised IoT sensor or gateway	High	High	Critical	Device identity, signed firmware, segmentation, secure lifecycle	IoT Service Owner
Critical provider outage	Medium	High	High	BIA, tested RTO/RPO, resilience, exit and portability plan	Service Owner
Supplier or fourth-party compromise	High	High	Critical	Tiering, evidence, access monitoring, notification and audit clauses	Procurement / CISO
Poor incident coordination	High	High	Critical	Playbooks, RACI, exercises, evidence and communication	CISO

Risk	Likelihood	Impact	Priority	Principal Treatment	Owner
				procedures	

4.2 Identity, IoT, Cloud, Data and AI Controls

Redesigning access should be based on continuous context, least privilege and verified identity. Authentication and access control should implement phishing-resistant multi-factor authentication, single sign-on, conditional access, joiner-mover-leaver automation and quarterly entitlement verification. Approved, recorded session and time-limited privileged account access should be via a managed access platform. Unmanaged devices are to be given limited access to the browser or virtual desktop. Any sensitive downloads and local storage and persistent sessions are to be blocked. The identity management and authentication and access control functions of the NIST CSF 2.0 are depicted in the PROTECT function, which connects these security measures with the risk outcomes, but not with the product choice [11].

IoT controls should be aware of constrained device resources and physical exposure. The sensor and gateway must have a device identity, authentication by a certificate, signed firmware, a secure boot (where possible), protected keys, vulnerability records and an end-of-support date. IoT networks must not be connected to corporate and customer systems, and the gateways must validate traffic, logging centrally. Alotaibi et al. (2025) demonstrate that the traditional use of a username-password method cannot be sufficient in a limited IoT setting and that authentication options come with trade-off compared to their computation, scalability and privacy [1]. ALL then needs to lay down security requirements at the time of procurement instead of attempting to retrofit the devices that are not supported.

There should be cloud controls to define the boundary between ALL and each provider. PII and commercially sensitive shipment data in transit and rest should be encrypted, where risk and capability to service warrants such keys, the customer should have control over keys. The public storage, excessive permissions, disabled logs and unapproved regions need to be detected through cloud configuration monitoring. Identity, endpoint, cloud control plane, SaaS applications and IoT gateways logs should provide alert triage and evidence to a central security monitoring service. High-risk transfers should be monitored by data-loss prevention, however, regulations have to be adjusted so that they do not disrupt legitimate global logistics operations.

Provider-managed services should be covered by vulnerability and configuration management along with the ALL-owned assets. Risk-based schedule needs to be a combination of

authenticated scanning, cloud posture, software and devices inventories, threat intelligence and supplier notifications. Remediation targets should have been characterized by critical weaknesses and compensating controls and senior approval have to be made in the case of exceptions. The purpose of data retention should also be minimised: the longer the shipment and customer record is kept the greater the breach impact and cost of storage. Secure deletion must be validated in the backups, SaaS systems and out of terminated contracts. These controls should have operating evidence, including scan results and approved exceptions, key-rotation records, coverage and restoration test logs, no policy statement alone can demonstrate the control of risk.

AI analytics entails a list of models, data, owners and authorized use. The NIST AI Risk Management Framework plans the activity into GOVERN, MAP, MEASURE and MANAGE and recognises privacy, transparency, reliability, safety and security as inter-related aspects of trustworthy AI [10]. ALL must record data provenance, access, model change approval, human supervision as well as tests against inappropriate disclosure or manipulation. This layer, does not allow the separation of AI governance and the ISMS.

4.3 Vendor and Service-Level Governance

The most material issue in terms of governance is that the supplier risk is the most because the majority of the infrastructure is outsourced. ENISA (2021) discovered that the number of and sophistication of supply-chain attacks was on the rise and emphasized the necessity to involve suppliers in the protection strategies [4]. ALL is supposed to categorize the providers in terms of the data sensitivity, privileged access, substitutability and criticality of operation. Due diligence should be done by high-risk providers before contracting them and offer independent assurance, architecture information, vulnerabilities-management evidence, data-location information and disclosure of sub-processors.

Security responsibilities can be expressed in contracts and SLAs, instead of using general availability clauses. At least they should contain: the notification of incidents with four hours of confirmation, assisting in the investigation and regulatory reporting, the deadlines of patches depending on the severity, the audit rights and providing evidence, encryption and key responsibility, recovery time and recovery point goals, annual recovery testing, approval or notification of material sub-processors, secure deletion certificate, data portability, and exit plan. Multilevel supply-chain strategies, policies, plans and risk assessments are recommended in NIST SP 800-161 Rev. 1 due to the limited visibility of how the acquired products and services are created and secured that organisations usually have [2]. The fourth party is then supposed to be registered and not be behind the actual supplier.

Control exceptions, occurrence of incidents, outstanding vulnerabilities, availability, recovery-test results and findings of audits should be included in a quarterly supplier scorecard. Failure of repeated failure ought to be a catalyst to corrective measures, commercial remedies or migration. This strikes the right balance between accountability and practicality: ALL will not be able to outsource legal or operational responsibility by outsourcing and expecting the same level of controls out of all low-risk suppliers, but this will waste resources.

Table 5: Minimum Security and Resilience SLA Provisions

SLA Domain	Minimum Provision
Security incident	Notify ALL within four hours of confirmation, preserve evidence and support regulatory decisions.
Vulnerability remediation	Critical issues within an agreed emergency target, high issues within a risk-based target, with approved exceptions.
Recovery	Service-specific RTO and RPO, annual witnessed recovery test and remediation of failed objectives.
Assurance	Right to audit, current independent reports, scope transparency and timely remediation evidence.
Data and sub-processors	Approved locations, sub-processor transparency, encryption duties, deletion evidence and transfer safeguards.
Exit and portability	Documented export format, support period, secure deletion and continuity assistance.

4.4 Incident Response and Business Continuity

The normal risk management should be combined with incident response and continuity. Stolen credentials, PII disclosure, ransomware, cloud outage, malicious supplier access, compromised IoT devices and AI data poisoning are all required to have playbooks. Every playbook must provide decision authority, have containment options, evidence handling, legal evaluation, communications and recovery standards. NIST SP 800-61 Rev. 3 considers incident response to

be a sub-component of cybersecurity risk management and focuses on preparation, detection, response, recovery and improvement [12].

Tracking, warehouse, customer portal and integration services that were found to be vital to business should be identified in a business impact analysis and their disruption will halt operations. Service owners should agree on the recovery goals and incorporate them into supplier SLAs. The backups should be encrypted, separated and monitored and restored during exercises as opposed to reported successfulness. Tabletop exercises (semi-annual and involving executives and key suppliers) and annual technical exercises (testing regional failover, identity recovery and clean restoration) should be undertaken. Training, controls, contracts and training must be updated in lessons.

5. Continuous Updating of Regulations and Standards

The control environment of ALL is constantly evolving and requires regular updating since every time a new cloud feature, IoT device, AI model, supplier or jurisdiction is added to this list, the control environment will change. The NIST CSF 2.0 clearly considers cybersecurity risk management as an ongoing process and promotes the repetitive comparison of the current and desired Profiles [11]. Monitoring on a legal level is also crucial: the NIS2 Directive enhances the focus on governance, incident reporting, supply-chain security and risk-management efforts of covered entities [7]. An unrevised policy may thus turn into a legal incompleteness and technical ineffectiveness despite being good when it was adopted.

However, a continual revision is not necessarily good governance. Uneven updates may result in a duplication of controls, conflicting procedures and cause training fatigue and diversion of specialists to high-risk work. New standards can also be in different terminologies and providers will take time to provide the evidence or make an alteration in services. ALL ought to thus apply quarterly horizon scanning and a yearly review of the ISMS and trigger-based reviews following significant events, new laws, acquisitions or new technology. Every change is to determine the requirement, risk impacts, control owner, cost of implementation, evidence and remaining risk. Emergency updates are to take a fast track and then be given a retrospective approval.

This method is flexible without considering all publications as being equally significant. New obligations, to be mapped on new controls, should be developed by the steering committee before new policies are developed and internal audit should test the changes in practice. The process of continual improvement is turned into an evidence-based, prioritisation and learning cycle, instead of document production.

6. Implementation Roadmap and Performance Measurement

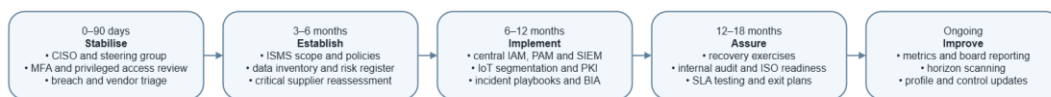


Figure 3: Eighteen-Month Implementation Roadmap

A roadmap is given in Figure 3. The identity stabilisation, privileged access and breach governance and accountable leadership should be created through immediate work. The following step should establish the ISMS, data inventory and the risk register and supplier levels. This should then be centralised using technical implementation to identify and monitor, segment the IoT services, formalise the playbooks and finalise the business impact analysis. The implementation phase should only be tested after the underlying processes are functioning consistently, audit control effectiveness is audited and the preparation of the ISO/IEC 27001 certification is prepared.

The progress will be reported using a few outcome measures: percentage of critical services that have named owners and tested recovery plans, critical suppliers evaluated, privileged accounts under managed control, high-risk access audited, critical vulnerabilities mitigated within target, mean time to detect and contain incidents, successful tests of restorations, outstanding actions in audit, and policy exceptions that are out of date. Indicators are to indicate direction, tolerance and responsible owner. The level of training completion such as high phishing-resistant authentication and access reviews is not adequate when the phishing-resistant authentication and access review are low.

Table 6: Recommended Board-Level Measures

Measure Area	Recommended Outcome Measure
Governance	% critical services with named owner and approved risk treatment
Identity	% privileged accounts managed, % high-risk access reviews completed
Supplier	% critical suppliers assessed, overdue high findings, concentration risk

Measure Area	Recommended Outcome Measure
Detection and response	Mean time to detect/contain, repeated incidents, playbook exercise results
Resilience	% critical services meeting tested RTO/RPO, restoration success
Assurance	Overdue audit actions and expired policy exceptions

7. Conclusion

ALL needs a change of governance as opposed to a set of a hodgepodge of security tools. The suggested model is based on the executive accountability with the help of COBIT, the management system with the help of ISO/IEC 27001, risk outcomes with the help of NIST CSF 2.0, service discipline and the CCM cloud assurance with the help of ITIL 4. The priority controls it provides cover the most important exposures of the scenario, uncontrolled identities, insecure IoT, distributed PII, unverified suppliers and unverified recovery. The privacy, AI governance and supplier accountability are also now considered to be routine decisions in the model. An independent assurance phase programme is more plausible as compared to instant certification. Lastly, risk-based, evidence-based and formal change management should be used to continually update. This would take ALL the pieces of a scatter-shot and responsive security into a posture that is repeatable, measurable and responsive.

References

- [1] Alotaibi, A., Aldawghan, H. and Aljughaiman, A. (2025) ‘A review of the authentication techniques for Internet of Things devices in smart cities: opportunities, challenges, and future directions’, *Sensors*, 25(6), 1649.
- [2] Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A. and Fallon, M. (2024) *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*. NIST SP 800-161 Rev. 1, Update 1.
- [3] Cloud Security Alliance (2026) *Cloud Controls Matrix*, version 4.1. [Online]. Available at: <https://cloudsecurityalliance.org/research/cloud-controls-matrix> (Accessed: 16 July 2026).
- [4] ENISA (2021) *ENISA Threat Landscape for Supply Chain Attacks*. [Online]. Available at: <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks> (Accessed: 16 July 2026).
- [5] European Data Protection Board (EDPB) (2023) *Guidelines 9/2022 on personal data breach notification under GDPR*, version 2.0. [Online]. Available at: https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf (Accessed: 16 July 2026).
- [6] European Union (2022) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive). *Official Journal of the European Union*, L333, pp. 80–152.
- [7] ISACA (2026) *COBIT: Control Objectives for Information and Related Technologies*. [Online]. Available at: <https://www.isaca.org/resources/cobit> (Accessed: 16 July 2026).
- [8] ISO (2022) *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements*. [Online]. Available at: <https://www.iso.org/standard/27001> (Accessed: 16 July 2026).
- [9] ISO (2022) *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls*. [Online]. Available at: <https://www.iso.org/standard/75652.html> (Accessed: 16 July 2026).
- [10] National Institute of Standards and Technology (NIST) (2023) *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1. [Online]. Available at: <https://doi.org/10.6028/NIST.AI.100-1> (Accessed: 16 July 2026).
- [11] National Institute of Standards and Technology (NIST) (2024) *The NIST Cybersecurity Framework (CSF) 2.0*. NIST CSWP 29. [Online]. Available at: <https://doi.org/10.6028/NIST.CSWP.29> (Accessed: 16 July 2026).

- [12] Nelson, A., Rekhi, S., Souppaya, M. and Scarfone, K. (2025) Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST SP 800-61 Rev. 3.
- [13] PeopleCert (2026) ITIL 4 Certifications and Practices. [Online]. Available at: <https://www.peoplecert.org/browse-certifications/it-governance-and-service-management/ITIL-1> (Accessed: 16 July 2026).
- [14] Taherdoost, H. (2022) 'Understanding cybersecurity frameworks and information security standards-A review and comprehensive overview', Electronics, 11(14), 2181.

Appendix A. Framework-to-Design Mapping

Design Requirement	Primary Source	Application at ALL
Board oversight and risk appetite	COBIT governance objectives, NIST GOVERN	Board reporting, risk acceptance and accountable owners
ISMS and assurance	ISO/IEC 27001/27002	Scope, policies, risk treatment, audit and management review
Operational cybersecurity	NIST CSF 2.0	Current/Target Profiles and six functions
Cloud and supplier assurance	CSA CCM, NIST SP 800-161	Shared responsibility, provider evidence, supply-chain risk plans
Service operations and resilience	ITIL 4, NIST SP 800-61	Incident, change, supplier, recovery and continual improvement
Privacy and AI	EDPB guidance, NIST AI RMF	Breach governance, impact assessment and model/data oversight