THE ZENITH CONTROLS

ISO/IEC 27001 ◊ GDPR ◊ NIS2 ◊ DORA ◊ NIST ◊ COBIT 2019

The Rosetta Stone for
Security Controls and
Regulatory Alignment

Legal Notice — Copyright and Usage Restrictions

Restrictions on Use

Prohibited Uses Without Prior Written Consent:

- Any commercial exploitation of the Work, including resale, redistribution, or provision as part of paid services, consulting engagements, workshops, or training programs.
- Uploading, sharing, or distributing the Work, in whole or in part, on public platforms, learning management systems (LMS), or internal knowledge bases beyond the purchasing entity.
- Utilization of the Work as training data or input for any form of artificial intelligence (AI) or machine learning (ML) models, including large language models (LLMs) or natural language processing (NLP) systems.
- Modification, translation, adaptation, or derivative works creation without explicit written authorization.

Permitted Use:

- Personal professional development and reference.
- Internal use by the purchasing organization solely for the purpose of information security program development and regulatory compliance implementation within the organization's legal entity.

AI/LLM Usage Restriction

The use of this Work, in any capacity, to train, fine-tune, calibrate, or validate AI, LLM, or ML models is strictly prohibited without a separately executed Enterprise Licensing Agreement. Unauthorized use for AI-related purposes constitutes a direct violation of Clarysec LLC's intellectual property rights and will be subject to civil remedies, including but not limited to injunctive relief and claims for statutory or compensatory damages.

Enforcement and Remedies

Unauthorized use, reproduction, distribution, or modification of the Work may result in legal action, including but not limited to claims for damages, injunctive relief, and termination of access to Clarysec LLC services and resources.

To request commercial licensing, enterprise distribution rights, or AI/LLM licensing,
visit us at https://clarysec.com **or contact us:** info@clarysec.com.

<table>
<tr><td colspan="5"></td><td colspan="7"></td></tr>
<tr><td colspan="5">Document number:
<strong>R001</strong></td><td colspan="7">Document Title:
<strong>Zenith Controls</strong></td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="3">Effective Date:
28.07.2025</td><td colspan="7">Document Owner:
ClarySec LLC</td></tr>
<tr><td></td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td>X</td><td>Other</td></tr>
</table>

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**
001	**25.07.2025**	**Initial Review**	**Igor Petreski**	

Introduction

What Is This Book

Zenith Controls – A GRC Rosetta Stone is a high-value reference toolkit for integrated compliance. In an era where regulations multiply and frameworks overlap, it tackles the universal challenge of translating complex standards into a clear, operational, audit-ready structure. This compendium bridges the ISO/IEC 27001:2022 Annex A control set with aligned requirements from GDPR, NIS2, DORA, NIST SP 800-53, and COBIT 2019 – mapping each control to specific external clauses with meticulous, control-level precision. In effect, it serves as a "master map" or crosswalk that connects the language of ISO 27001 to that of multiple major regulations and frameworks. The result is an authoritative one-stop reference that is as actionable as it is strategic, designed to bring order and clarity to the overlapping mandates of modern governance, risk, and compliance (GRC) programs. This book was engineered not just to explain what each control is, but to illuminate how it fits, where it maps, and why it matters across the broader compliance landscape.

Who Is It For

This toolkit is written for seasoned professionals who manage and assess security and compliance programs under real-world pressures. Key audiences include:

Chief Information Security Officers (CISOs) and GRC Leaders: Those responsible for an organization's security strategy and compliance posture will use Zenith Controls as a unifying map across standards. It connects high-level legal and regulatory expectations to concrete controls, fostering a shared understanding across technical and non-technical teams. Whether drafting a Statement of Applicability or briefing the board on risk posture, security leaders can draw on this reference to ensure nothing is lost in translation between frameworks.

Compliance Managers and Auditors: Audit and assurance professionals will find that each control "speaks their language". Every control section is annotated with audit readiness in mind – showing what evidence demonstrates maturity, which artifacts align with the control's intent, and what red flags to watch for. For internal auditors preparing an ISO 27001 certification or external assessors checking multi-standard compliance, this book supports true assurance (not just box-ticking) by providing direct, clause-by-clause mapping to requirements in GDPR, NIS2, DORA, NIST, and COBIT. It essentially equips auditors with a cross-reference for each control, so they can quickly trace how an ISO control addresses the specific points a regulator or another standard would expect to see.

Implementation Teams and Consultants: Implementers often face vague mandates and overlapping obligations. This guide offers a structured lens to interpret each control in practical terms, helping identify prerequisites and select suitable evidence without duplication. Each control section provides built-in "interpretations" and pointers that compress what could be weeks of research into a ready reference. For consultants and project leads, this immediacy is invaluable – it accelerates client onboarding and documentation alignment by presenting policy cues and integrated mappings upfront. In short, it allows implementation specialists to work smarter and faster, confidently covering multiple compliance bases at once.

Compliance Officers and Cross-Functional Teams: Beyond security specialists, legal and privacy officers, risk managers, and other GRC team members will find value in the control-level visibility this toolkit provides. It enables privacy teams to verify that data protection principles (like GDPR's requirements) are truly embedded in security controls, not just asserted in policy. Vendor management teams can reference the mappings for supplier security (e.g. NIS2 supply-chain provisions) and see exactly which ISO controls and evidence would fulfill those obligations. By empowering every stakeholder – from IT architects to privacy counsel – to work off the same mapped control set, Zenith Controls ensures everyone is aligned on compliance expectations using a common reference point.

How to Use It

Use Zenith Controls as a modular reference guide – not a book you read once from cover to cover. Each control in the ISO 27001:2022 Annex A catalog is presented as a fully self-contained section, meaning all relevant context, mappings, and guidance for that control are included right there in one place. You do not need to flip between chapters or appendices to understand how a given control relates to other standards or other parts of ISO 27001. This intentional design leads to a bit of controlled redundancy (certain key terms or references will appear under multiple controls), but that repetition is by design. It eliminates the need to cross-search elsewhere and ensures each control can serve as a standalone source of truth for implementation, assessment, or audit readiness. Practically, this means you can jump directly to whichever control you're focused on – say, 8.15 Logging or 5.12 Classification of Information – and immediately find all the context you need without wading through unrelated material. Ties to Other Controls sections within each control explain upstream or downstream linkages (for example, how asset inventory under control 5.9 enables effective vulnerability management under control 8.8) so you understand dependencies without having to consult another page. ISO Cross-References within the section point you to related ISO standards or guidance (27002, 27005, 27701, etc.) that inform that control's implementation. Cross-Compliance Mappings list the exact clauses or articles in GDPR, NIS2, DORA, NIST SP 800-53, and COBIT that correspond to the control. And Audit Considerations outline what an auditor might look for, including evidence examples and audit techniques (drawing on ISO 19011, COBIT 2019, NIST SP 800-53A/800-115, and other audit methodologies embedded in the text). Because all of this is packaged together per control, Zenith Controls effectively acts as your GRC quick-reference manual for any given control, ready to be consulted under tight timelines. This design is deliberate to support operational use under time pressure. Whether you are rushing to prepare for an audit, fielding tough questions in a board meeting, or triaging a security incident with compliance implications, you can obtain complete information at a glance for the control in question. There's no need to hunt through multiple documents or tabs – each control's section can be trusted as a full briefing on that topic. By reducing the cognitive load on the reader and providing immediate, contextual answers, the book shifts the user experience from a linear "read-it-once" format to a "grab-and-use" reference model. The Table of Contents and thematic organization (by ISO control categories) further facilitate this quick navigation. In short, use this book whenever you need authoritative cross-framework insight on a specific control, exactly at the moment you need it – it's built to be revisited often, not shelfware.

Not a How-To Guide – Complementing the Zenith Blueprint

It is important to understand what Zenith Controls is not. This compendium is not a step-by-step implementation manual or a policies-and-procedures cookbook. It does not provide an A-to-Z tutorial on how to establish an ISMS or configure security tools – that kind of guidance is outside its scope. Instead, this book assumes you are already working on implementing or managing controls and need a reference point to ensure alignment across multiple standards. For those seeking a prescriptive "how to implement ISO 27001" walkthrough, Clarysec offers the separate Zenith Blueprint, which is an auditor's 30-step roadmap to building an integrated compliance program for ISO 27001, NIS2, NIST, DORA, and GDPR. The Blueprint covers the programmatic rollout and operational best practices – essentially the project plan and process guidance for an ISMS implementation. By design, Zenith Controls complements that guide rather than duplicating it. In fact, the Zenith Blueprint itself directs readers to use the Zenith Controls toolkit for in-depth control mapping and legal cross-references. Think of it this way: if the 30-step Blueprint is the "how," then Zenith Controls is the authoritative source for "what" and "where." It provides detailed clause-by-clause mappings and control interpretations that you will reference during implementation and audits. Used together, the Blueprint and the Controls Map form a complete toolkit, one to drive implementation, and one to verify comprehensiveness and cross-compliance at each step. By clarifying this division of labor up front, we set the expectation that this book is a reference tool for professionals, not a training manual or beginner's guide to security controls.

A Living Document: Our Commitment to Currency

It is essential to recognize that this toolkit is a living document, not a static publication. The governance, risk, and compliance (GRC) landscape is in constant flux: regulations are updated, new threats emerge, and best practices evolve. Our commitment is to ensure this toolkit reflects the most current state of the industry. For this reason, Zenith Controls utilizes a software-style versioning system (e.g., v1.3, v1.4) rather than traditional book editions. This model allows us to release timely updates, whether to address a significant regulatory change, incorporate new framework mappings, or make minor corrections and clarifications. All updates are provided to our clients at no additional cost, ensuring the value of your toolkit grows and remains relevant long after the initial purchase.

Hidden Strategic Value

Beyond its immediate utility as an ISO-centric mapping resource, Zenith Controls offers a deeper strategic advantage: it functions as a bidirectional GRC reference or "Rosetta Stone" for compliance. While each section starts from an ISO 27001:2022 control, the integrated mappings mean you can just as easily work in reverse – from any given requirement in an external regulation or framework back to the ISO control universe. In other words, if a regulator, client, or auditor asks, "How are we addressing GDPR Article 32 or a specific NIST SP 800-53 control?", you can consult this toolkit and pinpoint exactly which ISO 27001 control(s) cover that requirement, complete with the justification and evidence expectations. One independent review highlighted this value, noting how the cross-mapping "translates the intent of an ISO 27001 control into the specific language and requirements of other critical frameworks," thereby creating a powerful linkage for users. By demonstrating that effective implementation of a given ISO control provides direct, auditable evidence of compliance with a corresponding GDPR, NIS2, or DORA clause, the toolkit operationalizes the mantra “implement once, comply many”. This bidirectional mapping capability turns Zenith Controls into a potent cross-compliance engine. It enables organizations to identify common denominators across their obligations and leverage one well-designed control to satisfy multiple oversight requirements at once. For example, a solid access control program (mapped in ISO control 5.18 and others) can be shown to fulfill not only ISO/IEC 27001 needs but also GDPR’s data security principle, NIS2’s cyber hygiene requirements, relevant NIST SP 800-53 controls, and COBIT governance objectives – all cross-referenced in one place. This not only reduces duplication of effort; it also supports a more unified compliance narrative when communicating with stakeholders. A CISO can confidently report that by implementing control X from ISO, the company simultaneously strengthens its posture under European law (GDPR/NIS2), financial sector rules (DORA), and industry best practices (NIST/COBIT), with evidence mapped and ready to show. The hidden strategic value lies in this breadth of insight: Zenith Controls doesn’t just map one standard to others as a one-way exercise; it gives you a two-way translation tool for your entire GRC ecosystem. It empowers you to navigate complexity by turning overlapping requirements into an integrated set of actionable controls, ensuring that no matter which compliance lens you or your stakeholders are looking through, you can find a clear answer in the same reference toolkit. By using **Zenith Controls – A GRC Rosetta Stone** as your daily companion for compliance work, you gain not only a meticulous ISO 27001:2022 control reference, but also a confident command of how those controls resonate across global standards. This introduction has outlined what the book is, who it serves, how to wield it, and where its unique value lies. In the pages ahead, you will find each control broken down with precision and purpose. Use it to bring consistency to your audits, speed to your implementations, and insight to your decision-making. No fluff, no filler – just a pragmatic toolkit to help you master the art of “mapping once, complying with many.” Welcome to your new cross-compliance reference standard.

ISO Cross-References: A Multi-Standard Backbone

While ISO/IEC 27001:2022 forms the central axis of Zenith Controls, this toolkit is reinforced by multiple ISO standards, each providing additional depth, clarity, or operational context. Below is an overview of the standards woven into this reference:

Core ISMS Standards

- ISO/IEC 27001:2022 – Defines the ISMS framework and required control domains.
- ISO/IEC 27002:2022 – Offers interpretative guidance clarifying control intent.
- ISO/IEC 27005:2022 – Provides structured risk management logic for controls.

Privacy and PII

- ISO/IEC 27701:2019 – Privacy Information Management Systems (PIMS), aligning with GDPR.
- ISO/IEC 29100:2011 – Framework and terminology for foundational privacy concepts.
- ISO/IEC 29134:2017 – Guidance for performing Privacy Impact Assessments (DPIAs).

Cloud Security

- ISO/IEC 27017:2015 – Security controls tailored for cloud services.
- ISO/IEC 27018:2019 – Protection of PII in public cloud environments.

Business Continuity and Resilience

- ISO 22301:2019 – Business Continuity Management Systems.
- ISO/IEC 27031:2011 – ICT readiness to sustain operations through disruptions.

Governance, Risk, and GRC Integration

- ISO 31000:2018 – Principles for enterprise-wide risk management.
- ISO/IEC 38500:2015 – Governance for IT leadership and accountability.
- ISO/IEC 27003:2017 – Implementation guidance for structured ISMS deployment.
- ISO/IEC 27004:2022 – Metrics and monitoring for ISMS performance.

Audit and Assessment

- ISO 19011:2018 – Audit methodologies aligned with management system standards.
- ISO/IEC 17021-1:2015 – Certification preparation and auditor expectations.

Secure Development, Testing, and Architecture

- ISO/IEC 27034 (Parts 1–6) – Application security through development and testing phases.
- ISO/IEC 21827 (SSE-CMM) – Maturity modeling for secure engineering practices.
- ISO/IEC 15408 (Common Criteria) – Security robustness criteria for procurement and assurance.

Third-Party and Supplier Security

- ISO/IEC 27036 (Parts 1–4) – Supplier relationship management across full lifecycle risk.

By embedding these standards into the fabric of each control, Zenith Controls becomes not just a reference for ISO 27001 certification but also a versatile framework supporting maturity assessments, strategic alignment, and integrated compliance efforts across multiple standards.

Contents

1. Organizational Controls

5.1 Policies for Information Security

Attribute	Value
Control Type	Preventive
Information Security Properties	Confidentiality, Integrity, Availability
Cybersecurity Concepts	Governance, Identify
Operational Capabilities	Governance, Policy Management
Security Domains	Governance and Ecosystem

Ties to Other Controls

5.2 Information Security Roles and Responsibilities: A robust information security policy is only effective if roles and responsibilities are clearly defined. Control 5.2 assigns accountability to individuals (e.g., CISO, IT managers) who develop, approve, and enforce the security policies set by 5.1. In practice, the policy provides the mandate, while roles/responsibilities specify who executes it (e.g., assigning a risk owner or a policy administrator).

5.31 Legal, Statutory, Regulatory and Contractual Requirements: Information security policies must reflect compliance obligations. Control 5.31 drives the content of the policy by identifying applicable laws (e.g., data protection, industry regulations) so the policy addresses necessary controls. For example, a policy may include clauses to ensure encryption or data handling requirements imposed by statute.

5.36 Compliance with Policies, Rules and Standards: Policies created under 5.1 become the benchmarks for compliance checked by control 5.36. In other words, 5.36 depends on 5.1 to define what “compliance” means (e.g., adherence to a password policy or incident reporting policy). Organizations implement monitoring and audit (5.36) against the baseline established by the policy.

6.3 Information Security Awareness, Education and Training: Communicating the information security policy is a key part of training. The high-level directives of 5.1 are translated into awareness programs and training under 6.3. For example, if the policy mandates acceptable use of email, training ensures staff understand and follow this directive.

5.24 Information Security Incident Management Planning: A security policy typically includes the requirement to prepare for incidents. Control 5.24 (incident management planning) depends on policy direction for establishing incident roles, communication plans, and resource allocation. The policy might mandate, for instance, that a documented incident response plan is maintained, linking 5.1 and 5.24.

5.37 Documented Operating Procedures: Operational procedures (5.37) often implement the intent of policies (5.1) at a detailed level. For example, a policy may require secure handling of sensitive data, and 5.37 will then describe the exact steps (backup frequency, encryption usage) that fulfill that policy requirement.

7.8 Clear Desk and Clear Screen: While 5.1 is abstract, it can include directives on physical security like "workstations must be locked when unattended," which tie directly to practical controls such as 7.8 (clear desk/clear screen). In this way, policies establish the "what and why," and specific controls (physical or technical) provide the "how."

ISO Cross-References

ISO/IEC 27001:2022 – *Clause 5.1* (Leadership and commitment): Requires top management to establish, approve and communicate the information security policy as part of the ISMS framework. This aligns directly with 5.1's intent by mandating senior management involvement in policy governance.

ISO/IEC 27005:2024 – *Clause 10.5* (Monitoring and review): Emphasizes that risk treatment measures must be continuously reviewed. An information security policy (5.1) provides risk treatment direction at the highest level. In conjunction with 27005, it implies that the policy should be reviewed in light of evolving risks, ensuring it remains effective.

ISO/IEC 27017:2021 – (Cloud security controls): Advises clarifying responsibilities between cloud providers and customers. A policy (5.1) may extend to cloud usage; 27017's guidance ensures that the policy includes cloud-specific roles and duties (e.g., who secures data in the cloud). Both standards together ensure clear governance in cloud environments.

ISO/IEC 27701:2021 – *Clause 5.2.4* (Privacy policies for PII): Requires an organization to implement privacy-specific security policies when managing personal data. Control 5.1's information security policy should incorporate or align with privacy policies (as guided by 27701). This ensures that the high-level security policy supports privacy objectives and regulatory obligations for PII.

ISO/IEC 27035-2:2023 – *Clause 7.1* (Incident management framework): Stipulates management commitment and policy for incident management. The information security policy (5.1) should reference incident management principles. ISO 27035-2 reinforces that the policy must include incident response responsibilities and review, cementing 5.1's role in the incident lifecycle.

ISO/IEC 27018:2019 – *Section 15* (Cloud PII security policy): Mandates that cloud providers establish policies for protecting personal data in the cloud. This cross-reference highlights that 5.1 applies to cloud contexts as well. For organizations using cloud services, the information security policy should ensure cloud data protection measures are formalized, as per ISO 27018's focus on PII in cloud.

Cross-Compliance Mapping

EU GDPR – Articles 5(2), 24, and 32 (Accountability, Responsibility, and Security of Processing): GDPR mandates not only implementation of appropriate safeguards (Article 32) but also clear assignment of responsibility and demonstrable accountability (Articles 5(2) and 24). Control 5.1 ensures the organization has a formal, approved information security policy that outlines security objectives, roles, and principles, fulfilling GDPR's requirement for structured governance. Article 32 emphasizes organizational measures, and a documented policy is a foundational component. Article 24 requires that data controllers implement and review policies to ensure processing aligns with GDPR principles. Evidence of Control 5.1 includes the approved information security policy, version history, policy owner assignment, and review schedules, demonstrating GDPR-aligned governance.

EU NIS2 – Articles 21(2)(a), (b), and (i) (Cybersecurity Risk Management and Governance): NIS2 requires that essential and important entities adopt a documented cybersecurity risk management framework, including governance-level security policies (Article 21(2)(a)). Control 5.1 directly fulfills this by mandating a policy that defines security objectives, management commitment, and assignment of responsibilities. Subsection (b) requires operational risk management procedures to be anchored in clear policies, while subsection (i) calls for human resource and access control policies, both of which derive from overarching information security directives. A strong implementation of 5.1 also demonstrates top-down commitment to cyber resilience, which national supervisory authorities assess under NIS2 supervision regimes.

EU DORA – Articles 5(1), 6(1), and Annex I Section A (ICT Governance and Risk Management Framework): DORA mandates that financial entities implement an internal governance framework that includes approved ICT policies set by the management body (Article 5(1)). Control 5.1 operationalizes this by requiring a formal information security policy approved at the executive level. Article 6(1) further requires clear definition of roles and responsibilities, which are embedded in policy documentation. Annex I (Section A) outlines minimum security measures, starting with governance and policy-setting. Evidence of Control 5.1 in DORA audits includes policy documents that specify scope, objectives, management roles, and integration with ICT risk management procedures.

NIST SP 800-53 Rev. 5 – PL-1, PL-2, PM-1, and PM-9 (Security Planning and Program Management): Control 5.1 maps to PL-1 (Security Planning Policy and Procedures), which requires development and dissemination of security policies and procedures. PL-2 extends this to ensure the plan defines security roles and responsibilities. PM-1 mandates an organization-wide security program plan, and Control 5.1 is often the entry point for that plan. PM-9 further supports integration of security into organizational processes, ensuring that security policies guide strategy and operations. Implementation of 5.1 provides a centralized foundation that satisfies U.S. federal requirements for formalized and reviewed security governance.

COBIT 2019 – EDM01.02, APO01.01, APO13.01 (Governance Framework and Information Security Management): COBIT emphasizes that executive management must define and maintain a governance framework (EDM01.02) with clear security policies and responsibilities. APO01.01 requires the creation of IT-related policies aligned with organizational goals. APO13.01 specifically addresses the establishment of an information security policy that is approved by senior management, communicated across the enterprise, and regularly reviewed. Control 5.1 fulfills these obligations by requiring a structured, approved, and maintained security policy that supports both operational control and strategic oversight.

Audit Methodology Considerations

ISO 19011:2018 – *Clause 6.4*: Auditors should verify that an information security policy exists and is approved by management. This involves reviewing the policy document itself and records (e.g., board meeting minutes) of its approval. They will also check evidence of communication (e.g., intranet postings or training records) and ask interviewees (executives, managers) to describe key policy elements, confirming awareness and endorsement.

ISO/IEC 27007:2020 – *Clause 6.2*: During an ISMS audit, examine whether the organization's security policy meets ISO/IEC 27001 requirements (e.g., covers scope, objectives, commitment). The auditor will trace risk assessments or audit findings back to policy elements to ensure consistency. For example, if a risk is identified in asset management, the auditor checks that the policy contains corresponding directives (such as asset inventory requirements).

ISO/IEC 27006:2020 – *Clause 9.4.2*: In a certification audit (Stage 2), the auditor evaluates policy implementation. They may require evidence such as a signed policy document, distribution logs, or training attendance. The auditor might ask to see records of periodic policy reviews. For instance, if the policy is due for annual review, auditors look for a review schedule and last revision date to ensure compliance with management review processes.

COBIT 2019 – *APO13.01 (Manage Security Policy)*: A COBIT-focused auditor would expect an approved security policy that aligns with business needs. They will examine governance documentation to ensure the policy was endorsed by leadership and integrated into enterprise processes. For example, auditors might request the policy and then interview senior managers or board members to confirm they have formally reviewed and ratified it. They may also check that security key performance indicators (e.g., policy compliance rates) are reported to management under COBIT's Monitor, Evaluate and Assess (MEA) processes.

NIST SP 800-53A – *PM-1 Assessment*: To assess policy and procedures, an auditor would collect the current information security policy and evaluate its completeness (scope, responsibilities, objectives). They will interview management and staff to confirm they know the policy's key points. For technical verification, the auditor might review system configurations to see if mandatory requirements (e.g., password rules or data classification mandates from the policy) are enforced by technology, linking policy to practice.

NIST SP 800-115 – *Document and Interview Guidance*: An auditor will review the organization's policy documents and related records (e.g., training materials, communication logs). For example, they might pick a random employee and ask, "What does the security policy say about protecting sensitive data?" to gauge understanding. They could also review evidence of policy dissemination, such as email announcements or new-hire briefings, ensuring the policy is not just written but effectively communicated.

ISACA ITAF (4th Edition) – *Performance Standard 2100/3300*: ITAF requires sufficient, appropriate evidence. The auditor will gather the security policy as primary evidence, then corroborate through multiple methods. They might use Computer-Assisted Audit Techniques (CAATs) to scan network drives or intranets for the presence of the policy text and track dissemination patterns. They will also probe change logs: if an older policy version exists, they check that updates went through a documented change process, ensuring the policy lifecycle is controlled (consistent with ITAF emphasis on change management even for documents).

5.2 Information Security Roles and Responsibilities

Attribute	Value
Control Type	Preventive
Information Security Properties	Confidentiality, Integrity, Availability
Cybersecurity Concepts	Identify, Protect
Operational Capabilities	Governance, Human Resource Security
Security Domains	Governance and Ecosystem

Ties to Other Controls

5.1 Policies for Information Security: Control 5.2 directly implements the management direction outlined in 5.1. Where 5.1 defines high-level expectations and principles, 5.2 operationalizes them by assigning actual responsibilities for maintaining, enforcing, and updating these policies. Without 5.2, policy documents risk being aspirational with no accountable owners.

5.36 Compliance with Policies, Rules and Standards for Information Security: Defined roles are critical for monitoring and ensuring adherence to policies. 5.2 supports 5.36 by establishing *who* is responsible for compliance tasks such as conducting reviews, enforcing rules, and escalating violations. For example, assigning a compliance officer to oversee password policy enforcement is a manifestation of this linkage.

5.24 Information Security Incident Management Planning and Preparation: Clear responsibilities must be assigned for incident detection, response, and escalation. 5.2 ensures that these roles such as incident handlers, forensics leads, or communication officers are formally documented and known to all relevant parties. Without this clarity, incident response becomes ad hoc and potentially ineffective.

6.3 Information Security Awareness, Education and Training: This control is only effective if someone is assigned to oversee awareness activities. 5.2 ensures that training obligations are embedded in job roles (e.g., HR or the CISO). It also supports defining which roles require specialized training (e.g., SOC analysts vs. general staff).

5.35 Independent Review of Information Security: To ensure objectivity, 5.2 supports the assignment of roles for independent assessment, often separated from operational roles. For example, internal audit teams must be free from implementation duties, a distinction enforced through properly defined responsibilities under 5.2.

5.28 Collection of Evidence: Assigning responsibility for the collection and handling of digital evidence is vital for maintaining chain-of-custody and admissibility. Control 5.2 ensures that roles such as forensic analysts or legal liaisons are clearly outlined within the ISMS.

8.2 Privileged Access Rights: Only authorized personnel should manage and review privileged access. 5.2 supports this by defining roles with authority to grant, revoke, and monitor such access. This limits overreach and enforces segregation of duties.

ISO Cross-References

ISO/IEC 27001:2022 – Clause 5.3 (Organizational Roles, Responsibilities, and Authorities): This clause is foundational to Control 5.2, requiring top management to assign, communicate, and document information security responsibilities across the organization. It mandates not only the identification of responsible personnel but also the assurance that these individuals have the authority and competence to carry out their roles. Control 5.2 is the operationalization of Clause 5.3 within the ISMS and must be clearly demonstrated during ISO 27001 certification audits through documented role assignments, organization charts, and accountability matrices.

ISO/IEC 27005:2024 – Clause 7.3.4 (Assignment of Responsibilities for Risk Treatment): In risk treatment planning, responsibilities must be assigned to ensure mitigation measures are implemented, monitored, and maintained. Control 5.2 supports this by ensuring that individuals or departments responsible for executing security-related controls are explicitly designated and aware of their obligations. Clause 7.3.4 emphasizes that this clarity is essential to avoid gaps in implementation and to support accountability in the risk management process.

ISO/IEC 27035-1:2023 – Clause 6.2.2 (Roles and Responsibilities in Incident Management): Effective incident response requires predefined roles, including incident handlers, escalation leads, communications coordinators, and forensic analysts. Clause 6.2.2 stresses that these roles should be documented and known in advance. Control 5.2 provides the overarching framework to assign and formalize these roles within the organization's broader security governance model, ensuring quick and coordinated responses to security events.

ISO/IEC 27017:2021 – Clause 6.2.1 (Cloud-specific Roles and Responsibilities): Cloud computing environments require shared responsibility models between providers and customers. Clause 6.2.1 recommends that organizations clearly define roles relating to key functions such as backup, access control, and incident response. Control 5.2 ensures that these responsibilities are properly assigned internally and contractually documented when delegated to cloud providers, supporting due diligence and service-level expectations.

ISO/IEC 27701:2021 – Clause 6.2.1 (Roles and Responsibilities for PII Processing): Privacy management systems built on ISO/IEC 27001 must assign clear roles for handling personally identifiable information (PII). Clause 6.2.1 mandates the designation of roles such as Data Protection Officer (DPO), privacy leads, and data custodians. Control 5.2 ensures that these privacy-specific roles are embedded in the broader information security role structure, providing alignment between privacy and security governance.

ISO/IEC 27018:2020 – Clause 8.1 (Accountability and Role Clarity in Cloud PII Management): This clause emphasizes that organizations must assign clear responsibilities for cloud-based PII protection. Control 5.2 supports this requirement by ensuring that roles such as cloud access managers, encryption key custodians, and monitoring personnel are defined, trained, and accountable. It also ensures that role-based segregation is enforced, reducing the risk of unauthorized access or mishandling of PII in hosted environments.

ISO/IEC 27036-2:2014 – Clause 8.3 (Assignment of Responsibilities in Supplier Relationships): This clause highlights the need to assign internal roles for managing information security within supplier agreements. Control 5.2 enables this by formalizing responsibility for managing supplier risks, including ensuring that contract owners understand and oversee security obligations throughout the supplier lifecycle.

ISO/IEC 27014:2020 – Clause 7.2.4 (Delegation and Decision-making Structure): Governance of information security requires a structured delegation model where decision rights and responsibilities are clear. Clause 7.2.4 underlines the importance of ensuring that roles are assigned not just at the operational level but also for strategic oversight. Control 5.2 enforces this structure, ensuring alignment between operational responsibilities and governance expectations.

Cross-Compliance Mapping

GDPR – Articles 5(2), 24, 37–39: Control 5.2 strongly aligns with the General Data Protection Regulation (GDPR) principle of *accountability* as outlined in Article 5(2), which requires data controllers to demonstrate compliance with all data protection principles. This necessitates clearly assigned roles for data protection tasks, ensuring every individual understands their responsibilities in processing and safeguarding personal data. Article 24 further mandates that data controllers implement appropriate technical and organizational measures reflecting the scope, context, and purposes of processing, again reinforcing the need for designated responsibilities. Moreover, Articles 37 to 39 detail requirements for appointing a Data Protection Officer (DPO), specifying their tasks and reporting lines. Control 5.2 facilitates GDPR compliance by institutionalizing structured responsibility frameworks where data protection roles such as the DPO, controllers, and processors are officially defined, ensuring accountability is operationalized.

NIS2 – Article 21(2)(a) and (i): Under the NIS2 Directive, Article 21(2)(a) requires essential and important entities to adopt a comprehensive cybersecurity risk management framework, which explicitly includes assigning roles and responsibilities for managing cybersecurity risks, incidents, and business continuity. Control 5.2 is critical here, providing the foundational mechanism for formally assigning those roles, whether in IT, compliance, or operational departments. Article 21(2)(i) also emphasizes cybersecurity training, which presumes that individuals responsible for security tasks are identified and provided with role-specific education. By implementing Control 5.2, organizations ensure that responsibility for key functions like incident handling, threat intelligence, and ICT resilience are assigned, documented, and supported with necessary competence directly supporting NIS2's organizational measures.

DORA – Articles 5(1), 5(2): The Digital Operational Resilience Act (DORA) demands that financial entities integrate ICT risk management within governance structures. Article 5(1) mandates that management bodies define, approve, oversee, and are accountable for ICT risk management, while Article 5(2) requires clear allocation of roles and responsibilities, including ensuring that individuals involved in ICT risk management functions report appropriately to senior management. Control 5.2 mirrors this by requiring an organization to explicitly assign roles such as those responsible for ICT governance, security monitoring, vulnerability management, and regulatory compliance. For instance, a financial institution must designate personnel overseeing threat monitoring and incident reporting. Without defined roles, the governance expectations in DORA cannot be met, making Control 5.2 essential for operational resilience in financial services.

NIST SP 800-53 Rev.5 – PM-23, PS-8, IR-1: Control 5.2 maps closely to NIST SP 800-53 Rev.5, specifically: PM-23 (Information Security Roles and Responsibilities) mandates that organizations designate and document roles for managing security functions. Control 5.2 fulfills this by setting out the requirement to assign and communicate these roles internally. PS-8 (Personnel Sanctions) is indirectly supported by 5.2, as defined responsibilities provide the basis for enforcing sanctions when duties are not performed appropriately. IR-1 (Incident Response Policy and Procedures) necessitates assigned roles for incident response, which Control 5.2 enables by formalizing responsibility assignment for all phases of incident management. Implementing 5.2 helps an organization align with NIST's risk management framework by ensuring that every key security task is owned by a capable and authorized individual.

COBIT 2019 – APO01.02, APO07.02, DSS01.03, MEA01.01: COBIT emphasizes the importance of defining and assigning roles to ensure governance and operational effectiveness. APO01.02 requires clear definition and communication of roles and responsibilities within the governance system, aligning directly with Control 5.2's intent to formalize security roles throughout the organization. APO07.02 mandates that roles and responsibilities be established and maintained to ensure optimal human resource deployment, including security-related functions. DSS01.03 supports operational clarity by requiring that service delivery roles (including those responsible for information security operations, user support, and incident handling) be clearly allocated and documented. Finally, MEA01.01 mandates performance monitoring of security functions, which is only possible when responsibilities are clearly assigned. Control 5.2 aligns with these COBIT objectives by ensuring that every information security responsibility is traceable to a defined role, supported by formal documentation and subject to ongoing review.

Audit Methodology Considerations

ISO/IEC 19011:2018 – Clauses 6.4.5, 6.4.7, and 6.5.6 (Information Collection and Role Validation): Auditors assess the clarity and effectiveness of assigned information security roles by interviewing key stakeholders (e.g., CISO, risk manager, department heads) and reviewing supporting documentation. Clause 6.4.7 directs the collection of evidence through interviews, observations, and document reviews. Clause 6.4.5 emphasizes risk-based prioritization, auditors may focus on roles with elevated access or strategic responsibilities. Under Clause 6.5.6, auditors examine how well the organization's structure supports the ISMS. Evidence includes organizational charts, job descriptions, and delegation records showing who is responsible and accountable for key activities such as risk treatment, access approvals, and policy enforcement. Nonconformities may be raised if roles are ambiguously defined or not communicated effectively.

ISO/IEC 27007:2020 – Clauses 6.3.3 and 7.4 (Competence and Effectiveness): Clause 6.3.3 instructs auditors to evaluate whether individuals assigned to information security roles possess the required competence. This includes reviewing training records, professional certifications, and documented onboarding procedures. Clause 7.4 focuses on the effectiveness of the ISMS, auditors assess whether roles contribute meaningfully to its performance by checking if responsibilities such as incident response, vulnerability management, or asset classification are consistently fulfilled. Evidence includes role-specific KPIs, delegation records, and staff evaluations linked to information security tasks.

ISO/IEC 27006:2020 – Clauses 9.4.2, 9.4.3, and 9.4.5 (ISMS Scope and Audit Evidence): Certification auditors confirm that security roles are formally assigned within the ISMS scope (Clause 9.4.2). Clause 9.4.3 requires evaluation of how responsibilities are distributed and whether they align with the ISMS policy and risk treatment plan. Auditors may request a RACI matrix or governance charter that defines roles such as asset owners, control owners, risk owners, and policy approvers. Clause 9.4.5 supports deeper evidence collection, including cross-checking documented roles with access logs, incident escalations, or training completion records to ensure that assigned responsibilities are exercised in practice.

COBIT 2019 – APO07, APO01, and MEA01: Under APO07 (Manage Human Resources), auditors evaluate whether roles related to information security are clearly mapped to the organizational structure. This includes reviewing whether role segregation exists between control implementation and control monitoring, especially for privileged operations. APO01 (Manage the IT Management Framework) supports review of governance mechanisms, including the definition and oversight of security responsibilities. MEA01 (Monitor, Evaluate, and Assess Performance) leads auditors to examine performance indicators tied to security roles, for example, whether individuals in defined roles complete required awareness or control validation tasks. Evidence includes HR workflows, training matrices, and audit trails linking individuals to control activities.

NIST SP 800-53A Rev.5 – PM-23, PL-1, and PL-2 Assessment Procedures: PM-23 requires auditors to verify that organizational roles for security and privacy are formally established, documented, and communicated. They review organizational charts, job descriptions, appointment letters, and governance documentation to confirm these assignments. Interviews are conducted to test awareness, auditors may ask employees to describe their security responsibilities or how they escalate incidents. PL-1 and PL-2 provide the baseline expectations for documented security policies and associated roles. Auditors often test real-world alignment by tracing a security task (e.g., patch validation, data backup) to its assigned individual or role, then confirming policy support and awareness.

ISACA ITAF (4th Edition) – Standards 1205 and 2203 (Evidence Collection and Role Assurance): Standard 1205 emphasizes sufficient, appropriate evidence, auditors must gather role-related documentation such as org charts, control owner listings, and records of delegated authority. Standard 2203, focused on audit planning, recommends that auditors assess whether critical roles have been assigned and whether security events are escalated through clearly defined responsibility paths. For example, if a log review identifies an incident, the auditor verifies whether the incident was triaged by the designated analyst, escalated to the incident manager, and resolved within role-defined SLAs. Control 5.2 is validated by proving that security functions are both assigned and operationalized.

Technical Validation – Role-Based Access Models and Delegation Records: Auditors may validate the implementation of Control 5.2 through practical evidence such as role-based access control (RBAC) configurations in Active Directory or IAM platforms. They cross-check system role assignments against documented job responsibilities. For instance, a system administrator with full access must have a documented job role, signed confidentiality agreement, and completed training on privileged access. Delegation logs, access reviews, and approval workflows are examined to ensure they match the intended role hierarchy.

5.9 Inventory of information and other associated assets

Attribute	Value
Control Type	Preventive
Information Security Properties	Confidentiality, Integrity, Availability
Cybersecurity Concepts	Identify
Operational Capabilities	Asset Management
Security Domains	Governance and Ecosystem, Protection

Ties to Other Controls

5.10 – Acceptable use of assets: Control 5.9 provides the authoritative inventory of all information assets and associated devices, enabling organizations to apply acceptable use policies consistently. Without a comprehensive asset inventory, it is impossible to define the scope of what users can or cannot use. When users sign acceptable use agreements (5.10), the categories of assets referenced such as laptops, mobile phones, email systems, or cloud storage platforms must align with those listed and maintained in 5.9. This ensures that usage rules cover all organizational assets, including newly introduced or retired assets.

8.9 – Configuration management: Configuration baselines and security hardening rely on a complete and accurate asset inventory. Control 5.9 ensures that all hardware, software, network devices, and cloud resources are documented, allowing 8.9 to enforce standard configurations, patch management, and secure setup. For example, if an organization introduces a new type of endpoint, it must first be recorded under 5.9 before 8.9 can apply appropriate security configurations.

5.14 – Information transfer: Effective control over information flows depends on knowing which information assets exist and where they are located. Control 5.9 supports 5.14 by maintaining inventories that include data classifications, storage locations, and ownership details. For example, classified data inventoried under 5.9 informs the enforcement of data transfer restrictions, ensuring that sensitive information is only transferred via approved channels and under secure protocols.

8.16 – Monitoring activities: To monitor the use of assets and detect anomalies, an organization must know what assets exist and their expected behavior. Control 5.9 supports 8.16 by providing the baseline inventory of devices, systems, and applications to be monitored. It ensures that monitoring tools are configured to track and analyze all known assets, reducing the risk of blind spots.

5.12 – Classification of information: An inventory of information assets (as required by 5.9) enables organizations to apply classification labels effectively. 5.9 lists information types, which are then classified under 5.12 for appropriate protection measures.

8.1 – User endpoint devices: The inventory maintained under 5.9 includes endpoints like laptops, phones, and workstations. This supports 8.1 by ensuring that all user devices are tracked, secured, and accounted for in the organization's security strategy.

ISO Cross-References

ISO/IEC 27005:2024 – Clause 7.2.1 (Asset Identification in Risk Assessment): The risk assessment process begins with identifying assets, understanding their value, and mapping their risk exposure. Control 5.9 provides the comprehensive asset baseline required to execute effective risk assessments under 27005. This inventory includes asset ownership, dependencies, and security requirements, enabling organizations to determine what is at risk and to prioritize risk treatment.

ISO/IEC 27011:2016 – Telecom Sector Guidance (Clause 8.1): In the telecommunications sector, asset inventory extends to network infrastructure such as routers, switches, transmission systems, and customer data repositories. Control 5.9 aligns with this sector-specific requirement, reinforcing that a robust inventory is essential for securing critical communications infrastructure, meeting both security and regulatory obligations, including national security mandates.

ISO/IEC 19770-1:2017 – IT Asset Management (ITAM): While primarily addressing software and hardware lifecycle management, ISO 19770-1 complements 5.9 by offering best practices for building and maintaining detailed IT asset inventories. Implementing 5.9 in line with 19770-1 ensures not only security coverage but also license compliance, cost control, and efficient asset utilization. This standard emphasizes accurate asset data, ownership accountability, and continuous updates, which reinforce security visibility.

ISO/IEC 27002:2022 – Guidance for 5.9: The updated guidance specifies that the asset inventory should include information assets (e.g., databases, documentation), technical assets (e.g., servers, network devices), and physical assets (e.g., buildings, power supplies), all associated with security responsibilities. Control 5.9 ensures that ownership, classification, and handling requirements are clearly linked to each asset.

ISO/IEC 22301:2019 – Clause 8.2.2 (Business Continuity – Resources): While focused on business continuity, this clause reinforces the need for an inventory of critical assets, ensuring that resilience planning is based on a clear understanding of what assets are essential. 5.9 supports this by providing the asset baseline necessary for continuity planning and disaster recovery.

Cross-Compliance Mapping

EU GDPR – Article 30 (Records of Processing Activities) and Article 32 (Security of Processing): Article 30 of the GDPR obliges both data controllers and processors to maintain detailed records of processing activities, including what personal data is collected, where it resides, how it is processed, and who is responsible. Control 5.9 supports this by ensuring organizations maintain a comprehensive inventory of assets, including data repositories, applications, and processing platforms, forming the foundation of the RoPA (Records of Processing Activities). Additionally, Article 32 requires appropriate technical and organizational measures to protect personal data. Without an accurate and current asset inventory, organizations cannot assess or implement appropriate protections. For example, a SaaS platform that processes customer data must be inventoried with its data flows, ownership, and protection status clearly defined, both to fulfill Article 30 documentation and support Article 32 safeguards.

EU NIS2 – Article 21(2)(b) and Annex I (Identification of Critical Systems): NIS2 mandates that essential and important entities identify and manage risks related to their network and information systems. Article 21(2)(b) requires asset management as a foundation for other security measures. Annex I further specifies that organizations must identify the critical systems and components that underpin their essential services. Control 5.9 fulfills this requirement by establishing an inventory of all assets, both IT and OT, including their role in service delivery, criticality, dependencies, and technical characteristics. This supports upstream controls such as access management, supply chain risk assessment, and incident classification.

EU DORA – Article 5(2), Article 9(1)(e), and Article 18(3): DORA obliges financial entities to maintain detailed knowledge of their ICT environments. Article 5(2) requires governance of ICT risks, which cannot be achieved without visibility into underlying assets. Article 9(1)(e) explicitly references the need to document dependencies on ICT systems and assets, including third-party providers. Article 18(3) further calls for organizations to establish standards and processes governing the development and management of ICT systems. Control 5.9 enables this by ensuring that all relevant ICT assets, including virtual machines, APIs, SaaS platforms, and cloud workloads, are tracked with ownership, versioning, criticality, and interconnectivity metadata. This inventory feeds into operational resilience, threat modeling, and vendor management.

NIST SP 800-53 Rev.5 – CM-8 (System Component Inventory), CA-7 (Continuous Monitoring), and PM-5 (Information System Inventory): CM-8 mandates a baseline and continuously updated inventory of hardware, software, firmware, and virtual components. Control 5.9 enables this through automated discovery tools, manual verification processes, and lifecycle tracking from acquisition to decommissioning. CA-7's continuous monitoring requirement relies on an accurate asset inventory to detect anomalies and unauthorized changes. PM-5 requires a complete listing of organizational systems, particularly those supporting mission-critical operations. For instance, Control 5.9 would ensure that all virtual machines spun up in a cloud tenant are registered, assigned an owner, and assessed for exposure, thereby supporting both operational and compliance requirements under SP 800-53.

COBIT 2019 – BAI09.01, BAI09.02, and DSS05.04: BAI09.01 emphasizes establishing and maintaining configuration repositories that include asset records, versions, and relationships. BAI09.02 supports tracking assets throughout their lifecycle, ensuring consistent identification and management. DSS05.04 addresses threat management and requires knowing which assets are exposed to which threats, a process dependent on having a reliable asset inventory. Control 5.9 ensures that hardware, software, services, data assets, and interdependencies are documented, tagged by criticality, and regularly updated, forming the governance foundation for security controls, patching, business continuity, and auditability.

NIST Cybersecurity Framework (CSF) – ID.AM (Asset Management): The Identify function in the CSF begins with ID.AM, which focuses on understanding the assets that support business functions. Control 5.9 directly maps to ID.AM-1 through ID.AM-6, ensuring that physical devices, software platforms, communications flows, and ownership are defined. This visibility supports downstream security measures such as access control, data protection, and anomaly detection. For example, if a zero-day is announced for a specific database version, 5.9 ensures the organization knows where that version is deployed and who is responsible for mitigating the risk.

ISACA ITAF (4th Edition) – 2204 (Risk Assessment) and 2301 (Evidence Collection): IT auditors evaluate the completeness and accuracy of asset inventories as part of assessing organizational risk and control design. Under ITAF 2204, an incomplete inventory is a control weakness, as unidentified assets may be unmanaged and vulnerable. Control 5.9 ensures that inventories support audit evidence requirements under ITAF 2301, providing traceability, ownership, and security posture data for each asset. For instance, during an audit, the absence of a critical cloud asset in the official register would raise a red flag; 5.9 ensures this scenario is avoided.

Audit Methodology Considerations

ISO/IEC 19011:2018 – Clause 6.4.5 (Audit Execution): Auditors will typically request the asset inventory early in the audit to help scope other control evaluations. For 5.9, they assess the completeness and accuracy of the inventory by conducting spot-checks. This includes verifying physical assets (e.g., comparing asset tags or serial numbers in a data center or office) and sampling software or cloud services against the documented inventory. Discovery of unrecorded assets (physical, virtual, or cloud) indicates a gap in the control's implementation, potentially exposing the organization to unmanaged risks.

ISO/IEC 27007:2020 – Clause 7.4.5 (Interviews and Operational Integration): Auditors evaluate not just the presence of an inventory but its maintenance mechanisms. They inquire: "How and when is the inventory updated?" Evidence includes change management records, procurement workflows, or decommissioning forms demonstrating that inventory updates are linked to asset lifecycle events. If a CMDB or asset management tool is used, auditors review audit logs to ensure regular updates. For example, auditors verify whether IT onboarding (e.g., issuing laptops) triggers inventory updates, showing that 5.9 is embedded in business processes.

ISO/IEC 27001:2022 – Annex A Control 5.9: Auditors confirm that ownership is assigned to each asset in the inventory. They may sample assets and ask designated owners to explain their custodianship and responsibilities. Lack of awareness by the listed owner suggests the inventory may be theoretical rather than operational. This also links to 5.2 (Roles and Responsibilities) and 5.10 (Acceptable Use), where asset management must be aligned with ownership and usage policies.

COBIT 2019 – BAI09 (Manage Assets) and DSS Domains: COBIT requires integrated asset management for effective access control and support operations. Auditors assess whether the asset inventory aligns with identity and access management systems (DSS05.04) and physical access controls (DSS05.05). For 5.9, auditors compare IT asset management practices with COBIT guidance, verifying that all assets (hardware, software, data) are tracked. Missing entries, like unlicensed software or untracked data stores, indicate inventory weaknesses requiring corrective action.

ISACA ITAF – Section 2300 (Evidence and Risk Consideration): ITAF guides auditors to focus on risk linked to incomplete inventories. Auditors investigate potential shadow IT by comparing procurement records to the inventory or conducting network scans (with permission) to detect untracked devices. For example, if 100 servers were purchased, but only 90 appear in the inventory, this signals a compliance failure. Auditors document such gaps, showing that 5.9 is not comprehensively enforced, exposing the organization to unmonitored asset risks.

NIST SP 800-53A – CM-8 (System Component Inventory): NIST-oriented audits verify that the inventory includes required details: asset type, owner, location, IP address, status, and whether it is active or decommissioned. Auditors assess whether the inventory is leveraged operationally e.g., is it integrated with vulnerability scanning? All inventoried IPs should be scanned regularly. Auditors also confirm that virtual, cloud-based, and mobile assets are included. An inventory focusing solely on on-premise assets indicates partial implementation of 5.9, leaving gaps in cloud security governance.

5.19 Information security in supplier relationships

Attribute	Value
Control Type	Preventive
Information Security Properties	Confidentiality, Integrity, Availability
Cybersecurity Concepts	Identify
Operational Capabilities	Supplier Relationships Security
Security Domains	Governance and Ecosystem, Protection

Ties to Other Controls

5.20 – Supplier Agreements on Information Security: 5.19 sets the security expectations for how suppliers should handle organizational information. 5.20 formalizes those expectations by ensuring that contracts or agreements explicitly include security clauses, such as confidentiality requirements, compliance with security policies, and incident notification procedures. Without 5.20, the requirements identified in 5.19 may not be legally enforceable.

5.21 – ICT Supply Chain Security: While 5.19 focuses on overall supplier relationships, including service providers, consultants, and outsourcing partners, 5.21 provides specific attention to the ICT supply chain ensuring that hardware, software, and development services procured are secure and vetted. Both controls work together to ensure comprehensive supplier risk management, from general third-party access to critical ICT components.

5.14 – Information Transfer: Supplier relationships often involve data exchange, such as support files, shared platforms, or cloud access. 5.14 mandates that such information is transferred securely through encryption, restricted access, and verification of recipients. When managing suppliers under 5.19, organizations must ensure that any data shared adheres to secure transfer protocols, and that suppliers are bound to uphold the same security standards.

5.36 – Compliance with Policies, Rules, and Standards: Supplier relationships need to be monitored for ongoing compliance with agreed security controls. 5.19 establishes initial security requirements, but 5.36 ensures that suppliers are audited, reviewed, and held accountable for compliance throughout the relationship lifecycle.

5.10 – Acceptable Use of Information and Assets: Suppliers accessing or processing organizational information must adhere to acceptable use policies. 5.19 requires that suppliers are aware of and follow rules regarding how information and assets are used, stored, and transmitted, extending internal user behavior expectations to external parties.

ISO Cross-References

ISO/IEC 27002:2022 – Clause 5.19 (Information Security in Supplier Relationships): Advises establishing a supplier security policy based on risk tiering, where higher-risk suppliers are subject to more stringent security requirements. The clause emphasizes defining controls per supplier tier, assigning responsibility for supplier security monitoring, and conducting regular assessments (e.g., audits, compliance reports). It also highlights the need to control supplier access using least privilege and to revoke access promptly when no longer needed.

ISO/IEC 27036-1:2021 – Clause 6.3 (Managing Supplier Relationships): Provides an overview of security requirements across all supplier types. It recommends risk-based approaches for managing suppliers, including identifying critical suppliers, ensuring security alignment, and integrating supplier risk assessments into organizational governance. This supports 5.19 by framing supplier relationships as part of the organization's extended security perimeter.

ISO/IEC 27036-2:2022 – Clause 7 (Supplier Agreement Requirements): Outlines how to translate information security requirements into supplier agreements. While this directly supports 5.20, it is intrinsically linked to 5.19 as it requires that all identified security needs be formalized contractually, including incident handling, access control, and compliance obligations.

ISO/IEC 27036-3:2023 – Clause 8.2 (ICT Supply Chain Risk Assessment): Focuses on ICT suppliers, emphasizing risk identification for hardware, software, and services. It advises including supplier assessments, validation of security controls, and ongoing monitoring of supply chain dependencies, reinforcing 5.19's application in ICT contexts.

ISO/IEC 27036-4:2016 – Clause 7.4 (Cloud Services Procurement): Highlights specific risks in cloud service supplier relationships, advising security due diligence, contractual clauses for data handling, availability, and exit strategies. It ties to 5.19 for cloud-based supplier engagements, ensuring cloud providers meet security requirements.

ISO/IEC 27701:2021 – Clause 7.2.5 (Processors): Requires that when suppliers process PII, the organization must ensure they provide sufficient guarantees for privacy protection (aligning with GDPR Article 28). This supports 5.19 by embedding privacy-specific security controls into supplier management, including audits, PII handling policies, and incident notification obligations.

Cross-Compliance Mapping

EU GDPR – Article 28 (Processor Obligations): GDPR Article 28 requires controllers to only engage processors (suppliers or service providers) that provide sufficient guarantees for implementing appropriate technical and organizational measures for data protection. This must be formalized in written contracts, typically through Data Processing Agreements (DPAs). Control 5.19 enforces supplier due diligence by mandating security assessments prior to onboarding, and requiring that contractual clauses specify data protection responsibilities. Evidence of DPAs, documented supplier assessments, and ongoing monitoring are all required for demonstrating compliance, particularly where suppliers process personal data on behalf of the controller.

EU NIS2 – Recital 54 & Article 21(2)(d) (Supply Chain Cybersecurity): NIS2 emphasizes the assessment and mitigation of cybersecurity risks across the supply chain. Article 21(2)(d) obligates organizations to include supply chain risk management as part of their security framework. Control 5.19 requires the evaluation of supplier cybersecurity practices, the acquisition of certifications (e.g., ISO 27001) or independent audit reports, and imposition of contractual security requirements. Supply chain vulnerability analysis and supplier selection are aligned with sector-specific guidance, such as ENISA's recommendations, ensuring continuous oversight and timely response to third-party risks.

EU DORA – Articles 28–30 (ICT Third-Party Risk Management): DORA mandates a robust ICT third-party risk management framework for financial entities, covering the full lifecycle of supplier relationships. Articles 28–30 require criticality classification of suppliers, pre-contractual due diligence, periodic risk assessments, and the inclusion of audit, resilience testing, and exit clauses in all key supplier contracts. Control 5.19 operationalizes these expectations by mandating supplier criticality reviews, regulatory notification and oversight rights, and concentration risk analysis to prevent overreliance on single providers.

NIST SP 800-53 Rev.5 – SA-9 (External System Services), SR-3 & SR-6 (Supply Chain Risk Management): SA-9 requires that security controls be extended to external providers, including the monitoring and management of all outsourced IT or cloud services. SR-3 calls for supply chain controls, including onboarding processes, supplier vetting, and periodic review, while SR-6 mandates ongoing supplier security assessments. Control 5.19 directly aligns by requiring formal risk-based management, security assurance evidence from suppliers, and continuous oversight of service delivery, mapped to the broader principles of NIST SP 800-161 (Supply Chain Risk Management Practices for Federal Information Systems).

COBIT 2019 – DSS04.03 (Manage Supplier Risk), APO10.03 (Manage Supplier Agreements): COBIT 2019 requires organizations to assess, monitor, and mitigate information security risks associated with suppliers and service providers. DSS04.03 mandates the integration of supplier risk management into the organization's information security processes, including pre-contractual risk assessment, ongoing monitoring, and review of supplier performance. APO10.03 requires formal agreements that clearly define security obligations, performance criteria, and rights for audit and corrective action. Control 5.19 directly supports these governance requirements, ensuring end-to-end lifecycle management of supplier risks.

Audit Methodology Considerations

ISO/IEC 19011:2018 – Clause 6.4.5 (Audit Execution): Auditors request the supplier inventory, focusing on those with access to information or systems. They assess whether suppliers are risk-categorized. An incomplete inventory or lack of risk-based classification signals deficiencies in supplier oversight.

ISO/IEC 27007:2020 – Clause 7.4 (Conducting the Audit): For sampled suppliers, auditors review due diligence records security questionnaires, ISO 27001 certificates, SOC 2 reports, or internal risk assessments. The depth of evaluation must correspond to the supplier's risk level. Missing or superficial reviews for high-risk suppliers are noted as significant gaps.

ISO/IEC 27001:2022 – Annex A 5.19 Compliance: Auditors inspect contractual clauses (aligned with 5.20) to verify inclusion of confidentiality, breach notification, audit rights, and compliance obligations. Contracts lacking security clauses undermine 5.19's objectives.

COBIT 2019 – APO10.04 (Manage Supplier Risk): Auditors evaluate ongoing supplier monitoring, such as annual security reviews, updated certifications, or vendor-provided test results. They review organizational responses to supplier-related incidents or publicized breaches, confirming if risk reassessments or mitigating actions were taken.

ISACA ITAF – Performance Standard 2402 (Evidence Collection): Auditors assess supplier access controls, verifying whether third-party accounts are unique, time-bound, and MFA-protected. For terminated suppliers, auditors check if accounts were revoked and whether access removal aligns with contract end-dates.

NIST SP 800-53 Rev.5 – SA-9 (External System Services), SR-3 (Supply Chain Controls), SR-6 (Supplier Assessments): Auditors verify supplier compliance evidence, requesting certifications and assessing if these were reviewed internally for relevance; Fourth-party risks are considered whether the organization requests supply chain transparency from key suppliers, and whether security flow-down requirements are enforced.

Procurement Process Review: Auditors interview procurement/legal teams, checking for security checklists in contract workflows. Security team sign-offs for high-risk contracts are validated against procurement policy, and contract case studies are reviewed for compliance.

Supplier Termination Controls: For ended relationships, auditors examine exit documentation: data return/destruction certificates, asset recovery, and whether termination checklists included security measures. Lack of structured termination handling poses residual access risks.

Continuous Improvement and Threat Adaptation: Auditors assess whether supplier management processes adapt to new threats (e.g., post-SolarWinds actions) or regulatory changes (e.g., DORA compliance enhancements). Reactive vs. proactive adjustments indicate the maturity level of supplier risk governance.

5.23 Information security for use of cloud services

Attribute	Value
Control Type	Preventive
Information Security Properties	Confidentiality, Integrity, Availability
Cybersecurity Concepts	Protect
Operational Capabilities	Supplier Relationships Security
Security Domains	Governance and Ecosystem, Protection

Ties to Other Controls

5.19 – Supplier relationships: Cloud service providers (CSPs) function as critical suppliers, and thus all controls regarding supplier selection, contracting, and risk management under 5.19 apply. However, 5.23 goes further by addressing cloud-specific risks, such as multi-tenancy, data location transparency, and shared responsibility models. It ensures organizations not only treat cloud providers as suppliers but also assess how virtualization, elasticity, and remote management inherent to cloud affect information security.

8.1 – User end-point devices and 8.20 – Networks security: Accessing cloud environments typically involves diverse endpoint devices and reliance on external networks. 5.23 emphasizes that endpoints must meet security standards such as enforced encryption, anti-malware, and compliance checks before connecting to cloud services. Additionally, network security controls from 8.20, like VPN usage, TLS enforcement, and firewall configurations, are essential to safeguard cloud access channels, especially in public or hybrid cloud setups.

5.14 – Information transfer: Cloud adoption necessitates secure data transfers to and from external cloud infrastructures. 5.23 extends 5.14 by demanding encryption in transit, API security, and secure integration methods for cloud-hosted data and services. This ensures that information flowing between on-premise systems and cloud platforms, or between multiple cloud services, remains protected against interception and unauthorized access.

8.11 – Data masking and 8.12 – Data leakage prevention: As data is stored and processed off-premises, 5.23 also ties to these controls by enforcing data minimization, tokenization, or masking techniques where appropriate, reducing exposure in cloud environments. DLP solutions, tailored for cloud contexts (e.g., CASB), are essential to prevent inadvertent or malicious data leaks.

5.9 – Inventory of information and other associated assets: Ensuring visibility into cloud-stored data and associated resources (e.g., virtual machines, storage buckets) is critical. 5.23 reinforces 5.9 by requiring tools and processes to maintain up-to-date inventories within dynamic cloud environments.

8.25 – Secure development lifecycle: When using Platform-as-a-Service (PaaS) or Function-as-a-Service (FaaS) offerings, organizations often deploy custom code in cloud environments. 5.23 links to 8.25 by mandating that secure development practices are extended into cloud-based development, including code repository security, automated testing pipelines, and secure deployment configurations.

ISO Cross-References

ISO/IEC 27017:2015 – Cloud Security Controls (CSP-01 to CSP-07): Provides specific implementation guidance for both cloud service customers and providers on securing cloud environments.
Example: For 5.23, organizations adopt ISO 27017 recommendations such as CSP-01 (Shared Roles and Responsibilities), ensuring clarity in responsibility demarcation between the cloud customer and provider. Controls like CSP-02 support secure virtual machine configurations, while CSP-06 advises on customer activity monitoring including access logs and audit trails essential for maintaining visibility in cloud ecosystems.

ISO/IEC 27018:2020 – Clause 9.2.1 (Protection of PII in Public Cloud): Focuses on privacy controls for personally identifiable information (PII) processed in cloud environments. 5.23 incorporates this by requiring contractual assurances before using cloud services for PII, ensuring that data is encrypted, that provider personnel access is strictly controlled, and that PII is not used for secondary purposes without consent. Example: Organizations mandate data location clauses in cloud contracts and use encryption key management to retain control over PII stored in cloud services.

ISO/IEC 27701:2021 – Clause 8.2 (Processor Obligations in Cloud Context): Extends privacy requirements into cloud environments where providers act as data processors. 5.23 ensures that all GDPR or other privacy law obligations such as right to access, data deletion, or data breach notification are fully operational within cloud services. *Example*: Auditors expect to see processes and contractual mechanisms enabling the organization to instruct the cloud provider on handling data subject requests or executing data deletion securely and in compliance with applicable regulations.

ISO/IEC 27036-4:2016 – Clause 7.2 (Monitoring Cloud Service Delivery): Recommends that cloud customers continuously monitor service delivery, including security metrics, incident notifications, and service availability. Under 5.23, this ensures active engagement with cloud providers, particularly in multi-tenant environments, to mitigate shared risks.

ISO/IEC 27005:2024 – Clause 8.3 (Risk Assessment in Cloud Services): Encourages organizations to perform detailed risk assessments when adopting cloud services, identifying specific threats like data co-mingling, lack of transparency, or vendor lock-in. 5.23 integrates this by requiring cloud security strategies based on evaluated risks.

Cross-Compliance Mapping

EU GDPR – Chapter V (International Data Transfers), Article 28 (Processor Obligations), Articles 33/34 (Breach Notification): GDPR strictly governs personal data transfers to cloud providers, especially when located outside the EU/EEA. Under Chapter V, organizations must use lawful transfer mechanisms, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), and ensure that the cloud provider's data residency and processing comply with EU requirements. Article 28 requires robust contractual arrangements for processors, which in cloud contexts means clear Data Processing Agreements specifying data handling, security, and breach response. Under Control 5.23, organizations must assess the provider's location and compliance, document transfer mechanisms, and integrate cloud monitoring with incident response processes, so that any cloud-based breach triggers the appropriate GDPR notifications (Articles 33/34).

EU NIS2 – Article 21 (Cybersecurity Risk Management), Recital 90 (Concentration Risk): NIS2 requires essential and important entities to ensure robust cybersecurity in cloud environments, with specific focus on measures such as multi-factor authentication, encryption, monitoring, and incident handling. Control 5.23 mandates that organizations assess and validate their cloud providers' security controls to ensure they meet or exceed NIS2 requirements, particularly when cloud is critical to business operations. Additionally, Recital 90 highlights the risk of systemic dependency on a single cloud provider. Control 5.23 addresses this by requiring contingency planning, such as multi-cloud strategies or tested exit plans, to maintain resilience if a primary provider is compromised or fails.

EU DORA – Articles 28–31 (ICT Third-Party Risk, Cloud Oversight): DORA designates cloud service providers as critical ICT third parties for the financial sector, imposing rigorous requirements for due diligence, risk assessment, contract management, and ongoing monitoring. Control 5.23 requires organizations to maintain up-to-date inventories of cloud assets and user accounts, establish cloud-specific KPIs and KRIs, and ensure regular reviews of provider controls. Organizations are expected to develop and periodically test cloud exit strategies and demonstrate oversight of cloud concentration risk, directly supporting DORA's operational resilience mandate.

NIST SP 800-53 Rev.5 – SC-2 (Security Function Isolation), SC-7 (Boundary Protection), SI-4 (System Monitoring), CA-7 (Continuous Monitoring), SA-9 (External System Services): NIST standards require organizations to ensure that security functions in cloud environments are isolated from untrusted or tenant systems (SC-2), that network boundaries are protected (SC-7), and that robust monitoring and logging are implemented (SI-4, CA-7). SA-9 specifically mandates that contracts with cloud providers include security controls and compliance requirements. Control 5.23 operationalizes these by requiring the organization to assess the provider's technical controls (e.g., segmentation, monitoring, access control), verify contractually mandated protections, and integrate cloud assets into continuous monitoring programs. Organizations must also ensure cloud provider personnel are vetted and that system changes (such as use of new sub-processors) are communicated and assessed for risk.

COBIT 2019 – DSS05.10 (Manage Network and Connectivity Security), DSS06.08 (Manage Data Exchange), APO10.04 (Maintain Supplier Relationships): COBIT 2019 addresses cloud-specific security through DSS05.10, which mandates that all networked/cloud services are secured and monitored; DSS06.08, which calls for robust controls over data exchange with cloud suppliers; and APO10.04, which requires ongoing supplier relationship management, including performance, compliance, and risk reviews. Control 5.23 ensures organizations define, review, and enforce cloud security requirements contractually and operationally, maintaining auditability and resilience across all cloud relationships.

C5:2020 – German Cloud Computing Compliance Criteria Catalogue: C5 is a widely adopted assurance standard for cloud providers in Europe, establishing requirements for data protection, incident response, service transparency, and auditability. Under Control 5.23, organizations should validate cloud provider certifications such as C5, CSA STAR, or SOC 2 Type II (with cloud-specific criteria), ensuring that the provider meets internationally recognized standards for cloud security and operational control.

Audit Methodology Considerations

ISO/IEC 19011:2018 – Clause 6.4.5 (Audit Execution): Auditors begin by establishing a cloud service inventory, reviewing whether the organization maintains a register of approved cloud services (IaaS, SaaS, PaaS) and monitors for unauthorized (Shadow IT) cloud usage. Absence of such oversight may prompt recommendations to implement CASB tools or network discovery mechanisms. Auditors request documentation or dashboards showing visibility into all active cloud services.

ISO/IEC 27007:2020 – Clause 7.4.5 (Interviews and Documentation Review): Auditors review cloud security configurations through assessment reports or direct inspection. *Example*: In AWS environments, they check S3 bucket permissions, encryption settings, IAM policies, and CloudTrail logging. Misconfigurations such as publicly accessible storage or unused default accounts are common findings. Auditors may sample CSPM tool results or request read-only access for validation.

ISO/IEC 27001:2022 – Annex A Control 5.23: Auditors evaluate cloud access management, ensuring MFA is enforced for cloud admin accounts, SSO integration is in place, and offboarding procedures include timely revocation of cloud access. Shared accounts or unmanaged credentials are red flags.

COBIT 2019 – DSS05.03 (Monitor Infrastructure for Security Events) & BAI06.05 (Evaluate Change Readiness): Auditors assess how cloud activity is monitored. They review alert configurations for critical events (e.g., new admin account creation), use of DLP controls, and whether cloud logs are regularly analyzed. SaaS tools like Microsoft 365 Secure Score are reviewed for utilization. Cloud changes (e.g., new services or regions) must undergo formal risk assessments, documented in change management logs or risk registers.

ISACA ITAF – Section 2300 (Control Enforcement and Evidence Collection): Auditors inspect how data is protected in cloud. They verify whether data at rest is encrypted, whether encryption keys are customer-managed (BYOK/HSM) or provider-controlled, and how key management (rotation, storage) is handled. Backups are checked for proper access control, isolation, and recovery testing. If client-side encryption is used, key integrity and availability are also assessed.

NIST SP 800-53A – AC-2 (Account Management) & SI-4 (System Monitoring): Auditors ensure cloud accounts are managed like internal systems. They verify account provisioning, activity monitoring, and inclusion in vulnerability management. For IaaS environments, auditors check whether virtual machines are patched, scanned, and monitored with the same rigor as on-premises systems.

ISO/IEC 27701:2021 – Clause 8.2.3 (Processor Compliance in Cloud): For cloud environments processing personal data, auditors confirm GDPR compliance: DPA agreements, SCCs, and data residency controls are validated. Auditors look for incident readiness, including access to provider logs, availability of decryption keys, and evidence of disaster recovery tests (e.g., restoring data off-cloud).

5.24 IS incident management planning and preparation

Attribute	Value
Control Type	Corrective
Information Security Properties	Confidentiality, Integrity, Availability
Cybersecurity Concepts	Respond, Recover
Operational Capabilities	Governance, Information Security Event Management
Security Domains	Defense

Ties to Other Controls

5.25 – Assessment and decision on events: 5.24 provides the foundational incident management framework, including roles, responsibilities, and communication protocols. Without this preparation, the process of evaluating events under 5.25 cannot be performed systematically. For example, 5.24 ensures that when a potential incident is detected, pre-defined escalation paths and response thresholds are in place to allow for timely and consistent assessment and classification.

5.27 – Learning from incidents: Incident management is not complete without a feedback loop. 5.24 mandates that incident response plans incorporate post-incident review activities, such as root cause analysis, documentation of lessons learned, and recommendations for control improvements. These outputs directly support 5.27, turning each incident into an opportunity to enhance security posture and refine preparedness for future events.

8.15 – Logging and 8.16 – Monitoring: Effective incident detection relies on robust logging and real-time monitoring capabilities. 5.24 requires that incident response planning includes alignment with 8.15 and 8.16, ensuring that log data is not only collected but also actionable for responders. *Example*: A Security Information and Event Management (SIEM) system should be configured to generate alerts for anomalous activities, which are then tied into the incident response workflow. 5.24 ensures that such integrations are documented and rehearsed.

5.29 – Security during disruption: Incident planning under 5.24 includes anticipating business disruptions that might arise from security incidents. This supports 5.29, which focuses on maintaining security during disruptive events, ensuring that incident response procedures continue effectively even under degraded conditions.

5.17 – Information security continuity: 5.24 contributes to broader continuity planning by preparing the organization to respond to and recover from security incidents, ensuring that response actions are coordinated with continuity measures like failover protocols and alternative communication channels.

6.3 – Contact with authorities: As part of incident management readiness, 5.24 includes establishing processes for contacting regulatory bodies, law enforcement, or data protection authorities as required by applicable laws. This complements 6.3, ensuring legal and regulatory requirements are integrated into response plans.

ISO Cross-References

ISO/IEC 27035-1:2023 – Clause 7 (Plan and Prepare Phase): Provides foundational principles for information security incident management, including establishing incident response teams (IRT), defining roles and responsibilities, and ensuring tools and resources are available for effective response. 5.24 aligns directly with this by requiring organizations to set up comprehensive incident management frameworks, including training programs, incident classification schemes, and communication protocols.

ISO/IEC 27035-2:2023 – Clause 8 (Incident Management Process): Details the incident handling process, from preparation to lessons learned, supporting 5.24 by defining structured steps for incident readiness. *Example*: Organizations implementing 5.24 based on 27035-2 will have documented processes for incident detection, analysis, response coordination, and post-incident review, ensuring readiness for diverse threat scenarios.

ISO/IEC 22320:2018 – Clause 6 (Incident Response Management): Offers a broader emergency management framework, focusing on command-and-control, decision-making hierarchies, and structured communication during crises. *Example*: For 5.24, this translates into defining an Incident Commander, setting up clear reporting lines, and establishing multi-level coordination mechanisms during significant cyber incidents.

ISO/IEC 27701:2021 – Annex A.8.2.3 (Personal Data Breach Response): Recommends that incident response plans include provisions for privacy breaches, integrating legal notification requirements such as GDPR's 72-hour rule. *Example*: Under 5.24, the organization ensures that data protection officers (DPOs) are part of the incident response team, and that privacy impact assessments are conducted during incidents involving personal data, triggering timely notification to supervisory authorities if required.

ISO/IEC 27001:2022 – Clause 6.1.2 (Information Security Objectives and Planning): Supports the strategic aspect of 5.24, ensuring that incident response readiness is embedded in security objectives, and that resources for incident management are planned and allocated in advance.

ISO/IEC 27005:2024 – Clause 10.2 (Risk Treatment Planning): Guides how incident response capabilities should be based on risk assessments, ensuring that plans under 5.24 are tailored to the organization's specific threat landscape and asset criticality.

Cross-Compliance Mapping

EU NIS2 – Article 26 (Incident Handling) & Article 23 (Incident Notification): NIS2 Article 26 requires all essential and important entities to establish and maintain documented incident handling procedures for managing cybersecurity threats. This includes clear roles, responsibilities, escalation paths, and defined communication channels. Article 23 mandates that significant incidents are reported to competent authorities within specified timeframes. Under Control 5.24, organizations must not only develop a comprehensive incident response plan (IRP) but also ensure it covers identification, evaluation, reporting, and internal/external communications, including regulatory notifications in coordination with Control 6.8. Plans should be updated to incorporate lessons learned from actual incidents and threat intelligence.

EU GDPR – Articles 33 & 34 (Personal Data Breach Notification): GDPR requires organizations to notify the supervisory authority within 72 hours of discovering a personal data breach and, where there is a high risk to individuals, to inform affected data subjects without undue delay. Control 5.24 embeds data breach response into the broader incident management plan, with explicit procedures for assessing breach severity, involving the DPO and legal counsel, and documenting notification decisions. Evidence of regular incident response exercises and tabletop simulations involving breach scenarios demonstrates GDPR accountability and operational readiness to regulators.

EU DORA – Articles 17–21 (ICT-related Incident Reporting and Management): DORA establishes detailed requirements for ICT-related incident management and reporting in the financial sector. Articles 17–21 mandate that organizations: Maintain comprehensive incident response plans, Classify and assess ICT incidents based on predefined criteria, Establish internal escalation, communication, and reporting procedures, Notify competent authorities within specific timelines (e.g., within four hours for major incidents), Conduct post-incident analysis and continuous improvement. Control 5.24 operationalizes DORA requirements by ensuring incident response is a documented, tested, and regularly reviewed process, covering internal escalation, external regulatory notification, and lessons learned integration.

ISO 22301:2019 – Clause 8.4.3 (Response Structure and Integration with BC/DR): Clause 8.4.3 requires organizations to link incident response to business continuity and disaster recovery (BC/DR) planning, ensuring that technical incidents with operational impact (e.g., ransomware) can escalate to BC/DR activation. Control 5.24 mandates integration between incident response and BC/DR plans, with triggers and escalation paths for major incidents. Scenarios should be developed for technical, operational, and reputational threats, and playbooks should delineate when and how to activate business continuity protocols.

NIST Cybersecurity Framework (CSF) – Respond Function (RS.RP, RS.CO, RS.IM): The NIST CSF “Respond” function provides comprehensive expectations for response planning (RS.RP), coordinated communications (RS.CO), and continuous improvement (RS.IM). Control 5.24 operationalizes these by requiring detailed incident response plans, training and awareness for all relevant personnel, communication protocols for internal and external stakeholders, and documented post-incident reviews to drive iterative improvement. Auditors mapping to CSF will expect to see evidence of incident response drills, plan reviews, and regular updates based on emerging threats and organizational changes.

NIST SP 800-53 Rev.5 – IR-1 (Incident Response Policy and Procedures), IR-7 (Incident Response Assistance), IR-8 (Incident Response Plan): IR-1 calls for the establishment and dissemination of formal incident response policies and assignment of clear roles and responsibilities. IR-8 mandates the development, implementation, and regular testing of incident response plans, ensuring all incidents are managed according to documented procedures. IR-7 focuses on providing incident response support (e.g., external experts, managed services), which may be integrated into 5.24 for organizations lacking in-house resources. Control 5.24 aligns by requiring operationalization of plans, dedicated incident response teams, regular exercises (including tabletop and live simulations), and evidence that incidents are detected, responded to, and escalated according to policy.

COBIT 2019 – DSS02.01 (Manage Incident Response), DSS02.03 (Conduct Post-Incident Reviews): COBIT 2019 establishes a governance framework for incident response, requiring organizations to implement structured plans, assign ownership, and conduct regular response exercises (DSS02.01). DSS02.03 mandates that lessons learned from incidents are captured, analyzed, and integrated into process improvements, ensuring the IRP remains current and effective. Control 5.24 supports these objectives by formalizing all aspects of incident planning, detection, escalation, and post-incident learning, supporting both audit and management review.

Audit Methodology Considerations

ISO/IEC 19011:2018 – Clause 6.4.5 (Audit Execution): Auditors examine the incident response plan, assessing its completeness and alignment with best practices. They check whether the plan defines incident types, severity classifications, and clearly assigned roles (incident manager, technical lead, legal, communications). Contact lists, including after-hours escalation paths, must be present. The plan should outline standard operating procedures or at least high-level steps for various scenarios (e.g., data breaches, malware, DDoS). Missing elements such as lack of regulatory reporting instructions or media liaison roles would be flagged.

ISO/IEC 27007:2020 – Clause 7.4.5 (Interviews and Documentation Review): Auditors confirm that an Incident Response Team (IRT) exists and is operational. They interview team members to verify their understanding of responsibilities, and request training records or tabletop exercise reports. Evidence such as incident post-mortems or SANS/GIAC certifications support readiness. Lack of training or drills would indicate poor preparedness.

ISO/IEC 27001:2022 – Annex A Control 5.24: Auditors assess whether necessary tools and resources for incident handling are in place, such as forensic toolkits, incident ticketing systems, contact trees, and alternative communication channels. They check if external partners (e.g., forensic firms, legal, PR) are pre-identified and contracted. Absence of such arrangements could lead to delays during a real incident.

COBIT 2019 – DSS02.04 (Assess and Respond to Security Incidents) & DSS04.02 (Maintain Continuity): Auditors verify that incident plans are tested periodically. They request records of simulations, including the scenario, participants, and corrective actions. They assess whether lessons learned were implemented, showing plan evolution (linked to 5.27). An untested plan is considered high risk.

ISACA ITAF – Section 2300 (Control Enforcement and Evidence Collection): Auditors ensure incident detection mechanisms are integrated with the plan. They verify staff awareness by asking employees how to report an incident. The plan must include reporting channels, and real-world knowledge among employees is assessed. Lack of awareness leads to undetected incidents and is a key audit concern.

NIST SP 800-53A – IR-8 (Incident Response Plan) & IR-4 (Incident Handling): Auditors review escalation procedures and whether internal/external communications are covered, including law enforcement notifications, regulatory reporting, and client notifications. They validate that GDPR reporting timelines (72-hour rule) are accounted for, and that PR strategies exist for reputation management.

ISO/IEC 22301:2019 – Clause 8.4.3 (Response Structure): Auditors evaluate how incident response integrates with Business Continuity (BC) and Disaster Recovery (DR) plans. They review whether the plan includes triggers for BC/DR engagement, such as major ransomware events. Combined drills or documented liaison protocols between incident managers and BC managers provide strong evidence of coordination.

5.26 Response to information security incidents

Attribute	Value
Control Type	Corrective
Information Security Properties	Confidentiality, Integrity, Availability
Cybersecurity Concepts	Respond, Recover
Operational Capabilities	Information Security Event Management
Security Domains	Defense

Ties to Other Controls

5.24 – Information security incident management planning and preparation & 5.25 – Assessment and decision on information security events: 5.26 represents the execution phase of the incident management lifecycle. After an event is classified as a security incident through 5.25, and with predefined procedures and roles established in 5.24, 5.26 drives containment, eradication, and recovery activities. The quality and effectiveness of 5.26 are heavily dependent on the clarity and robustness of planning and assessment stages.

5.27 – Learning from information security incidents: While 5.26 focuses on the immediate actions needed to mitigate an incident, it naturally transitions into 5.27, where post-incident analysis takes place. An effective 5.26 process concludes with a wrap-up report, outlining the timeline, actions taken, and initial findings, which form the basis for root cause analysis and continuous improvement under 5.27. A well-structured incident response is incomplete without feeding into organizational learning.

5.30 – ICT readiness for business continuity: During severe incidents, such as ransomware or DDoS attacks, 5.26 may trigger business continuity or disaster recovery mechanisms. Response teams must recognize when to escalate from security containment to activating BC/DR plans, ensuring minimal disruption to critical services. 5.26 and 5.30 must be aligned, with clear transition points from incident response to continuity operations, ensuring coordination between technical teams and BC managers.

5.29 – Security during disruption: While handling the incident, especially during extended containment or recovery, 5.26 ensures that security controls remain effective even in degraded states. If systems are isolated, reverted to backups, or run in reduced capacity, 5.26 ensures that temporary measures still maintain security integrity until full recovery.

5.5 – Contact with authorities: 5.26 often involves external communications, including law enforcement, regulators, or industry partners. The response process must align with 6.3, ensuring timely notifications and cooperation with external stakeholders, especially in jurisdictions requiring mandatory reporting.

8.15 – Logging & 8.16 – Monitoring: Effective incident response requires access to logs and monitoring data to support containment and forensic analysis. 5.26 relies on these inputs to identify attack vectors, assess the scope of compromise, and validate eradication efforts.

ISO Cross-References

ISO/IEC 27035-2:2023 – Clause 8.4 (Response Phase): Defines the core response activities after an incident is confirmed, covering containment, eradication, and recovery. 5.26 is directly mapped to this phase, requiring organizations to implement structured containment strategies (e.g., isolating affected systems, disabling compromised accounts), followed by eradication measures (e.g., malware removal, vulnerability patching), and recovery procedures (e.g., restoring from secure backups, validating system integrity). *Example*: A ransomware attack would prompt 5.26 actions such as disconnecting infected systems, running malware scans, applying patches, and restoring data from verified backups, ensuring normal operations resume securely.

ISO/IEC 27035-3:2020 – Clause 7 (Incident Coordination and Communication): Provides guidance on coordinating response efforts across internal teams and with external stakeholders. 5.26 includes operationalizing the communication plans developed under 5.24, ensuring timely engagement with law enforcement, regulatory bodies, and third-party partners when applicable. *Example*: In a data breach involving third-party systems, 5.26 ensures that all affected entities are promptly notified, evidence is preserved, and collaborative mitigation efforts are initiated, as outlined in ISO 27035-3.

ISO/IEC 24762:2008 (now reflected in ISO 22301:2019 – Clause 8.4.4 Recovery): Though superseded, ISO 24762 provided focused guidance on IT disaster recovery, now embodied in ISO 22301. 5.26 includes invoking disaster recovery measures for severe incidents (e.g., full system compromise). Example: If an incident renders primary systems inoperable, 5.26 may involve transitioning to a DR site, restoring from backups, and validating restored services coordinating closely with business continuity teams.

ISO/IEC 22320:2018 – Clause 8.2 (Response Management): Offers general emergency management principles applicable during critical incidents, emphasizing command structures, resource mobilization, and stakeholder coordination. 5.26 integrates these principles, ensuring that response activities are controlled, timely, and well-communicated, particularly during large-scale cyber events.

ISO/IEC 27001:2022 – Clause 6.1.3 (Risk Treatment) & Clause 8.1 (Operational Control): Supports 5.26 by requiring that incident response controls be effectively implemented, monitored, and maintained to ensure operational resilience during incidents.

Cross-Compliance Mapping

EU GDPR – Articles 33 & 34 (Breach Mitigation and Notification): GDPR requires not only notification of personal data breaches but also effective actions to mitigate their effects and prevent recurrence. Article 33 specifies that organizations must “address the breach,” while Article 34 emphasizes minimizing risks to data subjects. Control 5.26 operationalizes this by requiring documented procedures to contain and remediate breaches, such as disabling compromised accounts, patching vulnerabilities, restoring affected data or systems, and communicating protective measures to impacted individuals. Regulators will assess the effectiveness and timeliness of mitigation actions to determine if organizations fulfilled their duty to protect data subjects and limit harm.

EU NIS2 – Articles 23 & 26 (Incident Response and Continuity Minimization): NIS2 mandates that essential and important entities possess mature incident response and business continuity processes, with clear procedures for rapid containment and mitigation. Article 23 requires prompt reporting and action on significant incidents, while Article 26 focuses on limiting service disruption and restoring normal operations. Under Control 5.26, organizations must demonstrate that incidents are systematically contained and remediated, showing regulators step-by-step evidence of the actions taken, from initial detection to final resolution. Delayed or inadequate response can result in regulatory findings and sanctions, especially if preventable escalation or prolonged disruption occurs.

EU DORA – Article 18 (Incident Response and Testing Requirements): DORA requires financial entities to maintain comprehensive incident response plans, regularly test these plans (e.g., through cyber war-gaming or tabletop exercises), and provide evidence of effective execution during actual incidents. Control 5.26 ensures the organization can immediately contain incidents that threaten critical financial services, document every step (from system isolation to patch deployment and communication with regulators), and incorporate lessons learned for continual improvement. Auditors will look for documented runbooks, automated response playbooks, and evidence of response actions during both simulated and real incidents.

NIST SP 800-53 Rev.5 – IR-4 (Incident Handling), IR-9 (Information Spillage Response): IR-4 requires organizations to follow structured incident handling procedures covering containment, eradication, and recovery for every security incident. Control 5.26 directly aligns, mandating comprehensive documentation of all phases within incident tickets and reports. For incidents involving information spillage (e.g., classified data or PII leaks), IR-9 applies, requiring immediate containment, detailed documentation, notification to authorities, and assurance that all data remnants are sanitized and systems are restored. Auditors will expect to see clear evidence of systematic incident handling, full remediation, and verification that affected data or systems cannot be further exploited.

COBIT 2019 – DSS02.01 (Manage Incident Response), DSS02.04 (Mitigate and Recover from Incidents): COBIT 2019 explicitly requires organizations to implement robust incident response processes, including documented procedures for incident containment, mitigation, and recovery (DSS02.01). DSS02.04 emphasizes the need to restore services, analyze root causes, and implement corrective actions to prevent recurrence. Control 5.26 supports these objectives by requiring organizations to execute and document response actions, ensure prompt service restoration, and conduct follow-up analysis to enhance future preparedness and resilience.

Audit Methodology Considerations

ISO/IEC 19011:2018 – Clause 6.4.5 (Audit Execution): Auditors review incident case studies by examining incident reports from recent or significant events. They assess whether the response followed documented procedures, and whether containment, eradication, and recovery actions were timely and effective. *Example*: In a malware incident, auditors verify that affected systems were isolated promptly, malware was removed, systems were rebuilt or reimaged, and normal operations were restored from verified backups. Delays or deviations from procedures are flagged unless justified and documented.

ISO/IEC 27007:2020 – Clause 7.4.5 (Interviews and Documentation Review): Auditors confirm if containment strategies were pre-defined and appropriately executed. They may interview incident responders with questions such as, "What's your immediate action when ransomware is detected?" Expectation: responders can cite network isolation, system shutdowns, or automated containment via EDR tools. Auditors assess if containment delays allowed the incident to spread, and may recommend enhancements like network segmentation or automated response systems.

ISO/IEC 27001:2022 – Annex A Control 5.26: Auditors evaluate forensic analysis and eradication efforts. They check for root cause determination (e.g., phishing vector, vulnerable software) and whether those causes were addressed. Eradication actions should be thorough closing exploited vulnerabilities, removing attacker persistence mechanisms, and applying patches. If reports fail to document these, it raises concerns about incident recurrence.

COBIT 2019 – DSS02.06 (Respond to Incidents) & DSS04.02 (Maintain Continuity): Auditors assess recovery and validation actions. Systems should be rebuilt from trusted sources, and data integrity must be verified. Evidence of post-recovery monitoring for signs of residual compromise is expected. If recovery actions missed steps (e.g., failure to restart security controls or verify restored data), auditors note operational risk.

ISACA ITAF – Section 2300 (Control Enforcement and Evidence Collection): Auditors check communication logs to verify if key stakeholders (executives, regulators, customers) were informed promptly. Compliance with regulatory reporting timelines is assessed (e.g., GDPR's 72-hour rule). Failure to notify authorities or customers as required, or delayed reporting, is noted as a compliance breach.

NIST SP 800-53A – IR-4 (Incident Handling) & IR-6 (Incident Reporting): Auditors assess if external support (forensics, legal, PR) was pre-arranged and activated effectively. They check if the organization has a retainer with a third-party incident response firm and whether such support was engaged swiftly and smoothly. Lack of external readiness is seen as a vulnerability.

ISO/IEC 27035-3:2020 – Clause 8 (Evidence Handling): Auditors ensure evidence collection procedures are in place. For significant incidents, system logs, disk images, and other forensic data should be preserved before remediation. *Example*: Responders should articulate that for critical hosts, imaging or log preservation is standard before system reinstallation. Lack of evidence handling risks undermining forensic investigations or legal actions.

ISO/IEC 27035-2:2023 – Clause 8.4 (Containment, Eradication, Recovery): Auditors compare actual response to the documented plan. Deviations must be justified and documented. Frequent unplanned deviations suggest either inadequate planning or lack of training. Plans may need revision or teams retraining.

ISO/IEC 22301:2019 – Clause 8.4.4 (Recovery Planning): Auditors assess multi-team coordination during incidents. Effective collaboration between IT, security, legal, PR, and business units is evaluated. Siloed responses are discouraged. Evidence includes meeting records, war room logs, or multi-disciplinary debrief reports.

6.3 Information Security Awareness, Education and Training

Attribute	Value
Control Type	Preventive
Information Security Properties	Confidentiality, Integrity, Availability
Cybersecurity Concepts	Protect
Operational Capabilities	Human Resource Security
Security Domains	Governance and Ecosystem

Ties to Other Controls

5.2 – Information Security Roles and Responsibilities: Once roles are defined under 5.2, 6.3 ensures that personnel receive appropriate awareness and training tailored to those roles. For instance, a person assigned as a data custodian would need specific training on data classification and handling relevant to their responsibilities.

6.1 – Screening: While 6.1 ensures that only qualified and trustworthy individuals are hired, 6.3 is responsible for shaping those individuals' behaviors post-hire by embedding knowledge of internal policies, acceptable practices, and specific security responsibilities. Without robust awareness training, even a well-screened employee may inadvertently pose a risk.

6.8 – Information Security Event Reporting: Although outside the current scope, 6.8 fundamentally depends on 6.3. Employees need awareness to recognize security incidents or weaknesses and must be educated on how and when to report such events effectively.

8.16 – Monitoring Activities: Staff involved in monitoring security events, logs, or performance indicators must be trained not only in the use of monitoring tools but also in recognizing anomalies and following response protocols. 6.3 ensures these operational tasks are performed competently through targeted training programs.

5.36 – Compliance with Policies, Rules, and Standards for Information Security: Compliance is contingent upon awareness. 6.3 ensures that employees are aware of security policies and understand their personal responsibility in adhering to them. Regular education and training mitigate the risk of unintentional policy breaches due to ignorance.

5.1 – Policies for Information Security: For policies to be effective, they must be communicated and understood by all personnel. 6.3 acts as the mechanism for policy dissemination, ensuring that staff understand the intent and requirements of the ISMS.

6.4 – Disciplinary Process: Awareness of consequences plays a preventative role. 6.3 includes training on acceptable behaviors and the repercussions of non-compliance, which reinforces 6.4 by ensuring personnel are informed about the disciplinary process for security breaches.

ISO Cross-References

ISO/IEC 27001:2022 – Clause 7.3 (Awareness): This clause mandates that persons doing work under the organization's control are aware of the information security policy, their role in contributing to the effectiveness of the ISMS, and the implications of not conforming. Control 6.3 operationalizes this requirement by establishing structured awareness campaigns, targeted role-based training, and ongoing education to ensure personnel understand their responsibilities and comply with security objectives.

ISO/IEC 27005:2024 – Clause 8.2.2 (Human Factor Risks): The standard highlights that human-related risks (e.g., phishing, social engineering, negligent behavior) are key risk sources and require appropriate risk treatments. Control 6.3 directly addresses this by mitigating human error through awareness and training, which 27005 recognizes as essential for risk treatment strategies aimed at reducing likelihood and impact of human-caused incidents.

ISO/IEC 27701:2021 – Clause 7.2.2 (Awareness, Education and Training): This clause requires that personnel involved in PII processing are made aware of privacy obligations, including data subject rights and secure handling of personal data. 6.3 should therefore extend beyond general security awareness to include privacy-specific content, ensuring that staff understand both the organizational privacy policies and external legal frameworks like GDPR.

ISO/IEC 27017:2021 – Clause 10.1.2 (Training and Awareness for Cloud Security): The standard advises that both cloud service providers and customers ensure relevant staff are trained in cloud-specific risks and security practices. Control 6.3 aligns by integrating cloud security topics into the awareness program, such as safe configuration of cloud services, shared responsibility models, and securing cloud credentials.

ISO/IEC 27018:2019 – Clause 9.1.1 (Training on PII Protection in Cloud Environments): It recommends that individuals involved in the processing of PII in cloud systems receive training on privacy and security. Implementing 6.3 in a cloud context means including content on secure cloud operations and PII protection within the organization's training regime, ensuring compliance with ISO 27018's cloud privacy requirements.

ISO/IEC 27035-1:2023 – Clause 6.3 (Awareness for Incident Management): This clause underlines the necessity of raising awareness on recognizing and reporting incidents. Control 6.3 ensures that employees are trained to detect early signs of incidents and understand the reporting mechanisms, which is foundational for initiating the incident response process as detailed in ISO 27035.

Cross-Compliance Mapping

EU GDPR – Articles 39(1)(b) and 47 (Binding Corporate Rules): Article 39 mandates that Data Protection Officers (DPOs) ensure training and awareness for personnel involved in personal data processing. This includes raising awareness of data protection obligations and risks among staff. Control 6.3 supports GDPR compliance by ensuring that all employees, particularly those handling PII, receive periodic and role-appropriate privacy and security training. Article 47 extends this requirement under Binding Corporate Rules, highlighting the need for structured training programs to embed privacy within corporate culture. Through 6.3, organizations can demonstrate that they maintain an informed workforce capable of safeguarding personal data, fulfilling GDPR's expectations for accountability and proactive risk management.

EU NIS2 – Article 21(2)(i): NIS2 explicitly requires that essential and important entities adopt human resources security measures, including policies for security training and awareness. Control 6.3 addresses this mandate by implementing a structured awareness program that educates all staff about cyber hygiene, emerging threats (e.g., phishing, ransomware), and their role in organizational cybersecurity. This extends from basic user awareness to role-specific training for IT and security professionals. By applying 6.3, organizations comply with NIS2's focus on cultivating a workforce that understands and mitigates ICT risks, contributing directly to improved cyber resilience and readiness to handle incidents as required under the directive.

EU DORA – Article 13 (ICT-Related Skills and Training): DORA obliges financial entities to ensure that their staff possess adequate ICT risk management skills. Control 6.3 directly supports this by providing ICT security training tailored to various roles: general staff receive awareness training on threats like phishing, while IT personnel undergo technical training on secure configurations, vulnerability management, and incident response. Managers may receive training on ICT risk governance and crisis management. DORA's focus on digital operational resilience is addressed through 6.3's emphasis on equipping employees with the knowledge necessary to maintain secure, resilient ICT systems, fulfilling both the regulatory expectation for training and the broader goal of maintaining financial stability through secure operations.

NIST SP 800-53 Rev.5 – AT-2, AT-3, AT-4 (Awareness and Training Family): Control 6.3 corresponds directly to AT-2 (Security Awareness Training), which requires all users to receive periodic security awareness training, typically on an annual basis. AT-3 mandates role-based training for individuals with specific security functions, ensuring they understand and can fulfill their responsibilities securely. AT-4 emphasizes maintaining accurate training records as evidence of compliance. A robust 6.3 program maps to these controls by delivering general security training organization-wide and targeted sessions for specialized roles, such as secure coding for developers or incident handling for IT staff. This comprehensive approach ensures human factors are addressed as part of risk mitigation, aligning with NIST's emphasis on people as integral to the security posture.

COBIT 2019 – APO07.03 (Maintain Labor Policies), BAI05.07 (Develop Skills): COBIT APO07.03 requires that labor policies ensure personnel are aware of their responsibilities, including security. Control 6.3 supports this by embedding security training within HR and operational processes. BAI05.07 specifically focuses on developing the skills required to support IT and business objectives, including security capabilities. Through 6.3, organizations implement structured training programs that not only fulfill compliance requirements but also enhance staff capability in managing and responding to ICT risks. Auditors will expect to see that training aligns with business needs and is regularly updated to reflect emerging threats, fulfilling COBIT's governance principle of equipping personnel to execute their duties securely.

Audit Methodology Considerations

ISO/IEC 19011:2018 – Auditors will evaluate both the existence and effectiveness of the awareness program. According to Clause 6.3.1, they start by reviewing the training curriculum, schedules, and materials (e.g., slides, posters, email bulletins). Evidence such as attendance records or completion certificates from e-learning modules will be checked to confirm that training is not only planned but delivered. Clause 7.2(h) stresses that auditors should consider whether the competence of trainers is sufficient – e.g., whether those delivering training are certified or experienced in information security, and whether content is current and reflects evolving threats.

ISO/IEC 27007:2020 – Clause 8.2.2 suggests that beyond paperwork, auditors gauge awareness through interviews. An auditor will interview a cross-section of employees to assess real awareness levels. They may ask simple but telling questions: *"What would you do if you receive a suspicious email?"*, *"Do you know whom to contact if you suspect a security incident?"*, or *"Can you recall any key message from recent security training?"* The goal is to determine if the training "sticks." If employees consistently provide correct, confident answers (e.g., *"I'd report it to the InfoSec team via our incident portal"* or *"Yes, we have annual training, and it emphasized using strong passwords"*), it provides evidence that 6.3 is effective. In contrast, hesitation or incorrect answers suggest that awareness may not be fully embedded.

ISO/IEC 27006:2015 – Clause 9.4.1.3: Certification auditors often trace requirements to implementation. For 6.3, they will check that new hires receive induction training – perhaps by examining induction records for recent employees – and that ongoing training is regularly provided, supported by logs or records from recent awareness campaigns or simulated drills.

COBIT 2019 – APO07 (Manage Human Resources) and APO12 (Risk Management) emphasize building a security-aware culture. An auditor referencing COBIT will look for enterprise-wide initiatives like phishing simulations, newsletters, or workshops as practical implementations of 6.3. They might review results of an internal phishing test – for instance, if 20% of employees initially clicked on a test phishing link and after training that dropped to 5%, that's compelling evidence of improvement through 6.3.

ISACA ITAF – Section 3400 encourages performance auditing. An ITAF-aligned auditor might request metrics the organization collects on its awareness program: training completion rates, quiz scores, incident reporting rates pre- and post-training. If such metrics are collected and analyzed, it shows maturity in 6.3. Auditors will also assess whether these metrics are reviewed by management, and corrective actions are taken – e.g., if a department lags in completion, does management intervene?

NIST SP 800-53A – AT-2 / AT-3: Auditors examine training content and records, ensuring that all staff receive general awareness training and that specialized roles (e.g., system administrators, developers) receive role-based training. For example, they might verify that a database administrator has completed a secure DBA course, not just a general security module.

NIST SP 800-115: Auditors might use creative techniques, such as social engineering calls or tests, to assess if employees apply their training. For instance, calling the helpdesk pretending to be another employee and observing whether helpdesk staff recognize the ploy and follow procedures. While such tests require approval, they reveal real-world preparedness and highlight whether 6.3 is achieving behavioral change.

7.2 Physical Entry

Attribute	Value
Control Type	Preventive
Information Security Properties	Confidentiality, Integrity, Availability
Cybersecurity Concepts	Protect
Operational Capabilities	Physical Security
Security Domains	Protection

Ties to Other Controls

Control 7.2 – Physical Entry governs the authorization, authentication, and supervision of individuals entering secure areas. It directly complements Control 7.1 – Physical Security Perimeters, where 7.1 establishes the boundary, and 7.2 defines how access is granted across that boundary. For example, a perimeter fence (7.1) may include a secured entry point controlled by keycards or biometric scanners (7.2). These controls are inherently co-dependent and are typically implemented as an integrated physical security solution.

Control 7.3 – Securing Offices, Rooms and Facilities builds upon 7.2 by ensuring that, after gaining authorized entry, internal areas remain secured. While 7.2 ensures that only permitted individuals enter, 7.3 mandates that sensitive areas (e.g., server rooms, records storage) are physically protected through structural reinforcements (e.g., sturdy doors, intrusion-resistant walls) and internal locking mechanisms.

Control 7.4 – Physical Security Monitoring is closely tied to 7.2, as entry points are typically monitored through CCTV, access logs, and alarm systems. Monitoring detects anomalies such as forced entry, tailgating, or propped doors, thus enforcing 7.2's preventive function with real-time detection capabilities.

Control 6.5 – Responsibilities After Termination mandates that physical access rights of former employees or contractors are promptly revoked. This directly interfaces with 7.2's requirement for maintaining access control lists and deactivating badges or keys upon termination or role change, ensuring that only current, authorized personnel retain access.

Control 6.1 – Screening and Control 6.2 – Terms and Conditions of Employment ensure that individuals granted access under 7.2 have been vetted and have contractual obligations regarding the responsible use of physical access privileges. 7.2 relies on these controls to ensure only trustworthy, authorized individuals are admitted into secure areas.

Control 5.19 – Information Security in Supplier Relationships and **Control 5.20 – Addressing Security Within Supplier Agreements** tie into 7.2 by requiring that third-party personnel accessing secure areas comply with the organization's entry protocols. For example, contractors may be required to use temporary badges, be escorted, or follow specific visitor procedures outlined in entry control policies.

Control 7.6 – Working in Secure Areas extends 7.2 by defining the expected behavior of individuals inside secure zones. It reinforces entry control integrity by requiring personnel to challenge unrecognized individuals, prevent tailgating, and report suspicious activity, ensuring that access once granted is not misused or circumvented.

Control 8.1 – User Endpoint Devices can relate to 7.2 where equipment is brought into or out of secure areas. Entry controls may require authorization for personal devices, asset tagging, or entry/exit logs to prevent unauthorized equipment from compromising the environment or enabling data theft.

ISO Cross-References

ISO/IEC 27001:2022 – Annex A.7.1: This annex covers both the establishment of secure perimeters and the enforcement of entry controls. Specifically, it mandates that "entry controls shall be in place to ensure that only authorized personnel are allowed access to secure areas." Control 7.2 operationalizes this by requiring detailed authorization procedures, entry logs, and physical access restrictions. During certification audits, compliance with Clause 9.1 (Monitoring, measurement, analysis, and evaluation) and Clause 6.1 (Actions to address risks and opportunities) is assessed, ensuring that physical access is monitored and reviewed for effectiveness. Organizations must maintain a controlled and documented process for granting, modifying, and revoking physical access rights, often tied to HR processes and asset management (related to Clause 8.1). For instance, if secure server rooms are accessible, the auditor expects to see both the entry control mechanisms (7.2) and records of who accessed and when, supporting compliance with both ISO 27001 and ISO 27002 frameworks.

ISO/IEC 27005:2024 – Clause 8.2.4 (Threat Identification), Clause 10.3 (Risk Treatment Planning): This standard identifies unauthorized physical access as a key threat vector, potentially leading to data breaches, theft, or sabotage. In Clause 8.2.4, it categorizes threats such as tailgating, forced entry, or misuse of access privileges. As a risk treatment, Clause 10.3 recommends implementing badge-based access control, biometric systems for high-security zones, and manual verification (e.g., guards at reception). These controls are direct mitigations aligned with 7.2, providing a clear risk-based justification for stringent entry procedures. For example, for areas classified as high-risk due to the nature of data processed (e.g., PII, financial data), the standard supports multi-factor entry control as a treatment measure, reinforcing the principle of proportionality in physical security.

ISO/IEC 27017:2021 – Clause 11 (Cloud Services Physical Security): For cloud service providers, Clause 11 extends ISO 27002's physical security requirements, emphasizing strict entry control to data center facilities. Providers are expected to implement multi-factor authentication for personnel entry, enforce visitor escort policies, and conduct background checks on data center staff. Cloud customers are advised to seek assurances such as ISO/IEC 27001 certification or third-party audit reports confirming that these controls are in place. For organizations using colocation or cloud environments, Control 7.2 is applicable in requiring contractual verification that providers comply with equivalent or stronger physical entry controls. For example, requiring providers to supply access logs for audit or ensuring onsite inspections are permitted strengthens the organization's assurance of 7.2 compliance even when physical assets are hosted externally.

ISO/IEC 27701:2021 – Annex A.8.11 (Access Control to PII Processing Areas): Although 27701 does not introduce new physical control requirements, Annex A.8.11 requires that access to areas where PII is processed is restricted to authorized individuals only, reinforcing the need-to-know principle. This privacy-focused view supports 7.2 by framing physical access as a privacy risk, particularly where unrestricted entry could lead to unauthorized PII exposure. Physical access control mechanisms such as biometric entry or manually signed visitor logs provide evidence that only those with a legitimate role are granted access to PII storage or processing environments, aligning with privacy compliance expectations under ISO 27701.

ISO/IEC 27018:2020 – Clause 11.1 (Protection of PII in Cloud Environments): For cloud providers managing personally identifiable information (PII), this clause mandates stringent physical access controls to prevent unauthorized entry into facilities housing customer data. These controls, as specified in 7.2, include access badges, PIN codes, biometric scanners, and surveillance at all entry points. The clause advises that cloud providers regularly audit access logs and review entry control policies, ensuring that only cleared personnel can access critical data environments. For customers, it emphasizes the importance of verifying these controls, either via audit rights or certification review, particularly when shared responsibility models are in place.

ISO/IEC 27035-1:2023 – Clause 7.3 (Incident Response for Physical Security Breaches): This clause addresses how organizations should respond to unauthorized physical access incidents. It requires that entry control systems (7.2) provide sufficient logging, monitoring, and alerting capabilities to support incident detection and response. In practice, organizations must have visitor logs, badge records, and CCTV footage to investigate any breaches. It also recommends conducting drills for physical intrusions, similar to cyber incident response exercises, to test personnel readiness and control effectiveness. These elements rely on 7.2's proper implementation and documentation to ensure that when incidents occur, timely and effective response is possible.

ISO/IEC 27033-3:2010 – Clause 8.2 (Defense in Depth for Network Security Gateways): This older but conceptually relevant clause draws a parallel between network security perimeters and physical security perimeters. Just as firewalls manage and restrict data flow, physical entry controls manage and restrict human access. The standard reinforces that both physical and network access must be tightly controlled, monitored, and auditable. Control 7.2 reflects this in the physical realm by enforcing layered access (e.g., reception, internal doors, server room locks), supporting comprehensive defense strategies.

ISO/IEC 24764:2010 – Clause 6.3 (Data Center Infrastructure Physical Security): This standard advises on multi-layered physical entry controls for data centers, such as security vestibules, mantraps, and two-factor authentication. While outside the ISO/IEC 27000 series, it provides enhanced guidance for high-security environments where 7.2 applies more stringently. It suggests separation of duties in physical access, restricted access zones, and continuous monitoring, aligning with and strengthening 7.2 for organizations with critical infrastructure.

Cross-Compliance Mapping

EU GDPR – Articles 5(1)(f), 24, 32: GDPR requires that personal data be protected against unauthorized access, including physical access. Article 32(1)(b) mandates "access control" measures to ensure data security, which logically extends to physical access restrictions for areas housing personal data. For example, if HR records are stored in a filing room, only HR personnel should have physical access. Control 7.2 ensures this by requiring authorization mechanisms such as electronic locks, badge access, and visitor logging. Article 24 (Accountability) further requires that organizations can demonstrate these controls are effective; access logs generated from 7.2 serve as compliance evidence. In case of a data breach involving physical intrusion, regulators assess whether entry controls were in place strong 7.2 implementation could mitigate fines under Article 83. Recital 39 also supports this by emphasizing the protection of processing systems against unauthorized access, highlighting that physical entry control directly supports GDPR's integrity and confidentiality principles.

EU NIS2 – Article 21(2)(d), Article 23(1): NIS2 mandates "appropriate and proportionate technical, operational, and organizational measures" including physical security to protect network and information systems. Article 21(2)(d) explicitly includes physical and environmental security, making Control 7.2 essential for sectors such as healthcare, energy, and digital infrastructure. Uncontrolled physical access can enable sabotage, unauthorized device connection, or malware planting. For instance, a control room where critical infrastructure is managed must be restricted to authorized personnel only; entry controls like badge readers or security guards enforce this. Additionally, NIS2's focus on supply chain risk means that third-party access is also under scrutiny visitor verification, escort policies, and access logging for contractors are part of 7.2's scope. If a third-party technician is allowed into a server room without controls, it constitutes a compliance gap under NIS2. Article 23(1) on incident notification includes physical breaches; well-documented 7.2 controls can demonstrate due diligence, reducing regulatory exposure.

EU DORA – Articles 5(1), 10(1), 18(1): DORA requires financial entities to ensure that ICT systems, including their physical environments, are secured against unauthorized access. Article 10(1) mandates protection of "all ICT systems and their supporting infrastructure," which includes controlling entry to data centers, trading floors, and backup sites. Control 7.2 ensures only authorized personnel can access these environments, using multi-factor access controls, security guards, or biometric verification. Article 5(1) emphasizes management responsibility for enforcing operational resilience, which includes maintaining strong entry control policies and testing them regularly. For example, scenario testing involving lost badge procedures or tailgating simulations aligns with DORA's resilience testing requirements. If a breach occurs, Article 18(1) mandates that physical intrusions be reported as incidents. Demonstrating robust 7.2 controls like maintained visitor logs, incident response protocols, and regular audits can mitigate penalties by proving adherence to DORA's preventive security posture.

NIST SP 800-53 Rev.5 – PE-2, PE-3, PE-8: Control 7.2 maps directly to NIST's PE-2 (Physical Access Authorizations), which requires organizations to define, document, and manage access to secure areas, including reviewing access rights periodically. Auditors expect to see a maintained list of individuals authorized to enter each secured zone and procedures for revoking access upon job changes or termination. PE-3 (Physical Access Control) mandates enforcement at entry points, such as card readers, biometric scanners, or guards verifying identity. Control 7.2 ensures these are in place, operational, and audited. PE-8 (Visitor Access Records) complements 7.2's visitor management by requiring detailed logging of all guest entries, including escort details and visit purpose. For example, a properly implemented 7.2 control would allow an organization to produce detailed reports showing who accessed the data center, when, for what reason, and who authorized and monitored the visit. This level of detail is essential in NIST compliance audits, particularly under federal contracting environments. Implementing 7.2 ensures organizations satisfy physical access requirements critical for FISMA or FedRAMP alignment.

COBIT 2019 – DSS05.02, DSS01.04, BAI03.03: DSS05.02 (Manage Physical Security) requires organizations to control physical access to IT environments, aligning directly with 7.2's principles. COBIT auditors will verify that entry controls are in place, including authorization procedures, visitor logging, and enforcement mechanisms like guards or CCTV. DSS01.04 (Manage Availability and Capacity) supports physical entry control by emphasizing the protection of critical systems from unauthorized physical disruption. For example, restricting access to data centers or server rooms ensures that operational availability is not compromised by unauthorized interference. BAI03.03 (Maintain Standards for Security) ties into how entry control policies are developed, maintained, and enforced, with periodic reviews to assess their effectiveness. A properly implemented 7.2 control allows the organization to demonstrate alignment with COBIT's governance objectives, providing evidence of responsible security management through documented processes, periodic access reviews, and incident handling for physical breaches.

Audit Methodology Considerations

ISO/IEC 19011:2018 – Clause 6.5.4 (Observation), Clause 6.5.6 (Review of Documentation), Clause 6.5.7 (Interviews): Auditors begin by reviewing the documented policy for physical entry control. They examine written procedures detailing who approves access, how visitor management is handled, and how authorization levels are defined (e.g., office access vs. restricted labs). Clause 6.5.4 enables observation of actual practice: auditors may conduct walkthroughs to see if staff follow entry control procedures. For instance, auditors test reception protocols do receptionists verify IDs, issue visitor badges, and notify hosts? Clause 6.5.7 permits interviews with facilities managers about badge issuance, and with employees regarding what they do if they see someone without a badge. Auditors compare observed behaviors against policy: if staff fail to challenge unescorted visitors, that's a non-conformity. Clause 6.5.6 supports document review, such as visitor logs, badge assignment records, and incident reports involving physical access. Evidence-based findings rely on whether the documented processes are actively enforced, ensuring that Control 7.2 is not just a paper policy but a living practice within the organization.

ISO/IEC 27007:2020 – Clause 7.4 (Conducting the Audit), Clause 7.5.2 (Interviews), Clause 7.5.4 (Document Review): Auditors conduct detailed interviews with security personnel, HR, and IT administrators. They ask how access rights are granted, reviewed, and revoked, ensuring alignment with HR processes for terminations. Auditors inspect physical entry controls: card readers, biometric scanners, and alarm systems. They verify if these controls are fail-secure (remain locked during power loss), and whether alerts are generated for forced entries. Live tests may include adding and revoking a badge, checking the response time. Auditors also review access control logs, sampling a list of authorized individuals for high-security zones. They verify that all listed individuals are active employees and still require access. Any discrepancies such as an ex-employee still listed are noted. Auditors assess whether visitor records are complete, with check-in/check-out times, host identification, and whether visitors were escorted. Corrective actions for past access-related incidents are evaluated, confirming that lessons were applied. Control 7.2 is deemed effective if entry processes are consistently applied, monitored, and auditable.

ISO/IEC 27006:2020 – Clause 9.4.2 (On-Site Verification), Clause 9.4.5 (Consistency Across Sites), Clause 9.4.7 (Corrective Action Follow-Up): Certification auditors assess whether secure areas across all in-scope locations implement 7.2 consistently. They may select a sample of sites to inspect entry control mechanisms. Differences in visitor logging practices or badge issuance among sites could result in non-conformities. Auditors cross-reference the risk assessment findings do higher-risk areas have enhanced entry controls, such as mantraps or dual-authentication? They review incident reports: if prior breaches occurred (e.g., tailgating or unsecured doors), did the organization conduct root cause analysis and implement corrective measures? Clause 9.4.7 supports evaluating whether such incidents led to policy updates, staff training, or technical upgrades. Auditors also review the Statement of Applicability to confirm 7.2 is marked as implemented, and validate the description (e.g., "badge-only access with CCTV monitoring") during site inspections. Inconsistencies or failure to act on known access weaknesses jeopardize certification outcomes, as continuous improvement is a requirement under ISO/IEC 27001:2022 – Clause 10.

COBIT 2019 – DSS05.02 (Manage Physical Security), APO13.01 (Establish and Maintain Security Policies), DSS01.04 (Manage Availability and Capacity): Auditors examine how physical access aligns with COBIT's security governance. Under DSS05.02, they assess key management practices for physical keys who holds keys, how they're stored, and whether access is logged. For electronic access, they evaluate whether metrics (e.g., unauthorized access attempts per quarter) are tracked, and whether policy enforcement is reviewed by management. APO13.01 supports evaluating whether physical entry control policies are integrated into the enterprise security strategy, with clear responsibilities and periodic reviews. Under DSS01.04, auditors assess whether physical entry controls contribute to availability objectives, such as preventing system disruptions from unauthorized physical interference. For example, server room access should be limited to prevent downtime from accidental or malicious actions. Audits focus on whether control ownership, monitoring, and improvement align with COBIT's emphasis on accountability and value delivery.

ISACA ITAF (4th Edition) – Standard 1205 (Evidence Gathering), Guideline 2203 (Testing Controls): Auditors use evidence-based testing to assess 7.2. They select random days to review entry logs, verifying that all entries correspond to authorized badges. Visitor logs are examined for completeness: did all visitors sign in, wear badges, and leave as documented? Auditors might conduct a simulated access test, sending someone without a badge to observe if staff challenge unauthorized presence. This tests the security culture and policy adherence. ITAF emphasizes documenting each audit step auditors collect screenshots of access lists, note badge serial numbers, and cross-reference with HR records. Discrepancies, like an inactive employee still having access, result in findings. ITAF requires traceable documentation, ensuring that audit conclusions are supported by verifiable data and that organizations can reproduce results during follow-ups or regulator inspections.

NIST SP 800-53A – PE-2, PE-3, PE-8: Assessors examine physical access authorization lists, ensuring they are up-to-date and reviewed periodically. They inspect visitor logs and access violation reports, verifying that corrective actions followed past incidents. Interviews with guards or receptionists cover procedures for lost badges, verbal access requests, and identity verification. Observations include entry point monitoring during high-traffic periods to detect tailgating. Walk-throughs help validate whether controls match policies if policies specify biometric + PIN for server rooms, assessors expect to see those in place. Testing includes attempts to use expired badges and requesting after-hours access logs to verify system alerting and logging accuracy. Anomalies trigger deeper investigation, ensuring Control 7.2 functions in both routine and exceptional circumstances.

NIST SP 800-115 – Section 5.3 (Physical Penetration Testing), Section 6.4 (Social Engineering): Testers conduct authorized simulations to test 7.2's resilience. Common tests include tailgating, using counterfeit badges, or bypassing access through delivery docks. Employee response is observed do they report intruders or allow breaches? Testers may attempt to access waste disposal areas or loading zones, identifying secondary entry vulnerabilities. If side doors or maintenance areas lack proper controls, findings are logged. Auditors reviewing these pentest reports assess the severity of findings and the organization's remediation plans. Recurrent issues, like unlocked secondary doors, reflect systemic weaknesses in 7.2 implementation. Auditors expect documented evidence of tests, findings, and corrective actions, ensuring continuous strengthening of entry controls.

8.8 Management of Technical Vulnerabilities

Attribute	Value
Control Type	Preventive
Information Security Properties	Confidentiality, Integrity, Availability
Cybersecurity Concepts	Identify, Protect
Operational Capabilities	Threat and vulnerability management
Security Domains	Governance and Ecosystem, Protection, Defense

Ties to Other Controls

Control 8.7 – Protection Against Malware: Vulnerability management and anti-malware form a complementary defense mechanism. While anti-malware tools detect and block known malicious code, patching removes exploitable weaknesses that malware may leverage. Unpatched systems are more susceptible to infection, and many malware variants target specific vulnerabilities.

Control 8.9 – Configuration Management: Proper configuration baselines include ensuring systems are patched to current levels. Vulnerability assessments often reveal configuration deviations or missing updates. Control 8.8 depends on configuration management to maintain secure states, while 8.9 relies on vulnerability findings to refine and enforce secure configurations.

Control 8.32 – Change Management: Applying patches is a controlled change. A robust vulnerability management program integrates with change management to ensure patches are tested, approved, and deployed systematically. Emergency patching follows expedited change processes, balancing security urgency with operational stability.

Control 8.1 – User Endpoint Devices and Control 5.10 – Acceptable Use: Endpoints are frequent targets due to their exposure. Control 8.8 ensures endpoints receive regular patches, while acceptable use policies (5.10) restrict user actions that could introduce vulnerabilities, such as installing unauthorized software. User compliance supports the effectiveness of vulnerability remediation.

Control 5.7 – Threat Intelligence: Effective vulnerability management prioritizes based on real-world threats. Threat intelligence informs which vulnerabilities are actively exploited, guiding patch prioritization. Control 8.8 uses this intelligence to focus resources where they mitigate the highest risks.

Control 8.16 – Monitoring Activities: Continuous monitoring may reveal attempts to exploit unpatched vulnerabilities. IDS/IPS, SIEM, or endpoint detection tools provide real-time data, which feeds back into the vulnerability management cycle. Observed exploitation attempts should escalate patch urgency.

Control 8.26 – Secure Development Practices: Vulnerabilities exist not only in third-party software but also in internally developed applications. Control 8.8 encompasses patching and remediation within custom codebases. Development teams integrate secure coding standards and conduct code reviews and vulnerability assessments as part of this broader management.

Control 5.25 – Assessment of Information Security Events and Control 5.26 – Incident Response: Many incidents trace back to unpatched vulnerabilities. Security event assessments should determine whether lack of vulnerability management contributed to an event. Incident post-mortems often highlight the need to improve patch management processes, including faster remediation and better vulnerability tracking.

ISO Cross-References

ISO/IEC 27005:2024 – Clause 8.2.3 (Vulnerability Identification) and Annex A (Risk Scenarios Involving Unpatched Systems): ISO/IEC 27005 explicitly recognizes unpatched vulnerabilities as a core contributor to information security risks. Clause 8.2.3 outlines that vulnerabilities in software, firmware, and hardware when not mitigated can lead to severe impacts, particularly when exploited by known threats. Annex A includes risk scenarios where systems become compromised due to delayed or absent patching. ISO/IEC 27005 recommends that organizations assess the *window of exposure*, i.e., the period between a vulnerability being known and it being remediated. Control 8.8 acts as a direct risk treatment for these vulnerabilities, ensuring timely identification, prioritization based on risk, and remediation through patching or compensating controls. ISO/IEC 27005 further advises organizations to incorporate vulnerability data from threat intelligence sources to adjust risk ratings dynamically, ensuring that critical vulnerabilities are closed promptly.

ISO/IEC 27017:2021 – Clause 12.6.1 (Technical Vulnerability Management in Cloud Contexts): ISO/IEC 27017, tailored for cloud environments, builds on the baseline of ISO/IEC 27002 and emphasizes shared responsibility in vulnerability management. Clause 12.6.1 requires cloud service customers and providers to clearly define roles in patching cloud infrastructure, platforms, and software layers. For instance, providers typically patch physical hosts and hypervisors, while customers patch virtual machines and applications. Control 8.8 aligns with this by requiring organizations using cloud services to engage providers in vulnerability disclosure, patching timelines, and security bulletins. ISO/IEC 27017 also recommends that customers demand transparency on vulnerabilities affecting their environments and assess providers' patch management processes as part of contractual and security due diligence. This standard amplifies Control 8.8's significance in cloud operations, where patching responsibilities can span multiple stakeholders and misalignment can leave critical gaps.

ISO/IEC 27701:2021 – Clause 6.8 (PII Protection Through Secure Systems): Although ISO/IEC 27701 does not explicitly define vulnerability management controls, it inherits ISO/IEC 27002's requirements, including Control 8.8, to ensure PII protection. Clause 6.8 emphasizes that PII processors and controllers must maintain secure environments to prevent unauthorized access or data breaches. Unpatched vulnerabilities in systems handling PII represent a significant privacy risk, as exploitation can lead to breaches triggering legal consequences. Control 8.8 supports compliance by ensuring that systems storing or processing PII are continuously assessed for vulnerabilities and remediated swiftly. Auditors referencing ISO/IEC 27701 would expect to see that technical vulnerabilities are tracked and addressed, aligning with privacy principles like *integrity* and *security of processing* under regulations such as GDPR.

ISO/IEC 27035-2:2023 – Clause 7.2 (Incident Prevention and Vulnerability Management): ISO/IEC 27035-2 reinforces the preventive aspect of vulnerability management. Clause 7.2 outlines that an effective incident prevention framework must include systematic vulnerability identification, assessment, and remediation processes. This includes both reactive patching of newly disclosed vulnerabilities and proactive scanning for latent issues in existing infrastructure. Control 8.8 is highlighted in this context as an enabler of security incident reduction by closing known vulnerabilities, organizations pre-empt exploitative events. Additionally, ISO/IEC 27035-2 recommends that vulnerability management be integrated with incident response planning: when vulnerabilities are exploited, post-incident analysis should improve patching workflows and reduce time to remediation. Continuous improvement cycles (Clause 10.1) emphasize using incident data to strengthen vulnerability controls.

ISO/IEC 27018:2020 – Clause 10.1 (Security Controls for PII in Cloud Services): While ISO/IEC 27018 does not list specific vulnerability management clauses, it implies their necessity in protecting cloud-hosted PII. Clause 10.1 recommends that cloud providers apply timely patches to systems hosting PII and that customers ensure their client-side components are equally secured. Control 8.8, when applied, ensures both parties reduce risks of PII breaches through unaddressed technical flaws. The standard further suggests that security measures, including patch management, be demonstrable to data controllers and regulators, reinforcing transparency and accountability in privacy-centric environments.

ISO/IEC 27033-1:2015 – Clause 9.3.6 (Vulnerability Management in Network Security): This standard addresses network security architecture and specifically links vulnerability management to network-level controls. Clause 9.3.6 advises that organizations perform regular vulnerability assessments on network devices (e.g., firewalls, routers, switches), including penetration testing to uncover technical weaknesses. Control 8.8 applies directly here, as vulnerabilities in network infrastructure are commonly targeted by attackers. ISO/IEC 27033-1 suggests integrating vulnerability scans with configuration management and ensuring that vulnerabilities in routing protocols, VPN configurations, and network segmentation are promptly mitigated. It also recommends using threat intelligence to adapt vulnerability management policies based on the latest network-based attack vectors.

ISO/IEC 27034-1:2011 – Clause 9.2.4 (Application Security and Vulnerability Remediation): This standard focuses on application security and highlights vulnerabilities in software development lifecycles. Clause 9.2.4 requires that identified vulnerabilities in custom or third-party applications be managed systematically. Control 8.8 supports this by ensuring that software vulnerabilities such as those revealed in code reviews, static/dynamic analysis, or reported via CVEs are logged, risk-assessed, and patched. Vulnerability management extends beyond infrastructure to include code-level weaknesses, requiring developers to follow secure coding and remediation practices. ISO/IEC 27034 mandates integrating vulnerability management with development pipelines (e.g., DevSecOps), ensuring secure software release cycles.

ISO/IEC 27031:2011 – Clause 6.3.2 (ICT Continuity and Vulnerability Mitigation): Within the ICT readiness for business continuity context, ISO/IEC 27031 identifies vulnerabilities as potential disruptors to critical ICT services. Clause 6.3.2 highlights the need for prevention through timely patching and securing infrastructure that supports resilience. Control 8.8 ensures that vulnerabilities are not only identified but managed in a way that supports service continuity, particularly for systems supporting essential business functions. Vulnerability management is seen as a pre-incident measure that strengthens the continuity posture, preventing outages caused by exploitation.

ISO/IEC TS 27008:2019 – Clause 8.2.3 (Assessment of Vulnerability Management Controls): This technical guidance for auditors provides specific methods for evaluating vulnerability management. Clause 8.2.3 recommends that auditors assess whether vulnerability scanning tools are in place, whether scan results are reviewed, and whether patch deployment timelines are reasonable. Control 8.8 must be demonstrable through audit trails showing how vulnerabilities are detected, risk-rated, and remediated. ISO/IEC TS 27008 reinforces the need for evidence-based validation, including records of emergency patch deployments and historical response to critical vulnerabilities (e.g., zero-days).

ISO/IEC 27019:2020 – Clause 9.2.1 (Vulnerability Management in Energy Sector Systems): Tailored for energy utility environments, ISO/IEC 27019 mandates strict management of vulnerabilities in industrial control systems (ICS) and SCADA environments. Clause 9.2.1 requires regular vulnerability assessments for field devices, programmable logic controllers (PLCs), and control servers, recognizing that these systems often have long patch cycles and unique constraints. Control 8.8 in this context involves risk-based prioritization, with compensating controls (e.g., network segmentation, access restrictions) when patching is delayed. Vulnerability disclosures from ICS vendors must be tracked, and patches validated in test environments before deployment to avoid operational disruptions.

Cross-Compliance Mapping

EU GDPR – Articles 32(1), 5(1)(f), Recital 83: GDPR requires data controllers and processors to implement “appropriate technical and organizational measures” to secure personal data, taking into account “the state of the art” and the risks to data subjects (Article 32(1)). Vulnerability management, including timely patching, is implicitly part of this mandate, as unpatched systems jeopardize data integrity and confidentiality (Article 5(1)(f)). Supervisory authorities across Europe have cited failure to patch known vulnerabilities as contributing to data breaches, often resulting in substantial fines. For example, lack of timely patching has been referenced in GDPR enforcement actions where critical CVEs were publicly disclosed yet left unaddressed. Recital 83 further emphasizes that risks must be “mitigated through the implementation of up-to-date measures.” Control 8.8 ensures compliance by enforcing regular scanning, risk-based prioritization, and timely flaw remediation, forming part of a demonstrable, proactive security posture that protects personal data. Documented vulnerability management processes and evidence of patch cycles can serve as compliance artifacts in data protection audits or investigations.

EU NIS2 – Article 21(2)(e), 23, 27: NIS2 establishes a direct legal requirement for vulnerability handling. Article 21(2)(e) mandates that essential and important entities implement measures for “security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.” This encompasses discovery, assessment, prioritization, patching, and communication regarding technical vulnerabilities. Article 23 requires incident reporting where unpatched vulnerabilities contribute to disruptions, while Article 27 allows national authorities to enforce compliance actions. Control 8.8 aligns with NIS2 by ensuring a structured vulnerability management process, including clear roles and responsibilities, asset inventories, and documented patching schedules. Additionally, the Directive encourages participation in coordinated vulnerability disclosure (CVD) programs, further integrating external sources into the organization's vulnerability handling lifecycle. A failure to maintain such controls may not only lead to operational risks but legal and regulatory repercussions under NIS2's enforcement mechanisms.

EU DORA – Articles 11, 15, Annex I Section A(5): DORA places explicit regulatory obligations on financial entities to manage ICT vulnerabilities proactively. Article 11 requires firms to establish policies for "identifying and tracking ICT vulnerabilities and promptly responding." Article 15 mandates "appropriate mitigation measures" for discovered vulnerabilities, including mandatory patching policies for all ICT systems. Annex I Section A(5) lists "protection and prevention measures, including timely patching" as key to operational resilience. Control 8.8 fully supports DORA by embedding risk-based vulnerability management into ICT risk frameworks, supported by continuous monitoring and formal reporting mechanisms. DORA compliance involves not only internal remediation but also supervisory engagement, where authorities can demand updates on outstanding vulnerabilities. Entities must demonstrate patch management discipline, including SLA-bound remediation timelines, and the use of automated tools to detect, prioritize, and manage vulnerabilities across complex, interconnected ICT environments.

NIST SP 800-53 Rev.5 – RA-5, SI-2, CA-7: NIST provides detailed, prescriptive requirements for vulnerability management. RA-5 (Vulnerability Monitoring and Scanning) requires regular scans, including for newly discovered vulnerabilities, and integration with threat intelligence to adapt scan scopes. SI-2 (Flaw Remediation) mandates timely correction of software and system flaws, requiring organizations to assign risk levels and patch accordingly, with defined deadlines (e.g., critical within 15 days). CA-7 (Continuous Monitoring) supports ongoing assessment of vulnerability status. Control 8.8 ensures these controls are operationalized, aligning directly with U.S. federal compliance regimes like FedRAMP, FISMA, and defense-related standards. Organizations are expected to maintain detailed vulnerability registers, use tools like Nessus, Qualys, or OpenVAS, and produce audit-ready evidence of remediation timelines. Failure to comply with these standards can result in non-compliance findings in federal or regulated audits.

COBIT 2019 – APO12.06, DSS05.03, BAI09.02: integrates vulnerability management into its governance and management objectives, emphasizing both risk treatment and operational execution. Under APO12.06 (Manage Risks – Respond to Risk), organizations are expected to address identified risks, which includes vulnerabilities, through structured mitigation plans. Control 8.8 aligns by ensuring that technical vulnerabilities are identified, assessed in terms of risk, and remediated based on business impact. Auditors will expect to see risk registers populated with vulnerability-related entries and clear ownership of remediation tasks. DSS05.03 (Monitor Infrastructure for Security Events) reinforces the need for real-time monitoring and alerting of vulnerability exploitation attempts. Vulnerability scans, system logs, and threat intelligence feeds must be integrated into the monitoring environment. Control 8.8 supports this through continuous scanning and automated alerting when vulnerabilities are detected, ensuring visibility and rapid response. COBIT requires that security events are not just monitored but also analyzed to inform future risk and vulnerability management efforts. BAI09.02 (Manage Change Acceptance and Transitioning) links vulnerability management with change management. Patching, which often results from vulnerability findings, must follow formal change control processes. Control 8.8 depends on tested, approved, and documented patch deployments, ensuring stability while closing security gaps. COBIT emphasizes tracking KPIs, such as mean time to patch, percentage of systems scanned, and compliance with patching policies, aligning fully with the operational goals of 8.8.

Audit Methodology Considerations

ISO/IEC 19011:2018 & ISO/IEC 27007:2020 – Clauses 6.4.5, 6.5.6, 6.5.7, 7.4, 7.5.2, 8.2: Auditors begin by reviewing the organization's vulnerability management policy, assessing whether it defines scan frequency, asset coverage, prioritization based on risk, remediation timelines (e.g., critical vulnerabilities within 14 days), and clear responsibilities. Clause 6.4.5 drives auditors to focus on high-risk systems and known vulnerability exposures. Clause 6.5.6 mandates collecting evidence, such as vulnerability scan outputs (e.g., Nessus, Qualys) and penetration test results. Auditors verify scan regularity, completeness (matching Control 5.9's asset inventory), and whether critical vulnerabilities reappear across reports. Clause 6.5.7 requires triangulating scan data with remediation actions auditors trace specific vulnerabilities (e.g., Log4Shell) through discovery, risk assessment, change records (8.32), and confirm closure in subsequent scans. Clause 7.4 focuses on evaluating the effectiveness of the process, while Clause 8.2 drives identification of systemic gaps, such as delayed patching or lack of documented risk acceptances.

ISO/IEC 27006:2020 – Clauses 9.4.2, 9.4.5, 9.4.7: Certification auditors assess whether vulnerability management is within ISMS scope (9.4.2), examining risk assessments that include unpatched vulnerabilities as a factor. Under Clause 9.4.5, auditors evaluate whether risk treatment plans exist for outstanding vulnerabilities, including remediation tracking and management sign-off. Clause 9.4.7 guides auditors to verify logical controls checking whether vulnerability scanners are correctly configured (authenticated scans, up-to-date plugins) and whether scan schedules are enforced. Auditors review whether scan coverage includes all production and critical systems, cross-referencing asset inventories, and confirm whether scan results are used to drive security improvements.

COBIT 2019 – APO12.06, DSS05.03, BAI09.02: Auditors assess whether the organization manages vulnerabilities as part of risk governance (APO12.06), with clear documentation of risk evaluation and treatment for technical flaws. They verify whether security event monitoring (DSS05.03) includes alerting on exploit attempts and whether vulnerability-related incidents are logged and acted upon. Under BAI09.02, patching is reviewed as a controlled change auditors trace whether change management records reflect timely patch application tied to vulnerability findings. Metrics such as mean time to patch, percentage of systems patched within SLA, and unresolved critical vulnerabilities are examined as indicators of control effectiveness.

ISACA ITAF – Standard 1205, Guideline 2203: Standard 1205 guides auditors to ensure sufficient evidence of vulnerability management auditors examine whether policies are implemented, scans are performed, and findings are remediated. Guideline 2203 assists in evaluating whether responsibilities are clearly assigned and whether management oversight exists. Interviews with security personnel validate whether threat intelligence (Control 5.7) informs prioritization, and whether external vulnerability disclosures are handled effectively.

NIST SP 800-53A – RA-5, SI-2, CA-7: RA-5 requires confirmation of routine vulnerability scanning, including when new threats emerge. Auditors assess scan frequency, scope, and integration with continuous monitoring (CA-7). Under SI-2, auditors verify that identified flaws are remediated, tracing individual vulnerabilities through their lifecycle discovery, risk rating, patch deployment, and validation. Evidence includes meeting minutes of patch management boards, risk acceptance forms, and remediation logs. Auditors may perform spot-check scans or manual version checks (e.g., OpenSSL versions) to validate scan accuracy.

Technical Validation: Auditors may test scanner efficacy by ensuring latest vulnerability signatures are applied and may perform authenticated scans on sample systems. Tools like EICAR test files for malware protection also apply conceptually validating whether scanners detect and report accurately. Manual checks on critical infrastructure (e.g., version banners, patch levels) are performed to validate scanner coverage.

Incident Integration: Auditors assess whether past incidents were linked to unpatched vulnerabilities, and whether the post-incident review improved patch management timelines. This ties into Control 5.27, ensuring lessons learned are embedded.

Governance & Reporting: Auditors examine whether vulnerability metrics (e.g., % patched, average remediation time) are reported to senior management. **Participation in coordinated vulnerability disclosure or bug bounty programs is reviewed as evidence of a mature posture, aligning with NIS2 and ISO 30111/29147.**

8.13 Information Backup

Attribute	Value
Control Type	Corrective
Information Security Properties	Integrity, Availability
Cybersecurity Concepts	Recover
Operational Capabilities	Continuity
Security Domains	Protection

Ties to Other Controls

5.30 ICT readiness for business continuity: Control 8.13 is a foundational component of ICT readiness, ensuring that critical data can be restored during a disruption. Without reliable and up-to-date backups, business continuity plans cannot be effectively executed, particularly in scenarios like ransomware attacks or system failures.

5.29 Information security during disruption: Backups play a pivotal role in maintaining security and availability during disruptive events. If data becomes corrupted, deleted, or compromised, backups provide the necessary redundancy to restore operations securely. 8.13 ensures that the integrity and availability of data are preserved during crises.

5.9 Inventory of assets: Effective backups depend on knowing what assets exist and their criticality. Control 8.13 relies on 5.9 to identify which systems, applications, and datasets must be prioritized for backup, ensuring that all vital information assets are covered.

5.31 Legal, statutory, regulatory, and contractual requirements and 5.33 Protection of records: Certain records are subject to mandatory retention and must be included in backup routines to meet compliance obligations. Additionally, backups themselves are records that need to be protected against loss, tampering, or unauthorized access, aligning with 5.33.

8.14 Redundancy of information processing facilities: While 8.14 ensures that systems can continue to operate during failures via redundant infrastructure, 8.13 focuses on ensuring that data can be restored if lost. Together, they form a resilience strategy one for systems, one for data.

8.10 Information deletion: Backups must align with data retention and deletion policies. Data deleted from production systems should not persist indefinitely in backups. Control 8.13 must include procedures for backup pruning or time-limited retention to ensure compliance with privacy laws and internal policies.

8.16 Monitoring activities: Backup processes must be monitored to confirm that they run successfully. Logs of backup jobs should be reviewed regularly, and alerts should be in place for failed or incomplete backups, as these can critically affect data recovery readiness.

8.7 Protection against malware: Backups must be protected against malware threats, especially ransomware, which can target backup files. 8.13 ties to 8.7 by requiring that backup environments are isolated, scanned, and possibly air-gapped or immutable, to prevent infection and ensure recovery integrity.

7.1 Secure areas and 7.2 Physical entry: Physical security of backup media is essential, especially for off-site storage. Controls around secure locations, access control, and environmental protection (e.g., fire, flood) are vital for ensuring backup availability and confidentiality.

5.34 Privacy and protection of PII: Personal data within backups must be protected, subject to the same privacy requirements as live data. Control 8.13 necessitates encryption, access controls, and retention limits for backups containing PII, ensuring compliance with regulations such as GDPR or similar.

ISO Cross-References

ISO/IEC 27005:2024 – Clause 8.3 (Risk Analysis) and Clause 8.4 (Risk Treatment Options): ISO/IEC 27005 identifies the absence or inadequacy of backups as a key vulnerability, particularly in the context of availability risks. Clause 8.3 highlights that incidents such as hardware failures, ransomware attacks, or accidental deletions do not need to be prevented to maintain resilience as long as effective backups exist, their impact can be mitigated. Clause 8.4 recommends backup strategies as a risk treatment option to reduce downtime and data loss, aligning directly with Control 8.13. A practical example from the standard: even if a system is compromised, restoring data from clean, recent backups ensures continuity with minimal loss. Risk treatment plans must explicitly consider backup frequency, integrity checks, and restoration capabilities to be effective. Auditors and risk managers are encouraged to assess whether backup systems are tested regularly, whether data criticality is properly mapped to backup policies, and whether backup systems are isolated from potential threats, ensuring that this fundamental control supports availability objectives within an ISMS.

ISO/IEC 22301:2019 – Clauses 8.4.3 (Business Continuity Procedures) and 8.5.2 (Restoration of Activities): This business continuity management system (BCMS) standard establishes that regular and reliable backups are a cornerstone of maintaining operational continuity. Clause 8.4.3 mandates organizations to ensure that critical information is protected and recoverable in line with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). Clause 8.5.2 further requires that restoration activities include the recovery of data from backups as part of resuming disrupted operations. Control 8.13 supports these clauses by ensuring that backup processes are defined, tested, and capable of restoring systems in a timeframe that supports continuity goals. For instance, if a core financial system must be restored within 4 hours, the backup solution must support such a recovery. ISO/IEC 22313:2020, the accompanying guidance, reinforces that backups must be verified (e.g., through restore tests), protected (via encryption and secure storage), and aligned with the business continuity strategy. This ensures that backup reliability directly supports organizational resilience during crises.

ISO/IEC 27017:2021 – Clause 9.5.1.4 (Cloud Backup Responsibilities): In cloud environments, backup responsibilities can become blurred between providers and customers. Clause 9.5.1.4 of ISO/IEC 27017 advises that organizations clarify backup roles, ensuring that neither party assumes the other is handling backups, potentially resulting in no backups at all. Control 8.13 mandates that cloud customers understand their provider's backup capabilities, limitations, and whether they need to maintain independent backups for critical data. For instance, while a SaaS provider might offer daily snapshots, a customer with stricter RPO requirements may need to export and store backups independently. The standard stresses formalizing these responsibilities in contracts or service level agreements (SLAs), ensuring that backup frequencies, retention periods, and data recovery procedures are clearly understood. ISO/IEC 27017 supports 8.13 by ensuring that backup strategies remain effective even in outsourced environments, preserving data availability irrespective of the operational model.

ISO/IEC 27018:2020 – Clause 10.4 (PII Backup in Cloud Services): This standard, focusing on PII protection in cloud computing, addresses backup from a privacy perspective. Clause 10.4 mandates that cloud service providers only create backups of customer PII under explicit instruction from the customer, ensuring data minimization and respecting purpose limitation principles. Control 8.13 aligns by enforcing that backups of personal data are not only conducted securely but also lawfully, respecting contractual and regulatory limits. Furthermore, 27018 stipulates that PII in backups must be protected with equivalent controls to live data this includes encryption, access restrictions, and retention management. For example, if a customer deletes personal data to comply with GDPR Article 17 (Right to Erasure), backups must also be configured to exclude or remove this data over time, ensuring ongoing privacy compliance. This elevates 8.13 from a pure availability concern to one of legal accountability, especially in regulated industries.

ISO/IEC 27035-2:2023 – Clause 7.3 (Backup in Incident Preparedness): ISO/IEC 27035-2, dealing with incident response planning, highlights backup management as a core element of incident preparedness. Clause 7.3 recommends that organizations maintain backup operators, documented procedures, and tested recovery capabilities to ensure that data loss incidents can be effectively mitigated. Control 8.13 supports this by embedding backup into the incident lifecycle ensuring that, post-incident, data can be restored quickly, minimizing downtime and data loss. Auditors expect to see that backup procedures are integrated into incident response plans, with clear roles, responsibilities, and testing schedules. For example, an organization might simulate a data breach, validating whether backups can restore clean data without introducing malware or violating retention policies. ISO/IEC 27035-2 ensures that backup readiness is not static but an active component of organizational resilience.

ISO/IEC 27701:2021 – Clauses 7.4.5 (PII Retention in Backups) and 7.4.9 (Access Control for PII in Backups): Extending ISO/IEC 27001 to privacy management, this standard stipulates that backup processes for PII must comply with retention requirements and be secured against unauthorized access. Clause 7.4.5 ensures that PII in backups is not retained longer than necessary, aligning backup policies with data retention schedules. Clause 7.4.9 requires that access to backups containing PII is controlled, monitored, and limited to authorized personnel. Control 8.13 enforces these by ensuring backup encryption, access auditing, and pruning mechanisms are in place. For example, if a backup contains customer data that is subject to erasure requests, policies must ensure this data is excluded from future backups or deleted from archival copies in line with privacy obligations. ISO/IEC 27701 elevates backup from a purely technical control to a privacy governance issue, requiring that availability and confidentiality are jointly maintained.

Cross-Compliance Mapping

EU GDPR – Articles 5(1)(f), 32, and 17(1): The General Data Protection Regulation (GDPR) mandates that personal data be processed securely, including protection against accidental loss, a core concern addressed by Control 8.13. Article 5(1)(f) enshrines the integrity and availability principle, requiring organizations to ensure that data remains accessible and accurate. Reliable information backup directly supports this by enabling restoration of data in the event of system failures, cyberattacks, or accidental deletion. Article 32 further requires that organizations implement technical measures such as backup procedures to protect personal data. Regular, tested backups demonstrate compliance with this obligation, particularly when paired with secure storage (e.g., encryption and access control on backup media). Article 17(1), the Right to Erasure, has implications for backups: organizations must ensure that when personal data is deleted from live systems, it is also managed within backups, ensuring that erasure requests are respected over time. Backup retention schedules must therefore align with data minimization and retention policies. Control 8.13 helps organizations fulfill GDPR's demand for resilient data management while ensuring that backup systems do not inadvertently become a compliance risk due to outdated or unpruned personal data.

EU NIS2 – Articles 21(2)(f), 21(2)(h), and 23: The NIS2 Directive emphasizes the resilience and availability of essential services, with backup systems being a crucial component of this resilience. Article 21(2)(f) requires that organizations adopt measures ensuring availability and authenticity of information systems and data. Control 8.13 directly addresses this by providing mechanisms for data restoration, ensuring that even in the event of disruption, critical services can resume using backup data. Article 21(2)(h) calls for policies that ensure business continuity and crisis management, which are impossible to achieve without robust and tested backup strategies. Organizations must demonstrate that they can recover data in line with operational needs, minimizing downtime. Additionally, Article 23 mandates that incidents affecting availability be reported if a service is disrupted due to data loss, and no backup exists, this could constitute a serious compliance failure. By implementing 8.13, organizations can prevent prolonged outages and demonstrate due diligence in securing essential information assets, aligning with NIS2's broader goals of cyber resilience and incident readiness.

EU DORA – Articles 10(1), 11(1), and 15(3): Under the Digital Operational Resilience Act (DORA), financial entities are required to ensure that critical functions remain resilient to ICT-related disruptions. Article 10(1) mandates the establishment of ICT continuity plans, where data backup is fundamental. Without comprehensive backup mechanisms, entities cannot assure the recovery of critical data, which is essential for operational continuity. Article 11(1) requires entities to identify critical ICT systems and data, ensuring that appropriate protections (including backup) are in place. Control 8.13 supports this by ensuring critical data is not only backed up but recoverable within timeframes that support business continuity. Article 15(3) requires that operational resilience testing includes the verification of backup systems, ensuring that data can be restored effectively in simulated disruptions. Regulators expect evidence of regular backup testing, retention management, and the secure handling of backups, particularly given the sensitivity of financial data. Control 8.13 ensures that financial stability is maintained through effective backup strategies, reducing risks associated with data loss, corruption, or system compromise.

NIST SP 800-53 Rev.5 – CP-9, CP-10, MP-5, and SI-12: NIST SP 800-53 Rev.5 provides a comprehensive framework for backup and recovery under Contingency Planning. CP-9 (Information System Backup) requires organizations to perform backups consistent with recovery objectives, including frequency, scope, and protection of backup media. Control 8.13 ensures that these requirements are met by defining policies for regular, automated backups, validated through periodic testing. CP-10 (System Recovery and Restoration) mandates the capability to restore systems to operational status using backups, requiring restoration procedures to be documented and tested. Auditors expect proof of restore tests, with results indicating recovery timeframes and data integrity. MP-5 (Media Transport Protection) ensures that backup media, when moved (e.g., offsite storage), is protected from physical damage and unauthorized access, aligning with 8.13 requirements for backup media security. SI-12 (Information Handling and Retention) reinforces that data, including backups, must comply with retention policies, ensuring obsolete or sensitive information is not retained unnecessarily, reducing compliance and security risks. Together, these controls align tightly with 8.13, ensuring that backup systems provide reliable recovery, regulatory alignment, and protection of data assets.

COBIT 2019 – DSS04 (Manage Continuity), DSS01 (Manage Operations), APO12 (Risk Management): COBIT 2019 incorporates backup as part of IT continuity and risk management. DSS04 mandates the creation and maintenance of backup and recovery plans as part of ensuring business continuity. Control 8.13 fulfills this by ensuring that data critical to business operations is backed up at intervals that reflect its value and volatility. DSS01 focuses on operational control, requiring that backups be monitored, tested, and integrated into daily IT service management. Auditors look for evidence of backup success rates, alerting mechanisms for failures, and escalation procedures. APO12 stresses identifying risks associated with data unavailability, for which backup is a direct mitigation. Risk registers should reflect the role of backups in reducing potential impact from data loss scenarios. COBIT requires that backup processes be aligned with business needs, including RPO/RTO definitions, and that ownership of backup activities is assigned, measured, and reviewed. Control 8.13 ensures that data protection is not isolated but part of a governed, risk-aware IT environment, ensuring accountability and continuous improvement.

Audit Methodology Considerations

ISO/IEC 19011:2018 – Clauses 6.4.5, 6.5.6, 6.5.7: Following ISO/IEC 19011, auditors begin by reviewing the organization's backup policy, ensuring it specifies data types, frequency, retention periods, and storage protocols. Clause 6.4.5 requires gathering objective evidence, including backup schedules, job logs, and failure reports. The auditor will sample recent backup job logs to verify that backups run as scheduled (e.g., daily incremental, weekly full backups) and that any failures were identified and addressed. Clause 6.5.6 emphasizes evaluating implementation effectiveness: the auditor will assess whether restore tests have been conducted regularly, with documentation of results. For example, records showing successful restoration of test databases or files from backup media are critical. Clause 6.5.7 encourages verification the auditor may request a live demonstration, such as retrieving a specific file from backup or initiating a database restore to a test environment. Backup security controls are also evaluated: are backups encrypted, access-controlled, and stored off-site in secure conditions? If physical media (e.g., tapes) are used, auditors verify storage facility security measures (access logs, environmental controls). Non-compliance or poor performance in backup execution, monitoring, or security is reported, ensuring the organization's backup systems are both functionally sound and aligned with its continuity objectives.

ISO/IEC 27007:2020 – Clauses 7.4, 7.5.2, 8.2: Clause 7.4 guides auditors to conduct interviews with key personnel (e.g., backup administrators, IT managers), assessing their understanding of backup responsibilities. Questions include: "What is the RPO/RTO for critical systems?" and "How are backups tested for reliability?". Clause 7.5.2 instructs auditors to examine whether backup controls cover all relevant systems, including cloud environments, databases, and endpoints. The auditor will review configuration settings of backup software, verifying encryption settings, retention rules, and failure alert mechanisms. Clause 8.2 requires evaluating personnel competence auditors check that staff can explain restore procedures, handle backup anomalies, and demonstrate familiarity with the backup policy. Auditors also examine whether backup testing is integrated into continuity drills, and whether test results inform continuous improvement. If discrepancies exist between backup scope and business impact analyses, auditors will flag this as a critical gap. For example, if high-priority systems lack daily backups while the RPO demands it, it indicates misalignment. The audit also verifies whether cloud backup responsibilities are clearly defined between provider and customer, avoiding gaps due to assumed accountability.

ISO/IEC 27006:2020 – Clauses 9.4.2, 9.4.5, 9.4.7: Clause 9.4.2 mandates that auditors determine whether backup processes are effective and suitable for supporting the ISMS. Auditors validate that backups exist for all critical data, that retention periods comply with both legal requirements and internal policies, and that backup media are properly safeguarded. Clause 9.4.5 requires that audit trails for backup activities are complete this includes backup schedules, execution logs, incident reports, and restoration records. Auditors assess whether backups are monitored for success/failure, and whether corrective actions follow any detected failures. Clause 9.4.7 emphasizes reviewing past non-conformities: for instance, if a previous audit found that backup jobs failed without remediation, auditors verify whether process improvements were implemented (e.g., better monitoring tools, revised schedules). Auditors may also cross-reference business continuity documentation, ensuring that backup operations support declared recovery objectives and are tested against realistic scenarios.

COBIT 2019 – DSS04 (Manage Continuity), DSS01 (Manage Operations), APO12 (Manage Risk): Under DSS04, auditors assess whether the organization has documented, tested backup and recovery plans. They verify that backup activities support continuity goals, such as RPO and RTO compliance. Auditors review performance metrics, like the frequency of backup failures, recovery success rates, and the time required for restorations. DSS01 focuses on day-to-day operations auditors examine whether backup processes are integrated into IT service management, with proper alerting, logging, and capacity planning. They also assess whether backups scale with data growth and whether resource constraints impact effectiveness. APO12 requires identifying risks associated with data unavailability auditors evaluate whether the risk register includes backup failure risks and whether mitigation strategies are in place. This includes verifying responsibility assignments, periodic reviews, and escalation protocols when backup issues arise. Auditors ensure that backup strategies are aligned with organizational priorities and that governance structures support continuous oversight of backup performance and security.

ISACA ITAF – Standard 1205, Guideline 2203: Auditors following Standard 1205 collect reliable evidence of backup system performance, including reviewing backup software configurations, media handling logs, and access control lists. Guideline 2203 emphasizes testing operational effectiveness: auditors simulate backup failure scenarios, assess how alerts are generated, and verify the response time. They also evaluate restoration accuracy auditors may request a partial or full system restore and measure whether data integrity is maintained. Auditors examine whether backup media are tracked (e.g., through inventory registers), ensuring no unauthorized removal or access occurs. Authorization workflows for initiating restores are reviewed, ensuring only approved personnel can access backups. For third-party backup services, auditors assess contractual agreements, verifying responsibilities for data protection, restoration timeframes, and audit rights over provider practices.

NIST SP 800-53A – CP-9, CP-10, MP-5, SI-12: Using CP-9 assessment procedures, auditors review whether backup frequencies align with business recovery objectives, and whether backup integrity checks (e.g., hash validation) are performed. Auditors inspect backup system logs for anomalies, verifying whether alerts for missed backups are promptly addressed. CP-10 guides auditors to test recovery capabilities, such as observing a disaster recovery drill, measuring recovery time, and evaluating restoration completeness. Under MP-5, auditors assess transport security for physical backup media whether encryption is used and whether transport logs document chain-of-custody. SI-12 requires auditors to verify that data retention policies apply to backups this includes ensuring that obsolete backups are destroyed securely and that personal data is not retained beyond legal limits. Auditors ensure that technical and procedural controls for backup align with both continuity and compliance mandates.

Found this Preview Useful?

The full version of The Zenith Controls contains 82 more meticulously mapped controls, including critical topics like:

- Access Control & Privileged Access (Controls 5.15, 5.16, 5.18, 8.2)
- Cryptography & Data Masking (Controls 8.11, 8.24)
- Secure Development, Coding & Supply Chain (Controls 8.25, 8.28, 5.21)

And much more...
[Click Here to Purchase the Full Toolkit and Master Your Compliance Landscape]

5. About the Author

Igor Petreski is a seasoned cybersecurity leader, auditor, and systems architect with over 25 years of in-the-trenches experience building and defending complex IT environments. His career has been defined by a unique duality: the hands-on, technical work of building IT infrastructure from the ground up for over 1,500 users, and the high-level strategic work of authoring global cybersecurity policies for a multinational corporation with 50+ plants in over 35 countries.

The Zenith Controls was born from this real-world experience. Igor developed this integrated system because he recognized the immense challenge organizations face in translating complex standards like ISO 27001, NIS2, DORA, and GDPR into a single, unified, and actionable program. This is not a theoretical framework; it is a battle-tested roadmap reflecting the lessons learned from over 100 audits and dozens of successful implementations.

Igor holds a range of elite industry certifications, including **CISA** (Certified Information Systems Auditor), **CISM** (Certified Information Security Manager), **CEH** (Certified Ethical Hacker), and is a **PECB Certified ISO/IEC 27001 Lead Auditor and Lead Implementer**. He is currently completing his **MSc in Cyber Security from Royal Holloway**, University of London, ensuring his expertise remains on the cutting edge of modern threats and defenses.

His mission with Zenith Controls is to empower other professionals to move beyond compliance as a checkbox and build security programs that are truly resilient, strategically aligned, and audit-ready from day one.