**L.01 – Information Security Policy (System-Based Perspective)**

**Control Description**  
Establish, implement, and maintain a system-wide information security policy supported by aligned processes and documented procedures.

The information security policy acts as the central component of the organization's security management system. It defines the governing principles, roles, and standardized practices required to protect both digital and physical assets. As a system control, it ensures that information security is managed holistically and integrated into all business functions. The policy, along with its supporting operational components, provides consistency, direction, and enforceable expectations across the organizational system. Without a defined and coordinated framework, the system lacks coherence, increasing operational risk and undermining overall security resilience.

**Risk Statement**  
Failure to define and implement a system-wide, structured information security policy—along with standardized supporting processes—creates a disjointed security posture. In such a fragmented system, departments may adopt inconsistent safeguards, fail to interpret security requirements accurately, or circumvent established protocols. This leads to uncoordinated risk management, unmanaged vulnerabilities, and misaligned decisions that do not support overarching organizational goals. Ultimately, this degrades the integrity of the system, elevating the likelihood of security incidents, compliance failures, and operational inefficiencies.

**Business Impact**

* System-wide exposure to unauthorized access, data breaches, or loss of confidentiality
* Deviation from regulatory and compliance requirements (e.g., ISO 27001, GDPR)
* Breakdown in stakeholder trust due to perceived systemic security failures
* Financial consequences from penalties, litigation, or lost business opportunities
* Redundant or conflicting security initiatives due to a lack of integrated planning

**ISO Control Alignment**  
**ISO/IEC 27001:2022 – Clause 5.2 – Information Security Policy**  
This clause mandates the creation of an information security policy that is appropriate to the organization’s purpose, supports its strategic objectives, and integrates with the overall management system. The policy must be communicated across the system, reviewed regularly, and clearly understood at all levels.

**Core Clauses Referenced:**

* **Clause 5.2** – Information Security Policy
* **Clause 5.1** – Leadership and Commitment
* **Clause 6.1.1** – Actions to Address Risks and Opportunities
* **Clause 7.3** – Awareness
* **Clause 7.5** – Documented Information
* **Clause 9.3** – Management Review

**Relevant Annex A Controls:**

* **A.5.1** – Policies for Information Security
* **A.5.2** – Information Security Roles and Responsibilities
* **A.6.1** – Security Objectives and Planning
* **A.6.2** – Security in Project Management
* **A.7.2** – Awareness, Education, and Training
* **A.8.1** – Asset Responsibilities
* **A.8.8** – Management of Technical Vulnerabilities
* **A.18.1** – Legal and Contractual Compliance

**L.02 – Information Security Roles and Responsibilities (System-Based Perspective)**

**Control Description**  
Establish and allocate clearly defined roles and responsibilities for information security across the organizational system.

Within an effective information security management system (ISMS), roles and responsibilities must be systematically defined, documented, and communicated to ensure accountability, consistent task execution, and unified operational alignment. This structural clarity supports the seamless functioning of critical activities such as risk management, threat response, compliance tracking, and awareness training. By embedding these responsibilities into the organization’s system, departments and individuals are empowered to proactively uphold the security posture and respond cohesively to security-related events.

**Risk Statement**  
If information security roles and responsibilities are not properly defined and assigned at a system level, the organization faces a lack of operational clarity and accountability. This can lead to critical security tasks being overlooked, inconsistently performed, or duplicated. Delays in incident detection and response, failure to meet compliance expectations, and breakdowns in coordination during security events can result. Ultimately, the absence of role-based structure compromises the organization’s ability to manage risk and protect assets effectively.

**Business Impact**

* Missed or inconsistent execution of key security tasks
* Inefficiencies due to unclear or overlapping responsibilities
* Slower incident response, increasing potential impact
* Greater risk of audit deficiencies and regulatory violations
* Reputational harm and reduced confidence from customers, partners, or stakeholders

**ISO Control Alignment**  
**ISO/IEC 27001:2022 – Clause 5.3 – Organizational Roles, Responsibilities, and Authorities**  
This clause requires that relevant roles be clearly established, and individuals assigned to those roles are empowered and competent to fulfill them. Responsibilities must be documented and communicated to enable coordinated, system-wide security management.

**Core Clauses Referenced:**

* **Clause 5.3** – Organizational Roles, Responsibilities, and Authorities
* **Clause 5.1** – Leadership and Commitment
* **Clause 7.2** – Competence
* **Clause 7.3** – Awareness

**Relevant Annex A Controls:**

* **A.6.1** – Responsibilities for Information Security (Primary Control)
* **A.5.2** – Information Security Roles and Responsibilities
* **A.5.3** – Segregation of Duties
* **A.5.4** – Contact with Authorities
* **A.5.5** – Contact with Special Interest Groups
* **A.5.7** – Threat Intelligence
* **A.6.3** – Information Security Planning
* **A.7.2** – Awareness, Education, and Training
* **A.16.1** – Responsibilities During Security Incidents
* **A.18.2** – Intellectual Property Rights

**L.03 – Supplier Information Security Risk Management (System-Based Perspective)**

**Control Description**  
Develop and enforce a system-wide policy for managing information security risks associated with supplier and third-party relationships.

As part of a comprehensive information security management system (ISMS), supplier risk management ensures that external entities—including vendors, contractors, cloud service providers, and other third parties—are integrated into the organization's risk and control environment. A structured policy provides a unified framework for evaluating, onboarding, and continuously monitoring suppliers. This includes setting baseline security requirements, conducting due diligence, establishing contractually binding obligations, and implementing ongoing oversight mechanisms. By embedding these activities within a defined system, organizations maintain control over externally introduced risks while aligning third-party activities with internal security expectations.

**Risk Statement**  
If the organization does not define and implement a structured policy to address supplier-related information security risks, it undermines systemic visibility and control over the extended enterprise. Suppliers may fail to meet security expectations, introducing vulnerabilities into the organization’s environment. Without clear requirements, monitoring mechanisms, or escalation procedures, risks may go undetected and unmanaged—leading to data loss, compliance failures, or service disruption. This weak link in the system exposes the organization to elevated threat levels and reduces resilience.

**Business Impact**

* Increased risk of data breaches due to insecure third-party handling of sensitive information
* Disruption to core operations from supplier security failures or incidents
* Regulatory and legal consequences stemming from third-party non-compliance
* Loss of customer or stakeholder trust following a supplier-related security event
* Complex recovery and remediation efforts due to lack of contractual clarity or oversight

**ISO Control Alignment**  
**ISO/IEC 27001:2022 – Clause 6.1.1 & 8.1 – Risk Management and Operational Control**  
These clauses emphasize the need for proactive identification and treatment of risks—particularly within supplier interactions—and for establishing controls to ensure supplier activities are planned, monitored, and reviewed in alignment with organizational requirements.

**Core Clauses Referenced:**

* **Clause 6.1.1** – Actions to Address Risks and Opportunities
* **Clause 6.1.3** – Information Security Risk Treatment
* **Clause 8.1** – Operational Planning and Control
* **Clause 9.2** – Internal Audit (Supplier Risk Monitoring)
* **Clause 9.3** – Management Review (Incorporating Supplier Risk Insights)

**Relevant Annex A Controls:**

* **A.5.19** – Information Security in Supplier Relationships (Primary Control)
* **A.5.20** – Information Security within Supplier Agreements
* **A.5.21** – ICT Supply Chain Risk Management
* **A.5.22** – Monitoring and Change Management of Supplier Services
* **A.5.23** – Information Security for Use of Cloud Services
* **A.5.17** – Information Security in Project Management (Third-Party Involvement)
* **A.6.1** – Policies for Information Security (Including Third-Party Governance)
* **A.15.1** – Supplier Relationship Security (Legacy Reference)

**M.01 – Information Security Reporting Policy (System-Based Perspective)**

**Control Description**  
Establish and implement a formal, system-wide policy governing the reporting of information security activities, events, and performance indicators.

Consistent and structured reporting is a critical function within an effective information security management system (ISMS). This policy defines standardized reporting practices—including report types (e.g., risk assessments, incidents, audits), reporting frequency, responsible roles, and escalation paths. It ensures that actionable insights flow through defined channels to senior leadership and relevant stakeholders. By embedding reporting mechanisms into the operational and governance layers of the organization, decision-makers are equipped with timely, relevant information to assess risks, track compliance, and measure the effectiveness of security controls—driving a continuous improvement cycle.

**Risk Statement**  
If the organization lacks a system-integrated policy for formal information security reporting, it risks insufficient visibility into security posture, delayed risk response, and missed opportunities for improvement. Inconsistent or informal reporting practices prevent leadership from receiving accurate intelligence, resulting in uninformed decision-making and unaddressed vulnerabilities. Without a clear reporting structure, critical events may be overlooked or underreported, weakening overall system resilience and accountability.

**Business Impact**

* Undetected or unaddressed vulnerabilities due to lack of visibility
* Ineffective or delayed responses to incidents or breaches
* Increased risk of regulatory non-compliance and failed audits
* Missed opportunities to enhance the security maturity level
* Reduced confidence from executives, auditors, and external stakeholders

**ISO Control Alignment**  
**ISO/IEC 27001:2022 – Clause 9.1 – Monitoring, Measurement, Analysis and Evaluation**  
This clause requires organizations to evaluate the performance and effectiveness of the ISMS through regular and structured monitoring and reporting. It supports informed governance and continual improvement across the security lifecycle.

**Core Clauses Referenced:**

* **Clause 5.1** – Leadership and Commitment
* **Clause 5.2** – Information Security Policy
* **Clause 9.1** – Monitoring, Measurement, Analysis, and Evaluation
* **Clause 9.2** – Internal Audit
* **Clause 9.3** – Management Review
* **Clause 10.1** – Continual Improvement

**Relevant Annex A Controls:**

* **A.5.1** – Policies for Information Security (Primary Control)
* **A.5.2** – Information Security Roles and Responsibilities
* **A.5.6** – Information Security in Project Management
* **A.5.10** – Acceptable Use of Information and Assets
* **A.5.13** – Information Security Event Reporting
* **A.5.14** – Information Security Incident Management
* **A.5.16** – Monitoring Activities
* **A.6.1** – Security Objectives and Planning
* **A.6.3** – Business Continuity and Security Reporting
* **A.8.7** – Protection Against Malware
* **A.12.1** – Logging and Monitoring

**M.02 – Pre-Access Information Security Responsibilities (System-Based Perspective)**

**Control Description**  
Implement a structured policy that defines and communicates information security responsibilities to all personnel—including employees, contractors, and third parties—prior to granting access to sensitive systems or data.

This control reinforces the importance of embedding pre-access security protocols within the organization's information security management system (ISMS). By assigning responsibilities before access is authorized, the organization ensures that individuals are informed of their obligations, acceptable use practices, and the consequences of misuse. This system-based onboarding step helps to mitigate insider risks, ensure compliance with internal policies, and align access rights with business and security objectives. It also supports a culture of accountability and prepares users to engage securely from the outset.

**Risk Statement**  
Without a defined policy outlining pre-access information security responsibilities, the organization risks introducing untrained or unaware users into sensitive environments. This creates a vulnerability within the system, where individuals may unknowingly violate security protocols or, in some cases, act with malicious intent. Lack of role-based responsibility awareness undermines accountability, increases the likelihood of data mishandling, and reduces the effectiveness of access control and incident prevention mechanisms.

**Business Impact**

* Higher probability of internal data misuse or negligent exposure of sensitive information
* Compliance risks due to failure to meet pre-access requirements in audits or legal reviews
* Operational disruptions linked to mishandled access or policy violations
* Reputational and financial damage from insider incidents or preventable breaches
* Weakened user accountability and reduced effectiveness of access controls

**ISO Control Alignment**  
**Primary Clause:**

* **A.5.2** – Information Security Roles and Responsibilities  
  Ensures that information security duties are clearly defined and communicated prior to access being granted.

**Supporting Clauses and Controls:**

* **A.5.1** – Policies for Information Security (Foundational policy structure)
* **A.6.1** – Screening (Verifies individuals' background and suitability for access)
* **A.6.2** – Terms and Conditions of Employment (Formalizes responsibilities in agreements)
* **A.6.3** – Information Security Awareness, Education, and Training (Pre-access training requirement)
* **A.8.2** – Information Classification (Ensures users understand sensitivity levels of accessible data)
* **A.9.1** – Access Control Policy (Formalizes preconditions and procedures for access rights)

**L.04 – Qualified Resourcing for Information Security (System-Based Perspective)**

**Control Description**  
Establish a formal policy that ensures all information security roles are supported by appropriately qualified, skilled, and adequately resourced personnel across the organization’s operational system.

Within a well-functioning information security management system (ISMS), human resource capability is as critical as technological controls. This policy supports a system-based approach to workforce planning by identifying the competencies required for various information security roles—whether internal or outsourced—and ensuring those capabilities are in place and maintained over time. It encompasses recruitment, training, resource allocation, and ongoing skill development to ensure the security function is sustainably resourced and aligned with evolving threat landscapes and organizational priorities.

**Risk Statement**  
If the organization lacks a structured policy ensuring that all information security functions are sufficiently staffed with qualified personnel, it risks systemic failure in the design, implementation, and operation of security controls. Skill gaps, resource shortages, or misaligned roles can lead to ineffective control execution, delayed incident response, and underperformance in audits or compliance reviews. Overreliance on under-resourced staff also increases the risk of fatigue, errors, and employee turnover—amplifying vulnerability across the organization.

**Business Impact**

* Misconfigured or poorly maintained controls that increase exposure to security breaches
* Delayed threat detection or incident response due to insufficient staffing
* Non-compliance with regulatory, contractual, or audit requirements
* Increased workload stress, leading to burnout and decreased accuracy
* Avoidable financial and reputational harm from preventable security failures

**ISO Control Alignment**  
**Primary Control:**

* **A.5.2** – Information Security Roles and Responsibilities  
  Mandates the assignment of roles and confirmation that they are resourced with appropriately skilled individuals.

**Supporting Clauses and Controls:**

* **A.5.1** – Policies for Information Security (Strategic planning and policy framework)
* **Clause 5.3** – Organizational Roles, Responsibilities, and Authorities  
  Requires top management to assign individuals with the authority and resources to ensure ISMS effectiveness.
* **Clause 7.2** – Competence  
  Requires ongoing evaluation and development of personnel competence impacting information security.

**L.05 – Define Employee (Including Contractor) Responsibilities for Information Security (System-Based Perspective)**

**Control Description**  
Establish a system-integrated policy that defines, communicates, and enforces the information security responsibilities of all employees, contractors, and third-party personnel.

A clear assignment of responsibilities across the organizational system is critical for maintaining accountability and consistency in information security practices. This policy ensures that all individuals—regardless of employment type—are aware of their specific duties, restrictions, and the consequences of non-compliance before they are entrusted with access to information systems. It aligns security roles with organizational objectives and embeds them into relevant business functions, contracts, onboarding processes, and performance expectations. This control promotes a culture of shared responsibility and supports ongoing compliance, risk reduction, and security awareness.

**Risk Statement**  
Failure to define and communicate information security responsibilities for employees and contractors introduces ambiguity into the system, weakening individual accountability and exposing the organization to internal threats. Without a unified understanding of expectations, personnel may unknowingly bypass controls, mishandle sensitive data, or fail to report security events—resulting in preventable incidents, operational disruption, or regulatory violations.

**Business Impact**

* Unauthorized access, data leakage, or accidental misuse of sensitive information
* Limited ability to trace actions or assign accountability during incidents
* Non-compliance with legal, regulatory, or contractual obligations
* Increased likelihood of insider threats, both intentional and accidental
* Diminished security culture and reduced stakeholder trust

**ISO Control Alignment**  
**Primary Clause:**

* **A.4** – Organizational Roles, Responsibilities, and Authorities  
  Requires the assignment of clear responsibilities and the provision of adequate resources to ensure effective performance in security roles.

**Supporting Clauses and Controls:**

* **A.5.1** – Policies for Information Security (Establishes the governing framework)
* **A.5.2** – Information Security Roles and Responsibilities (Specifies role-based duties and expectations)
* **A.6.1** – Screening (Supports responsible hiring and risk-based access)
* **A.6.2** – Terms and Conditions of Employment (Formalizes responsibilities contractually)
* **A.6.3** – Information Security Awareness, Education, and Training (Reinforces understanding of responsibilities)
* **A.7.2** – Competence (ISO/IEC 27001:2022 Clause 7 – Support) – Ensures individuals performing security-impacting tasks have appropriate skills and qualifications

**M.03 – Define and Implement a Repeatable Risk Assessment Process (System-Based Perspective)**

**Control Description**  
Establish a standardized, repeatable, and system-integrated risk assessment process that enables consistent identification, analysis, evaluation, and treatment of information security risks across the organization.

A repeatable risk assessment process is a foundational component of a mature information security management system (ISMS). It ensures that risk identification and evaluation follow a defined methodology and produce comparable results regardless of the department, project, or use case. This structured approach enables the organization to proactively address threats, support strategic security planning, and maintain compliance. By embedding the process into operational and governance workflows—such as project management, vendor selection, and change control—the organization achieves consistent visibility and responsiveness to evolving risks.

**Risk Statement**  
Without a defined and repeatable risk assessment process, the organization risks inconsistencies in identifying and addressing security threats. Ad-hoc or siloed assessments can result in critical risks being missed, underestimated, or inconsistently treated. This undermines decision-making, reduces the effectiveness of risk mitigation strategies, and increases the likelihood of incidents, regulatory breaches, or reputational damage.

**Business Impact**

* Overlooked vulnerabilities due to inconsistent or incomplete assessments
* Unaligned or ineffective risk treatment strategies across departments
* Non-compliance with legal, contractual, or audit requirements
* Misallocation of resources due to poor risk prioritization
* Increased organizational exposure to preventable threats

**ISO/IEC 27001:2022 Alignment**  
**Primary Clauses:**

* **Clause 6.1.2** – Information Security Risk Assessment  
  Requires the establishment of a repeatable risk assessment process with consistent outputs.
* **Clause 6.1.3** – Information Security Risk Treatment  
  Ties treatment decisions directly to assessment outcomes.
* **Clause 9.1** – Monitoring, Measurement, Analysis, and Evaluation  
  Supports continuous evaluation of risk and ISMS performance.

**Relevant Annex A Control:**

* **A.5.4** – Contact with Special Interest Groups  
  Optional support for external threat intelligence and horizon scanning inputs into the risk process.

**L.06 – Information Security Training Policy (System-Based Perspective)**

**Control Description**  
Establish and implement a formal policy that ensures all employees, contractors, and relevant third parties receive role-appropriate information security training as part of an integrated, system-wide security awareness program.

Effective information security relies on people as much as on technology. This policy defines a structured approach for ensuring all individuals within the organizational system understand security threats, safe practices, and their responsibilities. Training should be tailored to reflect organizational risk, individual roles, and regulatory requirements. By embedding training into onboarding, continuous development, and performance management cycles, the organization strengthens its overall security posture and reduces the likelihood of human error—the most common root cause of breaches.

**Risk Statement**  
Without a defined and consistently applied security training policy, personnel may lack the knowledge and awareness needed to identify and respond to security threats. This increases the risk of accidental data exposure, susceptibility to phishing, and inadequate incident handling. The absence of documented and auditable training processes can also lead to non-compliance with regulatory requirements and industry standards.

**Business Impact**

* Increased likelihood of successful phishing or social engineering attacks
* Mishandling of data due to a lack of secure behavior awareness
* Inadequate or delayed reporting of security incidents
* Audit findings or regulatory penalties for lack of training records
* Long-term erosion of the organization’s security culture

**ISO/IEC 27001:2022 Alignment**  
**Primary Clause:**

* **A.6.3** – Information Security Awareness, Education, and Training  
  Requires organizations to provide appropriate awareness and education to personnel based on their role and exposure to information security risk.

**Supporting Clauses and Controls:**

* **A.5.2** – Information Security Roles and Responsibilities  
  Training must align with assigned responsibilities.
* **Clause 7.2** – Competence  
  Ensures individuals have the skills necessary to perform tasks that affect information security.
* **Clause 7.3** – Awareness  
  Requires personnel to understand how their actions contribute to the effectiveness of the ISMS.
* **A.6.1** – Screening  
  Supports secure onboarding with an early introduction to security responsibilities.

**L.07 – Sensitive Information Identification and Classification Policy (System-Based Perspective)**

**Control Description**  
Establish and enforce a policy that ensures all sensitive information is clearly identified, labeled, and classified within the organizational system based on its confidentiality, integrity, and availability requirements.

Classifying and labeling information is a critical component of a well-structured information security management system (ISMS). This control ensures that sensitive data is systematically identified and appropriately handled according to defined risk levels and legal, regulatory, or contractual obligations. A consistent classification policy enables the organization to apply proportionate protection measures—such as access restrictions, encryption, and secure disposal—based on the sensitivity of the data. It also supports data lifecycle management, auditability, and alignment with data protection standards.

**Risk Statement**  
If the organization does not define and implement a policy for classifying and identifying sensitive information, it may result in inconsistent data handling practices, inappropriate application of controls, or undetected exposure of critical data. Without classification, it is difficult to prioritize protection efforts or demonstrate compliance, increasing the risk of breaches, operational disruption, and reputational damage.

**Business Impact**

* Exposure of confidential or regulated data due to improper handling
* Failure to meet compliance obligations (e.g., GDPR, HIPAA, CCPA)
* Increased difficulty managing data access, sharing, and retention
* Legal liability and financial penalties for non-compliance
* Reputational harm from publicized data misuse or breaches

**ISO/IEC 27001:2022 Alignment**  
**Primary Clause:**

* **A.8.2 – Information Classification**  
  Requires the classification of information assets based on business needs, legal obligations, and associated risks, including labeling and handling guidance.

**Supporting Clauses and Controls:**

* **A.8.1 – Responsibility for Assets**  
  Ensures asset ownership is defined and accountable for classification and protection.
* **A.5.1 – Policies for Information Security**  
  Provides the policy framework to support classification activities.
* **Clause 6.1.3 – Information Security Risk Treatment**  
  Uses classification to inform which controls are applied and where.
* **Clause 7.5 – Documented Information**  
  Ensures sensitive information is managed with appropriate protection across its lifecycle.

**Implementation Recommendations (System Integration View)**

✅ **Define Classification Levels**

* Examples: *Public, Internal, Confidential, Restricted*
* Each level should have clearly defined **handling**, **transmission**, and **retention** requirements.

✅ **Standardize Labeling Practices**

* Use templates, watermarks, metadata tags, or digital classification tools
* Apply automatic labeling in email, document management, and DLP systems where possible

✅ **Assign Ownership for Classification**

* Data owners are responsible for classification decisions and periodic reviews
* Incorporate classification into **asset inventories** and **data mapping exercises**

✅ **Integrate into Key Workflows**

* New document creation, project onboarding, third-party data sharing, and cloud storage
* Link to **access control**, **data loss prevention (DLP)**, and **encryption policies**

✅ **Train Staff and Reinforce Behavior**

* Include classification training during onboarding and awareness refreshers
* Use examples to clarify misclassification risks and real-world impact

✅ **Audit and Monitor Classification Accuracy**

* Include classification checks in internal audits
* Automate detection of unclassified or misclassified data through tooling

**M.04 – Secure Storage, Access, and Handling of Sensitive Information (System-Based Perspective)**

**Control Description**  
Establish and implement a policy that defines how sensitive information must be securely stored, accessed, and handled throughout its lifecycle, incorporating both technical and procedural safeguards.

This control ensures sensitive data is consistently protected within the organization’s information security management system (ISMS). The policy governs secure storage (e.g., encrypted databases, locked cabinets), controlled access (based on least privilege and need-to-know), and appropriate handling procedures (e.g., secure file transfers, disposal protocols). By integrating these requirements into both digital and physical environments, the organization reduces risk exposure and ensures that protective measures are applied according to data classification, regulatory standards, and operational needs.

**Risk Statement**  
Failure to define and enforce secure storage, access, and handling practices for sensitive information may result in unauthorized access, accidental exposure, or malicious misuse. Without clear guidance and control measures, the organization is more vulnerable to data breaches, non-compliance, and reputational harm.

**Business Impact**

* Compromise of confidential, proprietary, or regulated data
* Failure to pass security audits or meet compliance obligations (e.g., GDPR, HIPAA, PCI-DSS)
* Legal action or financial penalties due to negligent handling of sensitive information
* Operational disruption and costly incident response efforts
* Loss of trust among customers, partners, and stakeholders

**ISO/IEC 27001:2022 Alignment**  
**Primary Clauses & Controls:**

* **A.8.2 – Information Classification**  
  Ensures that data is classified to drive appropriate protection levels.
* **A.9.1 – Access Control Policy**  
  Restricts access to sensitive data based on role, responsibility, and necessity.
* **A.10.1 – Cryptographic Controls**  
  Requires the use of encryption and cryptographic methods to protect data in transit and at rest.
* **A.11.1 – Physical Security and Entry Controls**  
  Secures physical locations where sensitive data is stored or processed.
* **A.11.2 – Equipment Security**  
  Protects endpoints and infrastructure housing sensitive data.
* **A.11.2.7 – Secure Disposal or Reuse of Equipment**  
  Prevents data leakage from improperly disposed or repurposed hardware.
* **A.13.2 – Information Transfer**  
  Governs secure sharing and transmission of data across systems or with third parties.
* **Clause 7.5 – Documented Information**  
  Ensures that information is protected according to confidentiality, integrity, and availability requirements.

**Implementation Recommendations (System Integration View)**

✅ **Define Handling Requirements Based on Data Classification**

* Tie storage, access, and handling protocols directly to classification levels
* Use labeling to guide secure storage (e.g., encryption requirements for "Confidential" data)

✅ **Enforce Role-Based Access Controls (RBAC)**

* Implement “least privilege” and “need-to-know” principles
* Conduct periodic access reviews and revoke access promptly when no longer needed

✅ **Secure Storage and Transfer Methods**

* Encrypt data at rest (e.g., using AES-256) and in transit (e.g., TLS 1.2/1.3)
* Use secure file-sharing platforms with logging and expiration policies
* Physically secure sensitive documents and devices using access-controlled facilities

✅ **Define Clear Handling and Usage Protocols**

* Procedures for printing, emailing, storing, or transmitting sensitive data
* Prohibit storage of sensitive data on unauthorized removable media or personal devices

✅ **Train Personnel on Secure Handling Practices**

* Incorporate storage, access, and handling expectations into onboarding and awareness training
* Use real-life examples (e.g., misdirected emails, lost USB drives) to contextualize risks

✅ **Monitor and Enforce Compliance**

* Use DLP (Data Loss Prevention), logging, and monitoring tools to detect policy violations
* Integrate controls with incident response and audit functions for oversight and traceability

**M.05 – Data Loss Prevention (DLP) Policy (System-Based Perspective)**

**Control Description**  
Define and implement a system-integrated Data Loss Prevention (DLP) policy that governs the tools, procedures, and controls used to detect, monitor, and prevent unauthorized disclosure, movement, or misuse of sensitive information across the organization’s environment.

As part of a broader information security management system (ISMS), a DLP policy ensures that sensitive data is continuously protected—whether in use, in transit, or at rest—through automated mechanisms and contextual enforcement. The policy supports the identification and classification of critical data assets, enforces usage boundaries, and integrates with endpoint, network, email, and cloud systems to reduce data leakage risks. It ensures compliance with legal, regulatory, and contractual requirements while promoting a culture of security-by-design.

**Risk Statement**  
Without a defined and consistently enforced DLP policy, the organization risks accidental or intentional exposure of sensitive data. This includes the exfiltration of intellectual property, personal data, or confidential business information through unmanaged channels. Gaps in visibility or control over data flows significantly increase the likelihood of breaches, compliance failures, and reputational damage.

**Business Impact**

* Loss of sensitive or regulated data through accidental disclosure or malicious theft
* Regulatory fines or legal actions stemming from non-compliance (e.g., GDPR, HIPAA, PCI-DSS)
* Decreased stakeholder and customer confidence in data handling practices
* Increased cost of post-incident containment, remediation, and investigation
* Operational inefficiencies due to manual data governance and reactive threat mitigation

**ISO/IEC 27001:2022 Alignment**  
**Primary and Supporting Clauses & Controls:**

* **A.8.2 – Information Classification**  
  Ensures sensitive data is labeled and recognized by DLP systems for prioritized protection.
* **A.9.1 – Access Control Policy**  
  Restricts data access to authorized users, reducing risk of unauthorized sharing.
* **A.10.1 – Cryptographic Controls**  
  Enables encryption to complement DLP efforts, protecting data even if intercepted.
* **A.13.2 – Information Transfer**  
  Governs the secure movement of data across networks, systems, and third-party channels.
* **Clause 6.1.3 – Information Security Risk Treatment**  
  Incorporates DLP solutions into the mitigation strategy for data-related risks.

**Implementation Recommendations (System Integration View)**

✅ **Establish a DLP Governance Framework**

* Define **DLP objectives**, data protection goals, and enforcement zones
* Assign **data owners** and establish oversight responsibilities for sensitive data

✅ **Deploy and Configure DLP Technologies**

* Integrate DLP across **endpoints**, **network infrastructure**, **cloud services**, and **email gateways**
* Use **content inspection** and **contextual analysis** to detect data leakage attempts
* Enable **real-time alerts**, **automatic blocking**, or **quarantine actions** for high-risk violations

✅ **Link DLP to Classification and Access Policies**

* Align DLP rules with **information classification labels** (e.g., Confidential, Internal Use Only)
* Enforce **least privilege access**, file access tracking, and suspicious behavior analytics

✅ **Support with Awareness and Training**

* Educate staff on **acceptable data handling practices** and the purpose of DLP enforcement
* Include DLP topics in security awareness programs and role-based training

✅ **Monitor, Review, and Improve**

* Use **DLP dashboards and logs** to detect trends and recurring policy violations
* Perform **regular policy reviews** based on new threats, changes in data flows, or legal requirements
* Include DLP effectiveness in **management reviews** and **internal audit plans**

**M.06 – Off-line and Off-site Data Backup Policy (System-Based Perspective)**

**Control Description**  
Define and implement a comprehensive backup policy that ensures critical data is regularly copied, securely stored off-line, and maintained at off-site locations to support system recovery, data integrity, and business continuity.

As part of a resilient information security management system (ISMS), this control ensures that backup processes are standardized, verifiable, and integrated into broader continuity and recovery strategies. The policy should define backup frequency, retention schedules, encryption requirements, access restrictions, and testing procedures. Off-line backups (disconnected from active networks) safeguard against ransomware and insider threats, while off-site storage provides geographic redundancy to mitigate the impact of localized disasters.

**Risk Statement**  
If the organization fails to define, implement, and regularly test off-line and off-site backup procedures, it may be unable to recover from data loss events such as cyberattacks, system failures, or physical disasters. This could result in significant data unavailability, operational disruption, regulatory penalties, and reputational damage due to compromised integrity or continuity.

**Business Impact**

* Loss of mission-critical data with no reliable recovery point
* Inability to resume operations in the event of a disaster or ransomware attack
* Regulatory violations for failing to maintain data availability and integrity
* High recovery costs and productivity losses during extended downtimes
* Customer dissatisfaction and reputational damage due to service outages

**ISO/IEC 27001:2022 Alignment**  
**Primary Control:**

* **A.8.13 – Backup**  
  Requires the implementation of backup procedures that ensure data is protected and recoverable in the event of system or infrastructure failures.

**Related Clauses & Controls:**

* **A.8.1 – Responsibility for Assets**  
  Ensures backup data is managed with appropriate ownership and protections.
* **A.10.1 – Cryptographic Controls**  
  Mandates encryption of backup data to protect its confidentiality in transit and at rest.
* **A.17.1 – Information Security Continuity**  
  Aligns backup activities with broader disaster recovery and continuity strategies.
* **Clause 6.1.3 – Risk Treatment**  
  Supports backup implementation as a treatment for risks related to data availability and loss.

**Implementation Recommendations (System Integration View)**

✅ **Define Backup Requirements in Policy**

* **Frequency**: Daily, weekly, or near real-time based on criticality
* **Retention**: Define duration by data type (e.g., 30 days for logs, 7 years for financial records)
* **Encryption**: Apply strong encryption (e.g., AES-256) for storage and transit
* **Format**: Use secure, verifiable formats compatible with recovery tools

✅ **Implement Off-line and Off-site Storage Mechanisms**

* Store backups **off-line** (e.g., air-gapped, tape, or immutable storage) to prevent cyber compromise
* Use **off-site facilities** or cloud storage with geographic separation for disaster protection
* Validate that off-site storage providers meet **security and compliance requirements**

✅ **Integrate with Business Continuity & Disaster Recovery (BC/DR)**

* Ensure backups support **recovery time objectives (RTO)** and **recovery point objectives (RPO)**
* Include backup restoration testing in regular **BC/DR exercises**

✅ **Monitor, Verify, and Test Backups**

* Use **automated alerts** for backup failures or anomalies
* Perform **periodic test restores** to validate data integrity and recovery success
* Document and audit all backup activities and test results

✅ **Restrict Access and Monitor Usage**

* Limit access to backup systems to authorized personnel only
* Monitor and log all access and modifications to backup repositories

**L.08 – Access Control Policy (System-Based Perspective)**

**Control Description**  
Develop and implement a comprehensive, system-integrated access control policy that governs how access to information and information processing facilities is requested, authorized, provisioned, monitored, and revoked across the organization.

A robust access control policy is essential to the secure operation of an information security management system (ISMS). It defines the rules, responsibilities, and technical controls necessary to enforce the principle of least privilege, ensuring that only authorized individuals and systems have access to sensitive resources. This policy must address both **logical access** (e.g., system logins, applications, data repositories) and **physical access** (e.g., data centers, secure offices), covering all phases of the access lifecycle—from onboarding to offboarding.

**Risk Statement**  
Without a well-defined and enforced access control policy, unauthorized individuals may gain access to sensitive data or critical systems, increasing the risk of intentional or accidental compromise. Inconsistent or ad-hoc access provisioning and revocation practices can lead to excessive privileges, orphaned accounts, insider threats, and regulatory non-compliance.

**Business Impact**

* Data breaches or leaks caused by unauthorized access
* Disruption of operations due to compromised systems or accounts
* Regulatory penalties from failure to manage access securely (e.g., GDPR, HIPAA, SOX)
* Erosion of customer and stakeholder trust in the organization’s security controls

**ISO/IEC 27001:2022 Alignment**  
**Primary Clause:**

* **A.9 – Access Control**  
  Organizations must control access to ensure information is only accessible to authorized parties and prevent unauthorized use, modification, or disclosure.

**Key Supporting Controls:**

* **A.9.1.1 – Access Control Policy**  
  Requires a documented and enforced access control policy based on risk and business needs.
* **A.9.2 – User Access Management**  
  Covers user registration, access approval, privilege assignment, review, and removal.
* **A.9.3 – User Responsibilities**  
  Establishes user awareness around secure access practices (e.g., password hygiene, session management).
* **A.9.4 – System and Application Access Control**  
  Enforces technical mechanisms such as multi-factor authentication, access logs, and session timeouts.
* **A.5.2 – Information Security Roles and Responsibilities**  
  Ensures access-related roles are clearly assigned and managed.
* **A.6.1 – Screening**  
  Supports secure access provisioning by vetting individuals before granting access.
* **A.12.4 – Logging and Monitoring**  
  Ensures access events are recorded and reviewed for anomalies or policy violations.

**Implementation Recommendations (System Integration View)**

✅ **Define Access Categories and Rules**

* Establish access levels (e.g., general user, privileged admin, third-party)
* Link access rights to **job roles**, **data classification levels**, and **business need**

✅ **Integrate with Identity & Access Management (IAM) Systems**

* Automate user provisioning and deprovisioning through IAM
* Implement **role-based access control (RBAC)** and **least privilege** models
* Use **multi-factor authentication (MFA)** and **single sign-on (SSO)** for secure, centralized access

✅ **Standardize Access Lifecycle Processes**

* Clearly define procedures for **onboarding**, **role changes**, **temporary access**, and **offboarding**
* Periodically review access rights (e.g., quarterly access reviews)
* Maintain an **audit trail** for all access changes

✅ **Educate Users and Enforce Accountability**

* Train users on secure authentication, session management, and reporting suspicious access
* Include user access responsibilities in policy acknowledgments and training programs

✅ **Monitor and Audit Access Controls**

* Use **SIEM tools** or **access log analysis** to monitor for unauthorized or unusual access
* Include access control effectiveness in internal audits and **management reviews**

**M.07 – Asset Ownership and Access Control (System-Based Perspective)**

**Control Description**  
Establish a formal policy that ensures all information assets—such as data, applications, systems, and infrastructure—are identified, documented, and assigned to accountable owners who are responsible for classifying, securing, and managing access to those assets.

This control supports the broader information security management system (ISMS) by integrating asset ownership into core governance and risk management processes. Asset owners are responsible for defining classification levels, applying appropriate access controls, and ensuring the security posture of their assigned assets reflects business value, sensitivity, and risk exposure. This system-based approach ensures traceability, improves decision-making, and fosters accountability across all layers of the organization.

**Risk Statement**  
Failure to assign ownership and control over information assets weakens accountability and leads to inconsistent access control, inadequate protection, and unmanaged risks. Without clearly defined responsibilities, asset-related decisions may be delayed, misinformed, or overlooked—creating gaps in security and compliance coverage.

**Business Impact**

* Unauthorized access due to unclear or outdated permission structures
* Difficulty enforcing consistent security controls across the organization
* Failure to meet compliance obligations related to data protection and asset governance
* Increased risk of data leaks, system misuse, and operational disruption
* Reduced visibility and control over critical information assets

**ISO/IEC 27001:2022 Alignment**  
**Primary Control:**

* **A.8.1 – Responsibility for Assets**  
  Requires that all assets are inventoried and assigned owners accountable for their use and protection.

**Related Controls and Clauses:**

* **A.8.2 – Information Classification**  
  Asset owners are responsible for defining sensitivity and classification levels.
* **A.9.1 – Access Control Policy**  
  Connects asset ownership to access decisions, access reviews, and revocations.
* **A.5.2 – Information Security Roles and Responsibilities**  
  Ensures roles related to asset management and access control are well-defined.
* **A.5.1 – Policies for Information Security**  
  Provides a governance framework to guide ownership and control practices.
* **Clause 7.5 – Documented Information**  
  Requires documentation of asset-related responsibilities and protection mechanisms.

**Implementation Recommendations (System Integration View)**

✅ **Establish a Centralized Asset Inventory**

* Catalog all information assets by type (e.g., hardware, software, databases, documents)
* Include metadata: asset owner, classification, criticality, location, and retention period

✅ **Assign and Document Asset Ownership**

* Designate **asset owners** for each asset or asset group
* Include responsibilities for classification, access control, lifecycle management, and risk treatment
* Integrate asset ownership into job descriptions and onboarding

✅ **Enable Owner-Led Access Control**

* Require asset owners to approve access requests and review access permissions periodically
* Provide guidance and tools for owners to perform access reviews and validate least privilege

✅ **Support with Classification and Handling Standards**

* Empower asset owners with policy guidelines and templates for classification, storage, and usage
* Align asset classification with data protection and regulatory requirements

✅ **Train and Engage Asset Owners**

* Provide role-based training to asset owners on security responsibilities and access governance
* Reinforce accountability through audits, KPIs, and involvement in security reviews

✅ **Audit and Monitor Ownership Compliance**

* Periodically review the asset register to ensure ownership is current and responsibilities are fulfilled
* Include asset management in internal audit scopes and ISMS reviews

**L.09 – Cyber Essentials Scheme Plus Certification (System-Based Perspective)**

**Control Description**  
Maintain annual certification to the **Cyber Essentials Scheme Plus (CE+)** as part of the organization’s security assurance and continuous improvement system. This certification demonstrates the implementation of fundamental cybersecurity controls and validates them through independent testing.

As an integrated component of the organization’s information security management system (ISMS), CE+ provides a recognized benchmark for defending against common cyber threats. Achieving and maintaining this certification requires system-wide alignment with security best practices, including secure configuration, access control, malware protection, patch management, and boundary firewalls. It also serves as evidence of due diligence to clients, regulators, and partners, reinforcing trust and supporting contractual compliance.

**Risk Statement**  
Failure to maintain Cyber Essentials Scheme Plus Certification can expose the organization to preventable cyber threats and weaken stakeholder confidence in its security posture. Without annual reassessments, outdated controls may persist, and the organization risks non-compliance with client requirements, industry standards, or regulatory expectations.

**Business Impact**

* Reputational damage and loss of trust from customers and business partners
* Ineligibility for contracts or tenders that require CE+ as a minimum security standard
* Increased likelihood of successful cyberattacks due to lapses in basic protections
* Greater scrutiny from regulators or auditors
* Missed opportunities for demonstrating continual improvement of the ISMS

**ISO/IEC 27001:2022 Alignment**  
**Relevant Clauses and Controls:**

* **A.5.31 – Security Requirements for the Use of Suppliers**  
  Supports requiring certifications like CE+ from third parties or maintaining it internally to meet supply chain expectations.
* **A.5.1 – Policies for Information Security**  
  Certification supports policies that mandate adherence to recognized security frameworks.
* **A.6.3 – Information Security Awareness, Education, and Training**  
  CE+ requires user awareness and demonstrable application of controls like password hygiene, MFA, and malware defense.
* **A.12.1 – Operational Procedures and Responsibilities**  
  CE+ includes operational practices such as patch management and endpoint protection.
* **Clause 10 – Improvement**  
  Annual CE+ recertification supports the principle of continual improvement and reinforces control effectiveness within the ISMS.

**Implementation Recommendations (System Integration View)**

✅ **Integrate CE+ Requirements into Operational Security Processes**

* Align CE+ control areas with internal policies and technical standards (e.g., secure configuration, patch management)
* Use internal audits or GRC platforms to track CE+ readiness year-round

✅ **Designate CE+ Responsibility Within the ISMS Structure**

* Assign ownership for maintaining certification to an Information Security Lead or Risk & Compliance team
* Include CE+ status and readiness in management reviews and ISMS performance dashboards

✅ **Embed CE+ Requirements into Supplier and Contractual Obligations**

* Require CE+ (or equivalent) from critical suppliers or cloud service providers
* Reference CE+ compliance in RFPs, contracts, or vendor risk assessments

✅ **Conduct Pre-Audit Self-Assessments**

* Schedule internal reviews before formal CE+ assessments to identify and remediate gaps early
* Use assessment findings to inform ISMS improvements and update documentation

✅ **Leverage CE+ as a Communication Tool**

* Promote CE+ certification in security awareness campaigns, client communications, and compliance reporting
* Showcase certification in tenders and marketing to enhance competitive standing

**H.01 – Patch Management Metrics and Performance Assessment (System-Based Perspective)**

**Control Description**  
Establish and maintain a structured process for measuring, analyzing, and evaluating the effectiveness of the organization’s patch management program, ensuring timely remediation of software vulnerabilities in alignment with defined security policies.

As part of a resilient and data-driven ISMS, patch management must go beyond technical execution—it requires defined **metrics**, routine **performance reviews**, and integration with broader **risk and vulnerability management** processes. This includes tracking metrics such as patch deployment timelines, coverage rates, missed patches, and exception handling. Regular performance assessments allow the organization to validate control effectiveness, support audit readiness, and continuously refine the patching process based on emerging threats and operational realities.

**Risk Statement**  
If patch management performance is not measured or assessed against organizational policy, vulnerabilities may go undetected or remain unremediated. This increases exposure to known threats, undermines the organization's security posture, and can result in non-compliance with regulatory or contractual obligations—ultimately heightening the risk of costly incidents or service disruptions.

**Business Impact**

* Exploitation of known software vulnerabilities due to patching delays or oversight
* Regulatory fines or failed audits resulting from non-compliance with patching SLAs
* Disruption of business operations from preventable cyberattacks
* Reputational damage from breaches linked to outdated or vulnerable systems
* Increased cost and complexity in responding to security incidents

**ISO/IEC 27001:2022 Alignment**

**Primary Control:**

* **A.8.10 – Management of Technical Vulnerabilities**  
  Requires identification and remediation of vulnerabilities, including timely patching of systems.

**Related Clauses and Controls:**

* **A.12.1 – Operational Procedures and Responsibilities**  
  Integrates patching into daily IT and security operations.
* **Clause 9.1 – Monitoring, Measurement, Analysis, and Evaluation**  
  Supports the establishment of patching KPIs and performance metrics.
* **Clause 10 – Improvement**  
  Uses metric-driven assessments to identify gaps and drive corrective action.
* **A.12.6** (Legacy): Technical Vulnerability Management  
  Historical reference reinforcing the importance of systematic patch tracking.

**Implementation Recommendations (System Integration View)**

✅ **Define Patch Management Metrics**

* % of critical patches applied within SLA (e.g., 7 days)
* % of systems fully patched (monthly/quarterly basis)
* Average time-to-patch by severity level
* Number of exceptions and aging of unpatched systems
* Patch success/failure rate by platform or environment

✅ **Automate Tracking and Reporting**

* Use vulnerability management and patching tools (e.g., WSUS, SCCM, Qualys, Tenable, CrowdStrike, etc.)
* Integrate patching data with SIEM or GRC platforms for centralized visibility
* Generate dashboards and reports for security operations and management review

✅ **Establish Thresholds and Escalation Triggers**

* Define acceptable patching timelines based on **risk levels**
* Escalate overdue critical patches for executive or risk committee review
* Require documented justifications for patching exceptions

✅ **Link Metrics to Continuous Improvement**

* Include patch management metrics in **Clause 9** reviews (ISMS performance evaluation)
* Use trend analysis to identify recurring issues or underperforming systems/teams
* Initiate **corrective actions** for missed SLAs or recurring failures

✅ **Communicate and Align with Policy**

* Ensure patch metrics reflect commitments made in the **Information Security Policy** and supporting procedures
* Train IT and security staff on patching expectations and performance benchmarks

**H.02 – Secure Wireless Authentication (System-Based Perspective)**

**Control Description**  
Implement a policy and supporting technical controls to ensure all wireless network connections are secured through strong authentication, encryption, and access control mechanisms as part of the organization’s system-wide network security strategy.

Wireless networks represent an extended attack surface, often reachable beyond the organization’s physical perimeter. To manage this risk within the Information Security Management System (ISMS), organizations must authenticate all wireless connections using robust, industry-standard methods (e.g., **WPA2-Enterprise, WPA3**, RADIUS-based authentication, or certificate-based access). Secure wireless authentication must be enforced consistently across employee, guest, and IoT networks to prevent unauthorized access, protect sensitive data in transit, and reduce the risk of lateral movement by threat actors within the environment.

**Risk Statement**  
If the organization does not implement secure authentication for wireless access, attackers may exploit weak or unauthenticated connections to gain unauthorized network access. This can result in data interception, system compromise, and compliance failures, particularly where sensitive or regulated data is exposed via unsecured wireless infrastructure.

**Business Impact**

* Unauthorized access to internal systems or confidential information via unsecured Wi-Fi
* Man-in-the-middle (MitM) attacks through rogue access points or session hijacking
* Regulatory violations due to exposed personal or customer data
* Compromise of connected devices or lateral attacks across the network
* Erosion of trust among partners, regulators, and customers

**ISO/IEC 27001:2022 Alignment**

**Primary Controls:**

* **A.8.20 – Use of Network Services**  
  Requires that use of network services, including wireless, aligns with documented access control and authentication policies.
* **A.8.21 – Security of Network Services**  
  Ensures that proper authentication and encryption measures are applied to wireless and other network services.

**Supporting Clauses and Controls:**

* **A.9.4 – System and Application Access Control**  
  Reinforces the need for secure access to systems, including via wireless endpoints.
* **A.5.1 – Policies for Information Security**  
  Provides the overarching policy framework for enforcing wireless authentication standards.
* **A.6.1 – Network Security Management**  
  Addresses security architecture for wireless and wired networks, including segmentation and monitoring.

**Implementation Recommendations (System Integration View)**

✅ **Adopt Strong Wireless Authentication Standards**

* Enforce **WPA2-Enterprise** or **WPA3-Enterprise** with RADIUS-based authentication
* Use **802.1X** authentication with certificates or centralized identity providers
* Disable legacy protocols (e.g., WEP, WPA, or open SSIDs)

✅ **Segment Wireless Networks by Role and Risk**

* Separate **employee**, **guest**, and **IoT** networks
* Apply **network access controls** (e.g., VLAN segmentation, firewall policies)
* Restrict guest and unmanaged device access to internet-only routes

✅ **Integrate Wireless with Central Access Management Systems**

* Leverage **Active Directory**, **Azure AD**, or **Identity Providers (IdPs)** to control wireless authentication
* Monitor and log all wireless access events in **SIEM platforms**

✅ **Enforce Encryption for Wireless Data**

* Require **AES encryption** for all Wi-Fi connections
* Prohibit the use of unsecured wireless networks for corporate access

✅ **Audit and Review Wireless Access Controls Regularly**

* Conduct **wireless security assessments** and rogue AP detection
* Include wireless authentication in periodic **access control reviews**
* Test onboarding/offboarding processes for users and devices accessing wireless networks

✅ **Educate Users on Secure Wireless Use**

* Train staff to recognize and avoid connecting to unauthorized or untrusted wireless networks
* Include secure mobile device and remote access practices in awareness training

**L.10 – Policy for Removable Media Exchange (System-Based Perspective)**

**Control Description**  
Establish and enforce a formal policy governing the secure use and exchange of information via removable media devices (e.g., USB drives, external hard drives, optical discs) as part of the organization’s system-wide information security framework.

Removable media can introduce substantial security risks, including data leakage, malware infection, and unauthorized access. As such, this control defines the technical and procedural safeguards necessary to regulate their use—such as encryption requirements, approval workflows, endpoint scanning, physical labeling, and restricted access. These measures help ensure removable media usage is aligned with the organization’s information security management system (ISMS), data classification levels, and compliance obligations.

**Risk Statement**  
Without a defined and consistently applied policy for removable media, the organization faces elevated risk of data breaches, malware propagation, and unauthorized data exfiltration. Insecure use of removable devices can result in exposure of sensitive information, operational disruption, or violations of data protection laws.

**Business Impact**

* Loss or theft of unencrypted media leading to data exposure
* Introduction of malware into internal systems via infected devices
* Regulatory fines or audit failures due to non-compliant media handling
* Reputational harm following publicized incidents or third-party disclosures
* Increased IT and security workload for containment and remediation

**ISO/IEC 27001:2022 Alignment**

**Primary Control:**

* **A.8.11 – Use of Removable Media**  
  Requires that the organization implement controls to regulate the use of removable media and reduce the associated risks.

**Supporting Controls and Clauses:**

* **A.8.9 – Information Transfer**  
  Ensures secure exchange of data through all channels, including physical media.
* **A.8.10 – Management of Technical Vulnerabilities**  
  Includes requirements to scan removable devices and mitigate threats they may introduce.
* **A.9.4 – System and Application Access Control**  
  Reinforces the need for restricting and controlling access to devices and endpoints.
* **A.5.1 – Policies for Information Security**  
  Provides governance support for enforcing removable media controls within policies and procedures.

**Implementation Recommendations (System Integration View)**

✅ **Define Acceptable Use in Policy**

* Specify types of approved removable media
* Restrict usage to specific roles, devices, or departments based on business need
* Prohibit use of personal or unencrypted USB drives for company data

✅ **Enforce Encryption and Access Controls**

* Require full-disk encryption (e.g., AES-256) for any removable device storing sensitive data
* Apply password protection and automatic locking for inactive media
* Limit read/write permissions through endpoint control software

✅ **Implement Media Scanning Protocols**

* Enforce anti-malware scanning of all media before use
* Block unauthorized or unknown devices from auto-mounting on systems
* Use DLP (Data Loss Prevention) tools to monitor and control data movement

✅ **Log and Monitor Media Usage**

* Maintain an inventory of approved and issued removable devices
* Log all instances of data transfer to/from media and review regularly
* Integrate with SIEM or endpoint detection systems for real-time alerts

✅ **Educate Users on Secure Handling**

* Include removable media training in onboarding and refresher programs
* Reinforce physical security (e.g., locking devices, never leaving unattended media)
* Communicate incident reporting procedures in the event of loss or suspected misuse

✅ **Align with Data Classification and Transfer Policies**

* Prohibit high-sensitivity data from being transferred via removable media unless explicitly approved
* Ensure any transfer via physical media is logged, approved, and handled securely

This control focuses on the implementation of measures governing the usage of removable media, limiting unauthorized data transfers and protecting information from improper handling or compromise.

**L.11 – IT Estate Scope and Configuration Management (System-Based Perspective)**

**Control Description**  
Establish and maintain a system-integrated process for identifying, documenting, and managing the complete scope and configuration of the organization’s IT estate—including hardware, software, network components, and associated dependencies.

Effective configuration and asset management are foundational to a secure and resilient information security management system (ISMS). This control ensures the organization maintains a **comprehensive, accurate, and continuously updated inventory** of all information assets and their configuration states (e.g., versions, patch levels, deployment status). The inventory must support operational integrity, facilitate vulnerability and incident management, and enable compliance with internal controls and external standards. Configuration baselines should be established and monitored to detect unauthorized or unintended changes that could introduce risk.

**Risk Statement**  
Without defined processes to record and manage the scope and configuration of its IT assets, the organization is likely to experience security blind spots, uncontrolled system changes, and increased vulnerability exposure. Poor configuration tracking undermines the ability to respond to threats, remediate vulnerabilities, or ensure consistency across environments—leading to security incidents, operational inefficiencies, and non-compliance.

**Business Impact**

* Missed or delayed vulnerability remediation due to unknown or undocumented assets
* Increased frequency of misconfigurations, leading to service disruptions or data exposure
* Failure to meet audit and compliance requirements due to incomplete asset visibility
* Longer incident response and recovery times
* Increased operational costs from duplicated, shadow, or unmanaged assets

**ISO/IEC 27001:2022 Alignment**

**Primary Controls:**

* **A.5.9 – Inventory of Information and Other Associated Assets**  
  Requires organizations to identify and maintain an inventory of assets, assigning ownership and ensuring proper management.
* **A.8.9 – Configuration Management**  
  Requires organizations to manage configurations of hardware, software, and network components to preserve system integrity and prevent unauthorized changes.

**Supporting Clauses and Controls:**

* **A.5.1 – Policies for Information Security**  
  Provides policy-level guidance for asset and configuration management processes.
* **A.8.10 – Management of Technical Vulnerabilities**  
  Depends on an accurate inventory and configuration data to prioritize and deploy patches.
* **A.12.1 – Operational Procedures and Responsibilities**  
  Reinforces the need for documented processes for asset tracking, system configuration, and change control.
* **A.5.10 – Acceptable Use of Information and Associated Assets**  
  Ties system usage policies to known and managed assets in the configuration management system (CMS).

**Implementation Recommendations (System Integration View)**

✅ **Maintain a Centralized Asset and Configuration Management System (CMS)**

* Track hardware, software, virtual infrastructure, cloud assets, and endpoints
* Include configuration baselines (e.g., OS versions, patch levels, application builds)
* Establish links between assets and owners, data classifications, and network locations

✅ **Automate Discovery and Inventory Updates**

* Use asset discovery tools (e.g., SCCM, Lansweeper, JAMF, Tanium, or CMDBs) to detect new or changed systems
* Integrate with patching, vulnerability, and security monitoring platforms for full lifecycle visibility

✅ **Define Configuration Baselines and Exceptions**

* Establish secure configurations (e.g., CIS Benchmarks, DISA STIGs) for operating systems, databases, and devices
* Flag and log deviations; require formal approval for exceptions

✅ **Integrate with Change Management Processes**

* Ensure configuration changes go through formal change control
* Link configuration items (CIs) with change requests and implementation records

✅ **Conduct Regular Reviews and Reconciliations**

* Periodically validate the accuracy of the asset and configuration inventory
* Include configuration and scope accuracy in internal audits and management reviews

✅ **Enable Real-Time Alerts and Reporting**

* Use security tools to detect unauthorized changes to configurations or asset states
* Include IT estate metrics in ISMS dashboards and incident response planning

**M.08 – Policy for Handling Unpatched Vulnerabilities (System-Based Perspective)**

**Control Description**  
Establish and implement a policy to identify, assess, and manage unpatched vulnerabilities—particularly in situations where vendors have not yet released a fix—through compensating controls, documented risk acceptance, and continuous monitoring as part of the organization’s vulnerability management lifecycle.

Unpatched vulnerabilities, including zero-days or issues with no immediate countermeasures, require a coordinated and risk-informed response across the Information Security Management System (ISMS). This policy ensures a systematic evaluation of exposure, potential business impact, and appropriate interim actions such as system isolation, enhanced monitoring, or temporary mitigations. It enables the organization to maintain an acceptable security posture while awaiting permanent remediation and provides auditable evidence of due diligence.

**Risk Statement**  
If the organization lacks a defined process for evaluating and managing unpatched vulnerabilities, it increases the risk of delayed or inconsistent responses to exploitable threats. This may result in preventable data breaches, uncontrolled risk exposure, operational downtime, and non-compliance with legal, regulatory, or contractual obligations.

**Business Impact**

* Elevated risk of compromise from zero-day or known unpatched vulnerabilities
* Failure to demonstrate reasonable security measures during regulatory reviews or investigations
* Business disruption due to unplanned emergency responses or exploit activity
* Loss of stakeholder trust and increased exposure to financial and reputational damage

**ISO/IEC 27001:2022 Alignment**

**Primary Control:**

* **A.8.10 – Management of Technical Vulnerabilities**  
  Requires organizations to gather information about technical vulnerabilities, assess their risk exposure, and take timely, risk-informed actions—even when no vendor fix is available.

**Related Controls and Clauses:**

* **A.8.13 – Backup**  
  Supports contingency planning and recovery in the event an unpatched vulnerability is exploited.
* **A.12.1 – Operational Procedures and Responsibilities**  
  Reinforces the need for documented procedures covering exception handling and emergency response.
* **Clause 6.1.3 – Information Security Risk Treatment**  
  Guides the decision-making process around compensating controls or risk acceptance.
* **Clause 9.1 – Monitoring, Measurement, Analysis and Evaluation**  
  Supports the tracking of vulnerability mitigation efforts and effectiveness over time.

**Implementation Recommendations (System Integration View)**

✅ **Create a Formal Unpatched Vulnerability Handling Process**

* Define criteria for identifying and tracking vulnerabilities without available fixes (e.g., CVEs with no patch, zero-days)
* Require immediate **risk assessment** to evaluate likelihood, impact, asset exposure, and threat landscape

✅ **Determine and Apply Compensating Controls**

* Examples include:  
  • Network segmentation or isolation  
  • Restricting access to affected services  
  • Blocking specific ports, applications, or URLs  
  • Increasing logging and anomaly detection around vulnerable components
* Document and approve all interim mitigations through the change management process

✅ **Integrate with Existing Vulnerability and Incident Management Systems**

* Ensure vulnerabilities are tracked in your **risk register** or **vulnerability management platform**
* Assign accountability (e.g., system owner, ISMS lead) for status tracking and resolution

✅ **Review and Monitor**

* Establish **monitoring rules or alerts** for exploit attempts related to the unpatched issue
* Include high-risk unpatched vulnerabilities in **security dashboards** and **executive risk briefings**

✅ **Use Metrics to Drive Awareness and Decision-Making**

* Measure:  
  • Number of unpatched vulnerabilities  
  • Average duration of exposure  
  • Time to mitigation  
  • Effectiveness of compensating controls
* Include unpatched vulnerability metrics in **Clause 9.1** performance evaluations and **Clause 10** improvement actions

✅ **Document Risk Acceptance Where Needed**

* When no control is feasible or practical, require documented **risk acceptance** from relevant business or security leadership
* Set **expiration dates** for all risk acceptance decisions with scheduled re-evaluation

**M.09 – Secure Administrative Access with Multi-Factor Authentication (System-Based Perspective)**

**Control Description**  
Implement a policy requiring that all administrative access to systems and information assets be conducted using secure protocols and protected with multi-factor authentication (MFA), as part of a system-integrated privileged access management approach.

Administrative accounts carry elevated privileges and are prime targets for threat actors. This control ensures that such access is performed over **encrypted channels** (e.g., SSH, HTTPS, VPN with encryption) and secured with **MFA mechanisms**—such as one-time passcodes, hardware tokens, or biometric factors. This multi-layered control mitigates the risk of unauthorized access, credential theft, and lateral movement within critical systems, aligning with secure system engineering principles and supporting the organization’s ISMS.

**Risk Statement**  
Without enforcing secure access methods and MFA for administrative accounts, the organization is vulnerable to credential compromise and privilege abuse. Unprotected administrative access increases the attack surface and allows malicious actors to exploit systems at a high impact level, potentially resulting in data loss, operational failures, and regulatory breaches.

**Business Impact**

* Unauthorized access to core systems and sensitive data
* Credential-based attacks leading to system compromise or data exfiltration
* Audit failures and regulatory penalties due to insufficient access control
* Longer recovery times and costlier incident response
* Erosion of stakeholder trust due to administrative misuse or breach

**ISO/IEC 27001:2022 Alignment**

**Primary Control:**

* **A.8.23 – Secure Authentication**  
  Requires strong authentication for accessing systems—particularly for privileged accounts—emphasizing the use of MFA to reduce risk.

**Supporting Controls and Clauses:**

* **A.8.15 – Privileged Access Rights**  
  Mandates controlled assignment and monitoring of administrative privileges.
* **A.8.28 – Protection of Log Information**  
  Ensures administrator activities are logged and auditable for oversight and accountability.
* **A.8.27 – Secure System Engineering Principles**  
  Aligns secure administrative access with configuration hardening and secure access design.
* **Clause 6.1.3 – Information Security Risk Treatment**  
  Supports MFA as a control to mitigate risks related to privileged user threats.

**Implementation Recommendations (System Integration View)**

✅ **Enforce Secure Access Protocols**

* Require encrypted channels for all administrative sessions (e.g., **SSH, RDP over VPN, HTTPS**)
* Disable legacy or insecure protocols (e.g., Telnet, FTP)
* Require VPN or zero-trust network access for administrative interfaces

✅ **Apply Multi-Factor Authentication (MFA)**

* Enforce MFA for all privileged accounts—no exceptions
* Use strong second factors:  
  • TOTP apps (e.g., Google Authenticator, Microsoft Authenticator)  
  • FIDO2 hardware tokens (e.g., YubiKey)  
  • Biometrics (for supported endpoints)
* Integrate MFA with **identity providers (IdPs)** or **privileged access management (PAM)** platforms

✅ **Limit and Monitor Privileged Access**

* Implement **least privilege** and **just-in-time access** for administrative tasks
* Conduct regular reviews of privileged account entitlements
* Log all administrative actions and feed into a **SIEM** for real-time analysis

✅ **Include Administrative Access in Risk Assessments**

* Evaluate privileged access as part of threat modeling and vulnerability management
* Apply stricter controls for high-value systems such as domain controllers, financial systems, and production servers

✅ **Audit and Test Access Controls**

* Periodically test MFA bypass attempts and administrative access controls
* Include secure admin access in internal audits, penetration testing, and compliance reviews

**M.10 – Network Monitoring and Security Event Log Review (System-Based Perspective)**

**Control Description**  
Establish and implement a policy-driven, system-integrated approach for monitoring network activity and reviewing security event logs to proactively detect, analyze, and respond to anomalous or malicious behavior within the organization’s IT environment.

As part of a mature Information Security Management System (ISMS), this control ensures that **network traffic, user activity, and system-level events** are continuously captured, correlated, and analyzed through centralized logging and security information and event management (SIEM) tools. By reviewing logs from firewalls, IDS/IPS, endpoints, authentication systems, and critical infrastructure, organizations can detect suspicious patterns, escalate security incidents, and maintain forensic traceability. Effective monitoring also supports regulatory compliance and enables faster, more accurate incident response.

**Risk Statement**  
Without a defined policy and operational process for monitoring network behavior and reviewing security event logs, the organization is at risk of delayed detection, uncontrolled compromise, and incomplete incident response. Threats may go unnoticed, log evidence may be missing or tampered with, and forensic investigations may be hindered—leading to increased exposure and regulatory or reputational consequences.

**Business Impact**

* Missed or delayed identification of cyberattacks and insider threats
* Inability to effectively investigate and contain security incidents
* Breach of regulatory and contractual obligations (e.g., GDPR, PCI-DSS, ISO 27001)
* Reputational damage due to recurring or poorly handled security breaches
* Increased operational and legal costs related to incident recovery and reporting

**ISO/IEC 27001:2022 Alignment**

**Primary Controls:**

* **A.8.22 – Monitoring Activities**  
  Requires continuous monitoring of systems, networks, and services to detect abnormal behavior or potential attacks.
* **A.8.28 – Protection of Log Information**  
  Ensures logs are protected from unauthorized access, deletion, or modification.
* **A.8.29 – Logging**  
  Requires the logging of user activities, exceptions, and security events to support incident detection and response.

**Supporting Clauses and Controls:**

* **A.5.25 – Response to Information Security Incidents**  
  Ties monitoring to the organization’s ability to detect, respond to, and recover from security events.
* **Clause 9.1 – Monitoring, Measurement, Analysis and Evaluation**  
  Promotes regular evaluation of log review and monitoring effectiveness to support ongoing risk mitigation.

**Implementation Recommendations (System Integration View)**

✅ **Centralize Logging and Correlation**

* Implement a **SIEM solution** (e.g., Splunk, QRadar, Microsoft Sentinel) to aggregate and correlate logs
* Include logs from key systems: firewalls, VPN, servers, Active Directory, email gateways, cloud services, EDR/XDR platforms

✅ **Define Logging and Monitoring Policies**

* Set **retention periods**, **log sources**, and **minimum data points** (e.g., user IDs, IP addresses, timestamps)
* Categorize log events by severity and risk (e.g., failed logins, privilege escalation, suspicious traffic)

✅ **Automate Detection and Alerting**

* Configure real-time alerts for high-risk activities, including brute-force attempts, unauthorized access, or lateral movement
* Apply behavioral analytics and anomaly detection to improve detection of unknown threats

✅ **Conduct Regular Log Reviews**

* Define a schedule for **manual and automated review of key logs** (e.g., daily for high-risk systems)
* Review logs for both **security anomalies** and **policy violations** (e.g., unauthorized data transfers, blocked access attempts)

✅ **Protect and Archive Logs Securely**

* Store logs in **tamper-proof, access-controlled repositories**
* Use **encryption** and **role-based access** to ensure only authorized personnel can access sensitive logs

✅ **Integrate Monitoring with Incident Response**

* Ensure alerts feed into the **incident response process**, with clear thresholds for escalation
* Use logs as part of **forensic analysis**, root cause identification, and evidence collection

✅ **Report and Improve**

* Include log review metrics and SIEM effectiveness in **ISMS performance reviews (Clause 9.1)**
* Continuously refine logging rules, event sources, and alert thresholds based on lessons learned and evolving threats

**H.03 – Enhanced Network Monitoring Beyond Signature-Based Detection (System-Based Perspective)**

**Control Description**  
Implement advanced network monitoring capabilities that go beyond traditional signature-based detection by incorporating behavioral analytics, anomaly detection, and machine learning to identify novel, evasive, or zero-day threats within the organization’s network environment.

As part of a comprehensive and adaptive Information Security Management System (ISMS), this control ensures the organization is equipped to detect both **known** and **unknown attack patterns**. Signature-based tools are effective for recognizing established threats, but they offer limited defense against sophisticated techniques that evade known indicators. To address this gap, enhanced monitoring tools—such as **Network Detection and Response (NDR)** platforms, **UEBA (User and Entity Behavior Analytics)**, and **AI-powered threat detection engines**—should be deployed to baseline normal behavior and identify deviations that may signal compromise, insider threats, or advanced persistent threats (APTs).

**Risk Statement**  
Failure to augment traditional signature-based detection with advanced network monitoring techniques significantly limits the organization’s visibility into emerging threats. This can result in delayed detection of stealthy or targeted attacks, allowing adversaries to operate undetected within the network—leading to data compromise, business disruption, or regulatory violations.

**Business Impact**

* Inability to detect novel or polymorphic attacks, increasing breach risk
* Prolonged attacker dwell time due to lack of behavioral or anomaly-based detection
* Delayed incident response and greater damage scope
* Failure to meet expectations for proactive threat detection in audits and assessments
* Reputational harm from missed threats or long-undetected compromises

**ISO/IEC 27001:2022 Alignment**

**Primary Controls:**

* **A.8.22 – Monitoring Activities**  
  Requires monitoring of systems and networks to detect anomalies, supporting the integration of behavioral or AI-driven analytics.

**Supporting Controls and Clauses:**

* **A.8.29 – Logging**  
  Provides the data foundation needed for effective behavioral baselining and anomaly detection.
* **A.5.25 – Response to Information Security Incidents**  
  Emphasizes early detection and response—strengthened by visibility into unusual or suspicious behavior.
* **A.8.27 – Security Monitoring** *(if defined in the ISMS context)*  
  Encourages diverse, adaptive detection techniques beyond static rule sets, such as threat intelligence feeds, ML, and heuristic analysis.

**Implementation Recommendations (System Integration View)**

✅ **Deploy Complementary Detection Technologies**

* Implement **Network Detection and Response (NDR)** tools to observe east-west traffic and detect anomalies
* Use **UEBA solutions** to baseline and monitor user behavior, identifying account misuse or compromise
* Leverage **machine learning-based detection engines** integrated into SIEM, EDR, or XDR platforms

✅ **Define Behavioral Baselines**

* Establish baselines for user logins, network traffic volume, data access frequency, and inter-system communications
* Use deviation thresholds to trigger alerts for unusual behavior (e.g., data exfiltration attempts, lateral movement)

✅ **Integrate with Threat Intelligence and Contextual Enrichment**

* Correlate behavioral anomalies with external threat intelligence (e.g., known APT tactics, IOCs)
* Prioritize alerts based on context, asset criticality, and anomaly confidence level

✅ **Tune Alert Thresholds and Reduce Noise**

* Implement feedback loops to refine detection algorithms and reduce false positives
* Prioritize alerts by risk severity and business impact

✅ **Ensure Log and Data Availability for Detection Engines**

* Ingest logs from network devices, cloud workloads, endpoints, identity providers, and OT/IoT systems
* Ensure log formats, retention policies, and access controls support ongoing detection and forensic analysis

✅ **Embed into Incident Response and Continuous Improvement**

* Route behavior-based alerts into the incident response process
* Use post-incident reviews to update behavioral models and detection rules
* Include detection maturity as part of **Clause 9.1** (ISMS performance monitoring) and **Clause 10** (improvement)

**H.04 – Application Firewalls for Critical Servers (System-Based Perspective)**

**Control Description**  
Implement application-layer firewall controls—such as Web Application Firewalls (WAFs)—to protect critical servers by inspecting, filtering, and validating application traffic in real time. These controls form part of a system-integrated, defense-in-depth strategy to detect and block threats that traditional network firewalls may miss.

Critical systems that host sensitive applications or data are frequent targets of application-level attacks such as **SQL injection**, **cross-site scripting (XSS)**, **file inclusion**, and **protocol abuses**. Unlike traditional firewalls that filter based on IP and port rules, **application firewalls evaluate the behavior and structure of traffic**, enforcing granular rules and validating the legitimacy of requests at the application level. Positioned logically in front of high-risk systems (e.g., web servers, APIs, CRM/ERP platforms), application firewalls can actively prevent exploitation attempts and reduce the surface area exposed to internet-facing threats.

**Risk Statement**  
Without application firewalls, critical systems are exposed to sophisticated attacks that bypass traditional controls. The lack of deep inspection of application-layer traffic increases the likelihood of successful intrusions, data compromise, and regulatory non-compliance. This can result in significant operational, financial, and reputational damage.

**Business Impact**

* Successful exploitation of web-based applications or APIs through input manipulation or protocol abuse
* Breaches of systems containing regulated or sensitive customer data
* Increased costs related to incident response, data loss, and remediation
* Compliance failures tied to insufficient application-level security controls
* Long-term reputational harm and erosion of trust among clients, partners, or regulators

**ISO/IEC 27001:2022 Alignment**

**Primary Controls:**

* **A.8.26 – Application Security Requirements**  
  Ensures that applications and associated infrastructure are protected through security measures appropriate to identified threats, including WAFs.

**Supporting Controls:**

* **A.8.21 – Security of Network Services**  
  Mandates protection of network and application services, which WAFs enhance through application-layer visibility and enforcement.
* **A.8.23 – Secure Authentication**  
  Relevant when WAFs integrate with identity systems to enforce authentication or session validation.
* **A.8.22 – Monitoring Activities**  
  WAFs contribute to proactive detection through logging, real-time alerting, and integration with SIEM solutions.

**Implementation Recommendations (System Integration View)**

✅ **Deploy WAFs in Front of Public-Facing and Critical Internal Applications**

* Use **WAF appliances**, **cloud-based WAFs** (e.g., AWS WAF, Azure WAF, Cloudflare), or **host-based WAFs** for on-premises or hybrid infrastructure
* Position in **reverse proxy mode** to inspect inbound traffic before it reaches the server

✅ **Define Application-Layer Rulesets and Security Policies**

* Protect against OWASP Top 10 vulnerabilities (e.g., XSS, injection attacks, insecure deserialization)
* Apply **custom rules** based on application behavior, expected input types, or URL patterns
* Block malformed requests, bots, and known malicious payloads

✅ **Integrate WAF Logging and Monitoring**

* Feed WAF logs into your **SIEM** for centralized analysis and correlation with endpoint or network data
* Configure alerts for repeated attack patterns, brute-force attempts, or blocked request spikes

✅ **Regularly Update and Test WAF Configurations**

* Apply **threat intelligence feeds** or **automatic rule updates** to respond to emerging exploits
* Use **pen testing or red teaming** to evaluate WAF effectiveness and fine-tune rules

✅ **Align with Change and Incident Response Processes**

* Document WAF configurations and update them as part of **change control** for application deployments
* Include WAF events in the **incident response lifecycle** for quicker triage and mitigation

✅ **Evaluate Authentication & Session Controls at the WAF Layer**

* Enable **pre-authentication checks** (e.g., block unauthenticated access to admin panels)
* Integrate with **SSO**, **MFA**, or **identity-aware proxies** to control access at the edge

**H.05 – Network-Based Intrusion Detection Systems (IDS) (System-Based Perspective)**

**Control Description**  
Deploy and maintain network-based Intrusion Detection Systems (IDS) at critical ingress and egress points within the organization’s IT environment to detect, log, and alert on suspicious traffic patterns, known attack signatures, and policy violations in real time.

As part of a layered defense strategy embedded within the organization’s Information Security Management System (ISMS), IDS sensors enhance visibility into network activity and provide early warning capabilities for unauthorized access attempts, malware propagation, data exfiltration, and misuse of internal services. By inspecting traffic at the **network perimeter, demilitarized zones (DMZs), and internal segmentation points**, IDS solutions serve as a foundational component of proactive threat detection. Regular signature updates, centralized alert management, and log correlation ensure the IDS contributes to broader incident detection, response, and compliance efforts.

**Risk Statement**  
Failure to deploy and properly maintain IDS sensors at key network boundaries increases the likelihood that malicious activity will go unnoticed. Without real-time traffic inspection and alerting, organizations may face delayed breach detection, insufficient forensic data, and inadequate incident response—leading to increased exposure, legal liability, and reputational damage.

**Business Impact**

* Limited visibility into malicious or anomalous network traffic
* Delayed detection of attacks such as lateral movement, command and control (C2), or data exfiltration
* Failure to comply with regulatory mandates or industry standards requiring network monitoring
* Increased incident response time and potential legal and financial consequences
* Long-term erosion of customer trust and business continuity disruption

**ISO/IEC 27001:2022 Alignment**

**Primary Controls:**

* **A.8.22 – Monitoring Activities**  
  Requires continuous monitoring of network environments to detect unauthorized or anomalous activity, which IDS systems directly support.

**Supporting Controls:**

* **A.8.29 – Logging**  
  Ensures that network events captured by IDS are retained, correlated, and reviewed for incident investigation.
* **A.5.25 – Response to Information Security Incidents**  
  Relies on real-time alerts from IDS to detect, triage, and respond to security incidents effectively.
* **A.8.21 – Security of Network Services**  
  Requires that organizations secure internal and external network services with layered detection and protection mechanisms.

**Implementation Recommendations (System Integration View)**

✅ **Strategic Deployment of IDS Sensors**

* Place IDS sensors at key **ingress and egress points**, such as:  
  • Internet-facing gateways  
  • Cloud interconnects and VPN endpoints  
  • Internal network segmentation points (e.g., between departments or data centers)
* Use **SPAN ports, network taps**, or inline deployment based on architecture and risk tolerance

✅ **Keep Signature Libraries and Detection Rules Updated**

* Subscribe to **vendor signature feeds** and update automatically (e.g., Snort, Suricata, Zeek/Zeek-based tools)
* Supplement with **custom signatures** based on known threats or internal security policies

✅ **Integrate IDS with SIEM and SOC Workflows**

* Forward IDS alerts to your **Security Information and Event Management (SIEM)** solution for correlation and investigation
* Define response playbooks within the **incident response plan** to address IDS-detected events

✅ **Tune IDS for High-Fidelity Detection**

* Regularly **fine-tune detection thresholds and rules** to reduce false positives
* Use **anomaly detection** or **behavioral heuristics** alongside signature-based matching

✅ **Ensure Log Retention and Integrity**

* Store IDS logs securely with **timestamping, encryption, and access controls**
* Maintain logs in accordance with **retention policies and regulatory requirements**

✅ **Monitor IDS Performance and Coverage**

* Include IDS status and event volumes in **security dashboards and ISMS reviews**
* Periodically **test detection efficacy** through red teaming, simulated attacks, or vulnerability assessments

**L.12 – User Account Access Rights Management (System-Based Perspective)**

**Control Description**  
Implement a comprehensive policy and supporting systems to govern the lifecycle of user account access—ensuring that individuals are granted, modified, and revoked access to systems, applications, and data strictly in alignment with their role-based responsibilities.

This control enforces **least privilege** and **need-to-know principles** across the organization’s Information Security Management System (ISMS). It covers onboarding (provisioning), change (modification), and offboarding (revocation) events, and integrates with identity and access management (IAM), HR systems, and asset ownership to ensure secure, auditable access governance. Regular reviews of user access are essential to identify privilege creep, orphaned accounts, and misalignments between access rights and business needs.

**Risk Statement**  
Without clearly defined and enforced processes for managing user account access rights, organizations risk unauthorized access, insider threats, and regulatory violations. Poor account hygiene can lead to lingering access for former employees, over-privileged accounts, and gaps in auditability—creating vulnerabilities that can be exploited by internal or external actors.

**Business Impact**

* Increased potential for data misuse or unauthorized disclosure due to excessive access
* Inability to trace user actions during investigations or audits
* Greater exposure to insider threats and lateral movement post-compromise
* Non-compliance with security frameworks requiring access control (e.g., ISO 27001, GDPR, SOX)
* Financial and reputational costs resulting from access-related incidents

**ISO/IEC 27001:2022 Alignment**

**Primary Controls:**

* **A.8.15 – Privileged Access Rights**  
  Ensures privileged access is tightly controlled, documented, and justified.
* **A.8.16 – Use of Secret Authentication Information**  
  Supports secure handling of credentials, such as passwords or security tokens.
* **A.8.17 – Information Access Restriction**  
  Requires access to be limited based on business and security requirements.
* **A.8.18 – Access Rights**  
  Mandates that access rights be reviewed and updated regularly, especially during job or role changes.

**Related Controls and Clauses:**

* **A.5.2 – Information Security Roles and Responsibilities**  
  Aligns user access rights with defined responsibilities.
* **A.5.9 – Inventory of Information and Other Associated Assets**  
  Requires access to be mapped to specific systems and asset ownership.

**Implementation Recommendations (System Integration View)**

✅ **Establish Role-Based Access Control (RBAC)**

* Define user roles with associated minimum required access rights
* Create access profiles based on job functions, departments, or system responsibilities
* Use RBAC in IAM systems to automate provisioning and restrict deviation from approved roles

✅ **Automate Onboarding and Offboarding Workflows**

* Integrate IAM or identity governance tools (e.g., Okta, Azure AD, SailPoint) with HR systems for real-time updates
* Automatically provision access on start date, and deprovision access immediately upon termination or role change
* Remove or disable inactive and orphaned accounts regularly

✅ **Enforce Periodic Access Reviews**

* Schedule **quarterly or semi-annual access recertification** for privileged and high-risk systems
* Require system and data owners to review user access and validate continued business need
* Track review completion and maintain audit trails

✅ **Control and Monitor Privileged Accounts**

* Segregate admin accounts from user accounts
* Apply multi-factor authentication (MFA) and session logging for all privileged users
* Use Privileged Access Management (PAM) solutions to manage access duration and approval

✅ **Secure Authentication Practices**

* Enforce strong password policies and secure authentication mechanisms (e.g., MFA, SSO)
* Educate users on secure credential handling and phishing prevention

✅ **Log, Monitor, and Report on Account Activity**

* Monitor account activity for anomalies such as privilege escalation, unusual login times, or access outside of scope
* Integrate account events into SIEM for real-time alerting and incident correlation

**M.11 – Monitoring User Account Usage and Managing Access Changes (System-Based Perspective)**

**Control Description**  
Establish and enforce a policy and supporting technical controls to monitor user account activity, detect anomalies, and ensure timely updates to access rights throughout the user lifecycle—from onboarding to role changes and offboarding.

This control supports **least privilege enforcement**, **insider threat detection**, and **real-time security monitoring** by ensuring that user access is both appropriate and traceable. It combines continuous usage analysis (e.g., login behavior, privilege use, system access patterns) with structured access change management to ensure that access remains aligned with job responsibilities and that deviations or misuse are quickly identified and addressed. Integrated logging, audit trails, and automated alerts strengthen accountability and support forensic investigations in the event of an incident.

**Risk Statement**  
Without systematic monitoring of user account activity and timely management of access changes, the organization may fail to detect unauthorized behavior, retain outdated privileges, or allow former employees to maintain access. This can result in data breaches, misuse of resources, regulatory violations, and reputational harm.

**Business Impact**

* Misuse of excessive or outdated access rights leading to data leaks or sabotage
* Delays in identifying compromised or misused accounts
* Inability to meet compliance requirements related to access oversight (e.g., GDPR, ISO 27001, HIPAA)
* Increased incident recovery time and investigation complexity
* Loss of customer and stakeholder trust

**ISO/IEC 27001:2022 Alignment**

**Primary Controls:**

* **A.8.15 – Privileged Access Rights**  
  Requires heightened monitoring and control of elevated accounts.
* **A.8.18 – Access Rights**  
  Mandates regular review and adjustment of access rights as roles or responsibilities change.
* **A.8.22 – Monitoring Activities**  
  Calls for monitoring of systems and users to detect suspicious behavior and policy violations.
* **A.8.29 – Logging**  
  Ensures user activities are captured and retained to support auditability and investigation.

**Supporting Clause:**

* **Clause 9.1 – Monitoring, Measurement, Analysis and Evaluation**  
  Supports the use of access-related metrics and analytics to evaluate ISMS performance and detect abnormal usage patterns.

**Implementation Recommendations (System Integration View)**

✅ **Monitor User Activity with Contextual Awareness**

* Track login times, IP locations, unusual system access, file movement, and privilege escalations
* Implement **User and Entity Behavior Analytics (UEBA)** or integrate with **SIEM platforms** to detect deviations from baseline behavior

✅ **Automate Access Change Workflows**

* Use **Identity and Access Management (IAM)** or **Identity Governance and Administration (IGA)** platforms to auto-trigger access reviews and deprovisioning based on HR role changes
* Require **manager or asset owner approval** for changes to access entitlements

✅ **Establish Access Review Schedules**

* Conduct regular (e.g., quarterly) **access recertification** for all accounts—especially those with privileged or high-risk access
* Validate that access is still needed and appropriate based on current job functions

✅ **Define and Enforce Activity Logging Policies**

* Ensure logging covers:  
  • Logins/logouts  
  • Admin activity  
  • File access/modification  
  • System/resource usage
* Retain logs in **secure, tamper-evident systems** per regulatory and organizational retention requirements

✅ **Set Up Alerts for Suspicious Activity**

* Alert on:  
  • Multiple failed login attempts  
  • Off-hours access  
  • Sudden access to unfamiliar systems or data  
  • New privilege grants without justification
* Escalate alerts to security operations or compliance for triage

✅ **Offboard Accounts Promptly**

* Immediately revoke access for terminated users or transfers
* Implement a **zero-trust access model** for sensitive systems and data

✅ **Report and Improve**

* Include access usage metrics in **Clause 9.1 reporting**:  
  • Number of outdated accounts  
  • Number of access changes/month  
  • Number of anomalies detected
* Use findings to inform **Clause 10** continual improvement

**M.12 – Policy for Remote Access Control (System-Based Perspective)**

**Control Description**  
Establish and enforce a remote access control policy that governs how employees, contractors, and third parties securely connect to the organization’s internal systems and services from external or offsite locations. This includes specifying approved connection methods, authentication mechanisms, endpoint security requirements, and monitoring practices.

As part of a zero-trust security model and the broader Information Security Management System (ISMS), remote access must be managed with **multi-layered safeguards** to prevent unauthorized entry and mitigate threats such as stolen credentials, compromised endpoints, and unauthorized data access. Remote sessions should be routed through **encrypted channels** (e.g., VPN, TLS, SSH), validated with **multi-factor authentication (MFA)**, and monitored for unusual behavior. Endpoint compliance checks and session restrictions should also be enforced to prevent malware infiltration or lateral movement.

**Risk Statement**  
Failure to define and implement secure remote access policies exposes the organization to elevated risk of unauthorized access, data exfiltration, and service disruption. Without strong controls and oversight, remote connections can become a blind spot for threat actors and a source of non-compliance with regulatory standards.

**Business Impact**

* Unauthorized system access from unsecured or compromised remote endpoints
* Exposure of sensitive or regulated data across unencrypted or uncontrolled channels
* Remote exploitation of privileged accounts leading to system compromise
* Audit failures due to inadequate access control enforcement
* Reputational and financial losses from breaches involving remote access pathways

**ISO/IEC 27001:2022 Alignment**

**Primary Controls:**

* **A.8.20 – Use of Network Services**  
  Ensures the secure use of network services, including remote access channels.
* **A.8.21 – Security of Network Services**  
  Mandates the protection of remote access protocols using encryption and authentication mechanisms.
* **A.8.15 – Privileged Access Rights**  
  Requires enhanced controls for remote users with elevated privileges.
* **A.8.23 – Secure Authentication**  
  Requires robust user authentication, including MFA, especially for remote access.

**Implementation Recommendations (System Integration View)**

✅ **Define and Enforce Secure Remote Access Methods**

* Approve only secure connection protocols (e.g., **VPN with TLS, SSH, RDP over gateway, Zero Trust Network Access**)
* Prohibit direct access to internal systems over the public internet
* Require **gateway-based access controls** and **endpoint posture checks**

✅ **Apply Multi-Factor Authentication (MFA) to All Remote Access**

* Enforce MFA for all remote users, including internal staff, vendors, and contractors
* Integrate MFA with **identity providers (IdPs)** and **SSO platforms** for streamlined control

✅ **Implement Endpoint Security Requirements**

* Require up-to-date antivirus, disk encryption, and OS patches on devices used for remote access
* Use **network access control (NAC)** or **endpoint compliance checks** before granting access
* Restrict access from personal or non-compliant devices

✅ **Monitor and Log Remote Sessions**

* Capture logs of session initiation, duration, accessed systems, and user actions
* Route logs to a **SIEM** for alerting on anomalies (e.g., access outside of working hours, failed logins, data transfers)

✅ **Control and Review Remote Access Privileges**

* Limit remote access by default; grant based on business justification
* Regularly review and revoke access for inactive accounts, completed projects, or contractor offboarding
* Segregate remote access privileges from internal administrative access

✅ **Support Incident Response and Compliance**

* Include remote access pathways in threat modeling and risk assessments
* Simulate remote access breach scenarios as part of tabletop exercises and incident response plans
* Maintain documentation to demonstrate alignment with ISO 27001, GDPR, HIPAA, or industry-specific requirements

**M.13 – Authorized Software Usage Policy (System-Based Perspective)**

**Control Description**  
Implement a centralized, policy-driven control framework to manage the evaluation, approval, deployment, and lifecycle monitoring of all software used within the organization. This policy ensures that only **vetted, licensed, secure, and authorized software** is installed and executed across all corporate systems and devices.

Through integration with **Endpoint Management Systems**, **Software Asset Management (SAM)** tools, and **Configuration Management Databases (CMDBs)**, this policy helps prevent unauthorized applications, mitigate exposure to malware or unsupported software, and maintain alignment with licensing and compliance requirements. It defines clear roles and workflows for software requests, risk assessment, approval, deployment, auditing, and decommissioning, reducing operational risks and maintaining system integrity.

**Risk Statement**  
Without structured controls on software usage, unauthorized or insecure software may be introduced into the environment, increasing the risk of malware infection, data loss, legal non-compliance, and performance degradation. These risks are amplified when software is installed outside of IT governance or bypasses standard review procedures.

**Business Impact**

* Malware infections or data breaches caused by unauthorized or malicious software
* Legal consequences from license violations or pirated application usage
* Disruption of operations due to compatibility issues or unstable applications
* Reduced ability to track, patch, or secure applications across the enterprise
* Audit failures and reputational damage from policy non-compliance

**ISO/IEC 27001:2022 Alignment**

**Primary ISO Controls:**

* **A.8.30 – Installation of Software on Operational Systems**  
  Ensures all software installations are authorized and securely deployed.
* **A.8.24 – Use of Privileged Utility Programs**  
  Controls the use of high-risk administrative or debugging tools.
* **A.8.25 – Secure Coding Practices** *(for internally developed software)*  
  Requires secure, authorized libraries and tools be used during development.
* **A.5.10 – Acceptable Use of Information and Associated Assets**  
  Supports software usage aligned with internal and external compliance requirements.

**Implementation Recommendations (System Integration View)**

✅ **Centralize Software Inventory and Governance**

* Use **Software Asset Management (SAM)** or **CMDB tools** to maintain a real-time inventory of all software assets
* Tag software by risk level, license type, criticality, owner, and usage status
* Conduct regular audits to detect unapproved or unsupported applications

✅ **Enforce Software Authorization and Approval Workflow**

* Require formal **software requests** for all new applications
* Review requests against:  
  • Business justification  
  • Security and licensing posture  
  • Compatibility and support model
* Only allow deployment via **authorized IT tools or scripts**

✅ **Restrict User-Level Installation and Execution**

* Remove or restrict local administrative rights for non-IT users
* Use **application whitelisting** (e.g., Microsoft AppLocker, Intune, JAMF) or **deny-by-default execution policies**
* Monitor and alert on unauthorized installations or portable application execution

✅ **Control Use of Privileged or Technical Tools**

* Maintain a separate approval list for **admin utilities, debuggers, or network tools**
* Apply **just-in-time access controls** for privileged tools using a PAM solution
* Log and audit every invocation of high-risk utilities

✅ **Manage Software Licenses and Compliance**

* Track software license types, usage limits, and renewal dates
* Ensure full compliance with **commercial, open-source, and subscription-based software** licensing models
* Decommission software when no longer in use or when licenses expire

✅ **Educate Users and Monitor Enforcement**

* Provide regular awareness training about risks associated with unauthorized software
* Encourage reporting of any suspicious or unauthorized tools encountered
* Include violations in performance metrics and disciplinary procedures

**H.06 – Software Installation and Change Control Policy (System-Based Perspective)**

**Control Description**  
Establish a system-enforced policy that governs all software installations and changes within the organization’s IT infrastructure to ensure security, stability, and operational consistency. This includes formalizing **who can install software**, how changes are **requested, evaluated, approved**, and how installation is **executed, tested, and rolled back** if needed.

This control operates in conjunction with **Change Management**, **Configuration Management (CMDB)**, **Endpoint Protection**, and **Deployment Automation tools** (e.g., SCCM, Intune, Puppet, JAMF) to prevent unauthorized software installations, ensure proper documentation, and reduce the risk of introducing vulnerabilities, malware, or incompatible updates. The policy ensures a **repeatable, auditable process** for managing both standard and emergency changes across operational systems.

**Risk Statement**  
Uncontrolled software installation or change processes can introduce vulnerabilities, break existing configurations, or allow unauthorized or malicious applications into the environment—undermining security, service availability, and compliance.

**Business Impact**

* Malware infections or configuration drift due to unauthorized installations
* Downtime or instability caused by poorly tested patches or updates
* Legal and regulatory issues due to lack of audit trails or use of unlicensed software
* Reduced ability to respond to incidents due to undocumented or untraceable software changes

**ISO/IEC 27001:2022 Alignment**

**Primary ISO Controls:**

* **A.8.30 – Installation of Software on Operational Systems**  
  Mandates that software is only installed via controlled, approved processes.
* **A.8.27 – Secure System Engineering Principles**  
  Supports structured, secure software changes aligned with system design practices.
* **A.8.26 – Application Security Requirements**  
  Ensures that deployed software meets predefined security standards.
* **A.8.9 – Configuration Management**  
  Requires all system changes—including software updates—be tracked and consistent with known, approved baselines.

**Implementation Recommendations (System Integration View)**

✅ **Establish Role-Based Installation Privileges**

* Define clear roles for who can initiate, approve, and execute software installations
* Remove local admin rights for users by default
* Restrict use of privileged installation tools to IT, DevOps, or Infrastructure teams

✅ **Automate Software Deployment and Control**

* Use **centralized deployment platforms** (e.g., SCCM, Intune, JAMF, Ansible) to distribute software securely
* Integrate with **change ticketing systems** (e.g., ServiceNow, Jira) for approval workflows
* Maintain a **record of all installations**, including version, install date, requester, and approver

✅ **Integrate Testing and Rollback Procedures**

* Enforce testing in **staging or QA environments** before pushing updates to production
* Maintain **rollback scripts**, restore points, or container snapshots to recover from failed deployments
* Track success/failure metrics of each deployment for future improvement

✅ **Define Secure Software Sourcing Requirements**

* Only install software from **authorized vendors, repositories, or internal registries**
* Verify **digital signatures, hashes, or certificates** before execution
* Maintain a list of **blacklisted or restricted software**

✅ **Link Software Changes to Configuration and Asset Records**

* Update the **CMDB** and **asset inventory** automatically when new software is installed or modified
* Use **configuration management tools** (e.g., Chef, Puppet, Terraform) to enforce baseline compliance

✅ **Log and Audit All Software Change Activity**

* Record who initiated, approved, and executed each change
* Retain logs in a tamper-proof system (e.g., SIEM or audit vault) for compliance and forensic readiness
* Include software change metrics in **management review reports** (Clause 9.3)

**M.14 – Network Border Information Flow Control Policy (System-Based Perspective)**

**Control Description**  
Establish and enforce a policy to govern and secure the flow of information across network boundary points through the use of **perimeter defense systems** such as firewalls, web proxies, secure gateways, data loss prevention (DLP) tools, and intrusion detection/prevention systems (IDS/IPS). This policy ensures that **only validated, encrypted, and authorized traffic** enters or leaves the organization’s network, minimizing exposure to cyber threats and data leakage.

As part of a **defense-in-depth architecture**, this control requires the integration of **network flow enforcement tools** with centralized monitoring and threat detection systems. Border controls must enforce traffic restrictions based on **source/destination**, **protocols**, **data type**, **application behavior**, and **content sensitivity**, while supporting real-time analysis and **anomaly detection**. Configuration and rule changes must be governed by formal **change control procedures**, and all flows must be aligned with **business justification** and **regulatory constraints** (e.g., data sovereignty, export controls).

**Risk Statement**  
Uncontrolled or poorly managed information flows at the network perimeter can lead to unauthorized data exfiltration, malware infiltration, and non-compliance with data protection obligations. Failure to inspect, monitor, and control border traffic weakens the organization’s overall cybersecurity posture and impedes incident response.

**Business Impact**

* Loss or exposure of sensitive information via unauthorized outbound data flows
* Entry of malware, remote access trojans, or command-and-control traffic into the internal network
* Violation of data protection laws (e.g., GDPR, HIPAA, ITAR) due to unfiltered cross-border transfers
* Undetected communications with malicious infrastructure
* Reputational and financial consequences from avoidable security incidents

**ISO/IEC 27001:2022 Alignment**

**Primary ISO Controls:**

* **A.8.20 – Use of Network Services**  
  Requires organizations to assess and secure all network services used, particularly those enabling inbound/outbound traffic.
* **A.8.21 – Security of Network Services**  
  Mandates encryption, access controls, and security protocols for communications over external or public networks.
* **A.8.22 – Monitoring Activities**  
  Supports continuous inspection and analysis of data flows at the network perimeter for anomalies or unauthorized activity.
* **A.8.9 – Configuration Management**  
  Ensures perimeter security devices (e.g., firewalls, DLPs, proxies) are correctly configured, monitored, and maintained.

**Implementation Recommendations (System Integration View)**

✅ **Deploy Layered Border Protection Tools**

* Use **firewalls**, **next-gen firewalls (NGFW)**, **web/email security gateways**, **DLP solutions**, and **proxy servers** at ingress and egress points
* Enforce **stateful inspection, application-layer filtering**, and **SSL/TLS decryption** for deep packet inspection
* Isolate and secure **public-facing services** within **DMZs** or segmented zones

✅ **Control Outbound Data Flows**

* Define allow-lists for approved outbound destinations and protocols (e.g., HTTP/S, SFTP)
* Use **data classification tagging** and **DLP policies** to restrict sensitive data from leaving the network
* Prevent tunneling or unsanctioned services (e.g., Tor, VPN over port 443)

✅ **Secure and Monitor Inbound Traffic**

* Apply **geo-IP filtering**, **IP reputation filtering**, and **zero-trust controls** for external connections
* Require **TLS encryption**, **multi-factor authentication**, and **reverse proxies** for remote access services
* Monitor IDS/IPS alerts for common attacks (e.g., scans, brute-force, C2 callbacks)

✅ **Log and Analyze All Perimeter Events**

* Send logs from border devices to a **SIEM** for centralized correlation and threat hunting
* Use **network behavior analytics (NBA)** or **NDR tools** to detect unusual data movement
* Track bandwidth usage and inspect traffic anomalies linked to exfiltration or lateral movement

✅ **Control Changes to Perimeter Configurations**

* Route firewall and proxy rule changes through **change management workflows**
* Use **configuration baselining** and **drift detection tools** to detect unauthorized changes
* Conduct periodic **rule audits** and **recertification of business justification**

✅ **Regularly Test Border Security Effectiveness**

* Perform **penetration testing**, **red teaming**, and **data exfiltration simulations**
* Validate that DLP and filtering rules block sensitive exports and unauthorized traffic paths
* Test alerting and detection capabilities under various threat scenarios

**H.07 – Network Boundary Traffic and Content Inspection (System-Based Perspective)**

**Control Description**  
Establish a comprehensive, system-integrated policy for inspecting and controlling traffic at all **network boundaries**, using a combination of **next-generation firewalls (NGFWs)**, **deep packet inspection (DPI)**, **intrusion prevention systems (IPS)**, **behavioral detection**, and **content filtering technologies**.

This control is critical for maintaining perimeter defense and detecting threats such as **malware infiltration**, **data exfiltration**, **command-and-control (C2) communication**, or **policy violations**. Network boundary inspection should include **real-time traffic analysis**, **application-aware filtering**, and **automated rule enforcement** to block known attack vectors and suspicious patterns. Integration with **SIEM**, **network detection and response (NDR)**, and **data loss prevention (DLP)** tools ensures actionable visibility and threat correlation across the network perimeter.

**Risk Statement**  
Without comprehensive inspection of traffic and content crossing network boundaries, malicious activity may go undetected, leading to prolonged attacker presence, data leaks, and regulatory violations. Weak perimeter controls can be exploited for lateral movement, privilege escalation, and long-term compromise.

**Business Impact**

* Increased risk of advanced persistent threats (APTs) entering or maintaining presence undetected
* Unmonitored data exfiltration resulting in regulatory violations or loss of intellectual property
* Financial loss due to breaches, ransomware, or business interruption
* Reputational harm and erosion of stakeholder trust
* Operational inefficiencies in incident detection and response

**ISO/IEC 27001:2022 Alignment**

**Primary ISO Controls:**

* **A.8.21 – Security of Network Services**  
  Ensures controls are in place to protect data in transit across network services and boundaries.
* **A.8.22 – Monitoring Activities**  
  Requires proactive monitoring of system and network activity to identify abnormal behavior.
* **A.8.20 – Use of Network Services**  
  Mandates that network services are used securely and in accordance with policy.
* **A.8.29 – Logging**  
  Requires logging of system and network activity, including inspection tools, to support investigations and accountability.

**Implementation Recommendations (System Integration View)**

✅ **Deploy Advanced Network Security Tools at All Egress/Ingress Points**

* Utilize **NGFWs** with integrated **IPS**, **SSL/TLS decryption**, and **application control**
* Use **behavior-based anomaly detection** (e.g., NDR, UEBA) to identify suspicious or rare traffic patterns
* Enforce **geo-IP filtering**, **protocol restrictions**, and **rate limiting** at edge devices

✅ **Perform Deep Packet and Content Inspection**

* Inspect traffic at both **packet and payload level** to identify hidden threats or tunneling techniques
* Deploy **DLP** for outbound data monitoring, including **file types**, **keywords**, and **sensitive data patterns** (e.g., PII, financials)
* Block access to **known malicious domains, IPs, and URLs** via threat intelligence integration

✅ **Integrate with Security Analytics and Incident Response**

* Feed alerts from IPS/DPI tools into your **SIEM** or **XDR** for real-time correlation
* Automatically trigger response actions (e.g., isolate endpoint, block IP, notify SOC) for high-severity events
* Maintain forensic logs of all traffic and inspection events with appropriate **retention policies**

✅ **Apply Granular Content and Application Controls**

* Block risky content types (e.g., executable downloads, suspicious archives)
* Control access to SaaS, collaboration, and file-sharing platforms based on **business justification**
* Restrict protocols such as **Telnet, FTP, SMB** from traversing network boundaries

✅ **Continuously Update and Test Perimeter Detection Rules**

* Subscribe to **threat intelligence feeds** and regularly **update signatures, heuristics, and anomaly baselines**
* Conduct **red team exercises** and **breach simulation testing** to validate detection effectiveness
* Tune policies to reduce false positives and improve signal-to-noise ratio

✅ **Audit and Report on Inspection Effectiveness**

* Include inspection coverage metrics, alert resolution rates, and rule effectiveness in **Clause 9.1 evaluations**
* Present summary findings during **management reviews (Clause 9.3)** and support **continual improvement (Clause 10)**

**H.08 – Network Segmentation and Zoning (System-Based Perspective)**

**Control Description**  
Implement a policy and supporting technical architecture to segment the organizational network into **logical security zones** based on risk level, sensitivity, trust, and function. Network segmentation reduces the attack surface and limits lateral movement by separating systems such as user workstations, critical infrastructure, development environments, and externally exposed services.

This control requires the use of **virtual LANs (VLANs)**, **firewalls**, **network access control (NAC)**, **software-defined networking (SDN)**, and **zero-trust enforcement** to ensure that only explicitly authorized traffic can flow between zones. Boundaries between segments must be monitored with **traffic inspection tools** (e.g., IDS/IPS, NDR) and changes to segmentation rules must be governed through **configuration and change control** processes.

**Risk Statement**  
Without segmentation or zoning, attackers who gain access to any part of the internal network may move laterally to compromise critical systems or sensitive data. Lack of logical separation undermines incident containment, weakens compliance posture, and exposes the organization to widespread damage during security events.

**Business Impact**

* Rapid attacker propagation across systems due to flat or poorly segmented networks
* Greater difficulty in isolating compromised assets during incident response
* Violations of regulatory requirements mandating separation of duties and access control boundaries
* Prolonged operational outages during ransomware or malware outbreaks
* Increased forensic and recovery complexity after breaches

**ISO/IEC 27001:2022 Alignment**

**Primary ISO Controls:**

* **A.8.21 – Security of Network Services**  
  Requires controls to ensure secure operation of network services, including network architecture segmentation.
* **A.8.22 – Monitoring Activities**  
  Supports boundary inspection and anomaly detection at segmentation points.
* **A.8.29 – Logging**  
  Ensures logs from segmented network boundaries are captured for audit, detection, and investigation.
* **A.5.25 – Response to Information Security Incidents**  
  Depends on effective segmentation to support threat isolation and containment during incident response.

**Implementation Recommendations (System Integration View)**

✅ **Define Segmentation Strategy Based on Risk and Function**

* Separate environments such as:  
  • Workstations / user endpoints  
  • Servers and data centers  
  • Development / test / production  
  • IoT / OT / building management systems  
  • Guest or third-party access zones
* Align segmentation with **data sensitivity**, **asset criticality**, and **business impact analysis**

✅ **Use Technical Controls to Enforce Segmentation**

* Implement **firewalls, ACLs, VLAN tagging, or SDN policies** to restrict inter-zone traffic
* Apply **default deny policies** at all boundaries; allow only required traffic based on least privilege
* Leverage **microsegmentation** for fine-grained access control in virtualized and cloud environments

✅ **Integrate Network Segmentation with Identity and Access Management (IAM)**

* Apply **user-based or device-based policies** (e.g., via NAC or identity-aware firewalls)
* Use **role-based access control (RBAC)** to govern who can traverse zones
* Require **MFA and logging** for privileged access between security zones

✅ **Log, Monitor, and Alert on Inter-Zone Traffic**

* Inspect all traffic crossing segmentation boundaries using **IDS/IPS**, **NGFW**, or **NDR tools**
* Correlate suspicious patterns with endpoint, identity, and behavioral logs in **SIEM/XDR platforms**
* Generate alerts for:  
  • Lateral movement attempts  
  • Unexpected traffic between sensitive zones  
  • Data exfiltration behavior

✅ **Test and Validate Segmentation Effectiveness**

* Conduct **regular segmentation audits**, **firewall rule reviews**, and **traffic simulations**
* Use **red teaming or adversary emulation** to assess lateral movement resistance
* Maintain documentation of segmentation architecture and update with each infrastructure change

✅ **Support Incident Response and Containment**

* Design zones to enable rapid **isolation of compromised segments**
* Create **incident playbooks** that leverage segmentation for threat suppression
* Log all traffic for post-incident **forensic analysis**

**H.09 – Data Loss Prevention (DLP) at Egress Points (System-Based Perspective)**

**Control Description**  
Establish and enforce a system-level policy to deploy **Data Loss Prevention (DLP) controls at egress points**, where information exits the organizational network. DLP technologies must be integrated with **email gateways**, **web proxies**, **cloud access security brokers (CASBs)**, and **file transfer systems** to analyze outbound data flows for indicators of sensitive or regulated content.

These systems use **pattern recognition, data classification tags, fingerprinting, and contextual analysis** to detect unauthorized attempts to transmit confidential, proprietary, or personal data. Upon detection, the system can take automated actions such as **alerting**, **blocking**, **quarantining**, or **encrypting** the transmission. DLP controls must align with internal data handling policies and external regulatory requirements such as **GDPR**, **HIPAA**, or **PCI-DSS**.

**Risk Statement**  
Without DLP enforcement at data egress points, the organization risks unauthorized disclosure of sensitive data through email, web uploads, cloud storage, or file transfers. Whether accidental or malicious, such leaks can result in severe regulatory, operational, and reputational consequences.

**Business Impact**

* Breach of confidential information, intellectual property, or customer data
* Regulatory penalties for non-compliance with data protection laws
* Loss of competitive advantage or customer trust
* Legal action stemming from contractual or privacy violations
* Increased forensic and remediation costs following a data leak

**ISO/IEC 27001:2022 Alignment**

**Primary Controls:**

* **A.8.20 – Use of Network Services**  
  Requires outbound traffic via network services to be protected and filtered appropriately.
* **A.8.21 – Security of Network Services**  
  Ensures information is secured during transmission—supporting DLP at the transport layer.
* **A.8.22 – Monitoring Activities**  
  Enables real-time inspection and logging of outbound data for DLP analysis.
* **A.5.14 – Information Transfer**  
  Requires protective measures for the secure exchange of data, including transfers outside the organization.

**Supporting Control:**

* **A.8.11 – Use of Removable Media**  
  DLP policies should also apply to physical transfers such as USB drives or external disks.

**Implementation Recommendations (System Integration View)**

✅ **Deploy DLP Solutions at Critical Egress Points**

* Email: Integrate with **Secure Email Gateways** (e.g., Microsoft Defender, Proofpoint, Mimecast)
* Web: Use **Web Proxy/Cloud Gateways** (e.g., Zscaler, Forcepoint) to scan uploads and form submissions
* Cloud: Apply **CASBs** (e.g., Netskope, Microsoft Purview, McAfee MVISION) to monitor SaaS usage
* Network: Configure **NGFWs** with DLP inspection policies for outbound traffic

✅ **Define and Classify Sensitive Data Types**

* Use **data classification labels** (e.g., Confidential, Internal, Public) as DLP detection triggers
* Create fingerprinting or regex rules for:  
  • Personal Identifiable Information (PII)  
  • Financial data (e.g., credit card numbers, account info)  
  • Intellectual property or internal schematics  
  • Contractual data covered under NDAs

✅ **Set DLP Policies and Automated Enforcement Actions**

* Configure DLP systems to:  
  • Alert on policy violations  
  • Quarantine messages for review  
  • Block or encrypt high-risk transmissions  
  • Notify compliance teams or line managers for violations
* Apply **granular rules per business unit, user role, and risk profile**

✅ **Monitor, Log, and Investigate DLP Events**

* Forward DLP alerts to **SIEM/XDR platforms** for correlation and analysis
* Track trends in data movement, false positives, and user behavior
* Investigate suspicious transfers as potential insider threats or policy violations

✅ **Train Staff on Secure Data Handling and DLP Triggers**

* Educate employees on data classification, acceptable transfer methods, and DLP expectations
* Use real-time **DLP pop-ups** or **just-in-time training** to inform users when violations are blocked

✅ **Continuously Test and Tune DLP Effectiveness**

* Simulate data leak attempts to validate detection thresholds and policy enforcement
* Conduct **monthly policy reviews** and adjust for business changes or emerging threats
* Integrate DLP with **incident response plans** for rapid containment of data exfiltration attempts

**L.14 – Pre-Employment Credential Verification Policy (System-Based Perspective)**

**Control Description**  
Implement a formal, risk-aligned policy requiring **credential and background verification of all individuals** prior to employment or contract engagement. This policy ensures that all personnel granted access to systems, facilities, or sensitive information have been vetted for **identity authenticity**, **qualifications**, **experience**, and **trustworthiness**, in accordance with the role’s sensitivity and applicable legal or regulatory requirements.

Verification activities may include, but are not limited to:

* Identity and legal right to work validation
* Education and certification checks
* Employment history and reference validation
* Criminal record checks (as allowed by law)
* Professional licensing or regulatory clearance (where relevant)

The policy must integrate with **HR onboarding systems**, **access management workflows**, and **information security governance** to ensure no system access or privileged roles are assigned until required checks are satisfactorily completed and documented.

**Risk Statement**  
Failure to perform credential verification prior to employment may result in individuals with falsified records or hidden risk factors being granted access to sensitive systems or data. This increases the likelihood of insider threats, non-compliance with legal obligations, and reputational damage from negligent hiring practices.

**Business Impact**

* Unauthorized access to sensitive systems by unvetted individuals
* Reputational harm following incidents involving employees with questionable backgrounds
* Legal penalties or liability due to non-compliance with labor, security, or privacy regulations
* Increased risk of fraud, misconduct, or internal data breaches
* Loss of stakeholder confidence due to weak personnel controls

**ISO/IEC 27001:2022 Alignment**

**Primary Control:**

* **A.6.1 – Screening**  
  Requires background checks and credential verification for all candidates, proportionate to the information access level and sensitivity of the position.

**Supporting Controls and Clauses:**

* **A.5.2 – Information Security Roles and Responsibilities**  
  Ensures that individuals assigned to sensitive security roles are competent and trustworthy.
* **Clause 7.2 – Competence**  
  Requires verification of qualifications, certifications, and experience relevant to assigned job functions.

**Implementation Recommendations (System Integration View)**

✅ **Define Risk-Based Screening Levels**

* Differentiate screening depth based on job role criticality (e.g., general staff vs. privileged access holders)
* Map roles to background check requirements in a **risk matrix**
* Define trigger events for re-screening (e.g., internal transfers, clearance expiration)

✅ **Standardize and Automate the Verification Process**

* Integrate credential verification with **HR onboarding systems** and **identity governance platforms**
* Use third-party screening providers with secure data handling practices
* Ensure that no **logical access** is provisioned via IAM systems until background verification is complete

✅ **Ensure Legal and Regional Compliance**

* Tailor screening scope to regional labor laws and privacy regulations (e.g., GDPR, FCRA, local labor laws)
* Obtain documented **candidate consent** prior to background checks
* Maintain audit records of screening completion, exceptions, and approvals

✅ **Link Verification to Access and Role Assignment**

* Ensure background verification is a **prerequisite for system access** or elevated privileges
* Use **conditional access policies** to block user onboarding in IAM or Active Directory until HR clearance is met
* Assign temporary or restricted roles if onboarding must begin before full screening is completed

✅ **Document and Communicate the Policy Clearly**

* Include screening policy and expectations in job descriptions and recruitment materials
* Inform hiring managers and HR staff of their responsibilities under the policy
* Require formal acknowledgment of the policy from new hires

**M.15 – Security Vetting Checks for Employees (System-Based Perspective)**

**Control Description**  
Implement a formal, risk-based policy to conduct **security vetting checks for employees** who are granted access to sensitive systems, privileged roles, or classified information. Vetting ensures the **trustworthiness, integrity, and suitability** of individuals in high-risk or high-privilege positions. Checks may include:

* Identity verification
* Criminal record background checks
* Credit checks (where appropriate by law and role)
* Verification of professional qualifications, certifications, or affiliations
* Review of previous employment and references

Vetting must be proportionate to the sensitivity of the role, aligned with regulatory and contractual obligations, and documented consistently across the organization. The process should be integrated with **human resources**, **identity governance**, and **access provisioning systems** to ensure that no elevated access is granted until clearance is complete.

**Risk Statement**  
Failure to perform adequate vetting for employees in sensitive roles increases the likelihood of **malicious insider activity**, **negligent access misuse**, or **privileged account abuse**, potentially leading to regulatory breaches, operational disruption, or reputational harm.

**Business Impact**

* Insider threats leading to data breaches or sabotage
* Access to classified or regulated information by unqualified personnel
* Contractual or legal non-compliance in regulated industries (e.g., defense, finance)
* Loss of client confidence and reputational damage
* Fines, audits, or loss of security accreditations due to inadequate screening

**ISO/IEC 27001:2022 Alignment**

**Primary Control:**

* **A.6.1 – Screening**  
  Requires security background checks proportional to the risk level of the role and aligned with local laws.

**Supporting Clauses and Controls:**

* **Clause 7.2 – Competence**  
  Ensures qualifications and suitability for job roles, particularly security-relevant ones.
* **A.5.2 – Information Security Roles and Responsibilities**  
  Links security responsibilities to appropriate personnel with verified integrity and qualifications.
* **A.8.15 – Privileged Access Rights**  
  Requires special control over users with elevated system privileges—including additional vetting.

**Implementation Recommendations (System Integration View)**

✅ **Establish Role-Based Vetting Tiers**

* Define vetting levels (e.g., Standard, Elevated, High-Security) based on:  
  • Access to classified or regulated data  
  • Use of administrative or privileged accounts  
  • Control over critical systems or infrastructure
* Create a **vetting requirements matrix** that maps roles to required screening levels

✅ **Integrate Vetting into Access Provisioning Workflow**

* Use **IAM/HRIS integration** to block system or privileged access until vetting is confirmed
* Trigger vetting checks automatically for sensitive roles during onboarding or internal transfers
* Require **re-vetting** at defined intervals or after role changes

✅ **Apply Legal and Ethical Screening Practices**

* Conduct checks in compliance with local laws (e.g., GDPR, FCRA, anti-discrimination laws)
* Obtain documented **informed consent** from employees prior to screening
* Limit the use of screening results to legitimate security and HR purposes

✅ **Document, Track, and Retain Vetting Results Securely**

* Maintain a secure repository of vetting reports, decisions, and justifications
* Ensure **audit trails** exist for access decisions based on vetting results
* Use encryption and access controls to protect sensitive HR and background data

✅ **Define Escalation and Exception Processes**

* Establish protocols for handling adverse findings or incomplete checks
* Create a governance body (e.g., Security & HR Committee) to review complex cases
* Log all exceptions and link them to compensating controls (e.g., access limitations, increased monitoring)

✅ **Continuously Review Vetting Effectiveness**

* Include vetting metrics (e.g., time to clearance, exception rates) in ISMS reviews (Clause 9.3)
* Update vetting policies based on lessons learned from incidents, audits, or threat changes
* Reassess employees during contract renewal or when elevated responsibilities are assigned

**L.15 – Non-Recriminatory Security Violation Reporting (System-Based Perspective)**

**Control Description**  
Establish a formal, accessible, and confidential process that enables all employees, contractors, and affiliated personnel to report actual or suspected **information security violations** or policy breaches **without fear of retaliation or disciplinary consequence**, provided the report is made in good faith.

The reporting process must include **secure, anonymous, and named reporting mechanisms**, such as internal reporting portals, anonymous hotlines, or secure email channels. All reports should be handled under strict confidentiality, reviewed by authorized personnel only, and processed through a **structured triage, investigation, and remediation workflow**. The policy must clearly communicate the **organization’s zero-tolerance stance on reprisal**, and promote a **speak-up culture** that empowers individuals to proactively contribute to threat detection and organizational resilience.

**Risk Statement**  
Failure to provide a safe, retaliation-free channel for reporting security violations may discourage early disclosure of risks or breaches. This can lead to unaddressed vulnerabilities, escalation of incidents, and erosion of employee trust in the organization’s governance and values.

**Business Impact**

* Delayed detection and containment of insider threats or recurring security issues
* Compromise of systems or data due to unreported policy violations
* Reputational harm and decreased employee morale
* Legal liability for failing to provide whistleblower protection as mandated by regulatory frameworks
* Missed opportunities for improvement through open feedback

**ISO/IEC 27001:2022 Alignment**

**Primary ISO Control:**

* **A.5.24 – Reporting Information Security Weaknesses**  
  Encourages users to report security concerns promptly and supports a culture of openness and accountability.

**Supporting ISO Controls and Clauses:**

* **A.5.25 – Response to Information Security Incidents**  
  Ensures that all reports are investigated through structured incident response procedures.
* **Clause 7.4 – Communication**  
  Mandates effective and transparent communication channels, including those for secure internal reporting.
* **Clause 10.1 – Nonconformity and Corrective Action**  
  Supports proactive reporting and continual improvement through non-punitive identification of issues.

**Implementation Recommendations (System and Process Integration View)**

✅ **Establish Clear, Accessible Reporting Channels**

* Provide multiple reporting options (e.g., anonymous hotline, secure online form, designated email)
* Ensure availability across global regions, devices, and working arrangements (e.g., remote staff)
* Integrate reporting access into **employee portals**, **intranet**, or **mobile HR apps**

✅ **Define a Safe Disclosure and Non-Retaliation Policy**

* Publish a clearly worded **non-recrimination statement** that applies to all personnel
* Explicitly state that **no adverse action will be taken** against good faith reporters—even if the report is mistaken
* Train managers and security teams on how to uphold non-retaliatory practices

✅ **Link to Incident Management and Compliance Functions**

* Route reports into your **Security Incident Response Process** (aligned with A.5.25)
* Triage reports based on severity and route them to security, compliance, HR, or legal teams as appropriate
* Track investigations, corrective actions, and lessons learned in the **ISMS or GRC platform**

✅ **Maintain Anonymity and Confidentiality**

* Encrypt and restrict access to all submitted reports
* Use tools that allow anonymous submission while enabling secure follow-up (e.g., EthicsPoint, NAVEX, Whispli)
* Store all records in line with **data protection and whistleblower laws**

✅ **Promote a Culture of Reporting and Awareness**

* Incorporate training on the reporting process into **security awareness and onboarding programs**
* Regularly communicate how reports are used to strengthen organizational security
* Celebrate “security champions” and acknowledge anonymous contributions that led to positive change

✅ **Monitor, Audit, and Improve the Process**

* Track metrics: report volume, response time, resolution time, escalation rate
* Include insights in **Clause 9.3 – Management Review** and **Clause 10 – Continual Improvement**
* Periodically test the system with simulated reports and gather feedback to ensure usability and trust

**L.16 – Disciplinary Process for Security Policy Violations (System-Based Perspective)**

**Control Description**  
Establish a documented, fair, and consistently enforced **disciplinary process** for managing violations of information security policies and procedures. This process must be integrated into the organization’s **HR governance framework** and aligned with applicable **labor laws**, **contractual obligations**, and **ethical standards**.

The policy must define:

* Categories of violations (e.g., negligent, intentional, repeated)
* Investigation protocols and responsible authorities (e.g., HR, Legal, Information Security)
* A graduated scale of sanctions (e.g., verbal warning, written notice, suspension, termination)
* An appeals or grievance process to ensure due process
* Clear roles for **security, HR, legal**, and **line managers** in enforcement

This process should be **communicated during onboarding**, **reinforced through training**, and **applied consistently across all departments**, including for contractors, remote workers, and third-party personnel. Integration with security incident response workflows ensures timely and effective enforcement of consequences when breaches occur.

**Risk Statement**  
Without a clearly defined and enforced disciplinary process, violations of security policies may go unaddressed or be handled inconsistently, weakening deterrence, eroding trust in governance, and increasing the likelihood of repeat incidents or deliberate insider threats.

**Business Impact**

* Repeated noncompliance and normalization of security violations
* Ineffective deterrence of negligent or malicious behavior
* Legal exposure from inconsistent or inappropriate disciplinary action
* Diminished trust in leadership and security accountability
* Regulatory sanctions for failing to enforce internal security policies

**ISO/IEC 27001:2022 Alignment**

**Primary ISO Control:**

* **A.6.2 – Disciplinary Process**  
  Requires implementation of a process to handle personnel who breach information security policies, proportionate to the violation and applicable legal considerations.

**Supporting Controls and Clauses:**

* **A.5.2 – Information Security Roles and Responsibilities**  
  Links violations to clearly assigned accountability for security obligations.
* **Clause 7.3 – Awareness and Training**  
  Ensures employees understand policies and the consequences of noncompliance.
* **Clause 10.1 – Nonconformity and Corrective Action**  
  Reinforces policy enforcement as a corrective mechanism for breaches or deviations.

**M.16 – Personnel Risk Assessments and Qualification Verification (System-Based Perspective)**

**Control Description**  
Establish and implement a formal process to conduct **personnel risk assessments** and **qualification verification** for all employees and contractors, particularly those in roles with access to sensitive systems, data, or elevated security responsibilities. The assessment should consider factors such as:

* Verified education and certifications
* Relevant professional experience
* Security awareness and training completion
* Results from background screening (as per A.6.1)
* Behavioral indicators or risk posture (e.g., prior policy violations or disciplinary history)

This process should be **embedded into onboarding**, **role assignment**, and **access provisioning workflows**, ensuring that only individuals with appropriate competence and trustworthiness are granted access to privileged systems or information. Personnel risk assessments must be reviewed **periodically** or when individuals change roles, access levels, or show indicators of elevated insider risk.

**Risk Statement**  
Without formal personnel risk assessments and qualification verification, individuals may be assigned to security-critical functions without adequate vetting, leading to increased susceptibility to insider threats, errors, or compliance failures.

**Business Impact**

* Poorly qualified staff may mishandle critical systems or data
* Increased likelihood of breaches due to human error or negligence
* Legal and regulatory findings related to insufficient personnel due diligence
* Damage to business operations and brand due to insider-driven incidents
* Greater cost and complexity in remediation and post-incident response

**ISO/IEC 27001:2022 Alignment**

**Primary ISO Control:**

* **A.6.3 – Competence**  
  Requires that personnel are appropriately trained, experienced, and qualified for their responsibilities related to information security.

**Supporting Clauses and Controls:**

* **Clause 7.2 – Competence**  
  Mandates that the organization define, assess, and maintain the competence of individuals doing work under its control.
* **A.6.1 – Screening**  
  Supports pre-employment checks that inform risk-based suitability assessments.
* **A.8.15 – Privileged Access Rights**  
  Reinforces the need for elevated scrutiny and validation of individuals with admin or privileged access.

**Implementation Recommendations (System Integration View)**

✅ **Develop a Role-Based Risk Assessment Framework**

* Categorize roles into **risk tiers** based on access level, system criticality, and business impact
* Define **competency requirements** for each tier (e.g., minimum experience, mandatory certifications, background check level)
* Align assessments with your **job architecture** and **security roles and responsibilities matrix**

✅ **Embed Risk Checks into the HR and IAM Lifecycle**

* Integrate assessment checkpoints during:  
  • Onboarding  
  • Internal transfers or promotions  
  • Access elevation requests (e.g., admin roles)  
  • Annual access reviews
* Leverage **HRIS, GRC, or IAM tools** to automate and track verification workflows

✅ **Assess Both Competence and Behavior**

* Verify:  
  • Professional qualifications (e.g., CISSP, CISM, ITIL, Azure/AWS certs)  
  • Completed security training (e.g., phishing awareness, secure coding)  
  • Recent role-specific experience
* Monitor for indicators of insider risk (e.g., policy violations, disciplinary actions, access misuse)

✅ **Maintain Centralized Personnel Risk Profiles**

* Store risk ratings and competency status securely within the HR or GRC system
* Link personnel risk level to access privileges or monitoring intensity (e.g., enhanced logging for high-risk roles)
* Use data to support compliance reporting and internal audits

✅ **Review and Reassess Regularly**

* Schedule **annual reassessments** for sensitive roles or at major access changes
* Tie reassessments to **Clause 9.3 Management Review** and **Clause 10 – Improvement**
* Adjust requirements based on updated threat models or business changes

✅ **Train Managers and Reviewers on the Process**

* Provide guidance on how to evaluate qualifications and behavioral risk
* Create escalation paths for personnel who fail to meet vetting thresholds
* Ensure HR, security, and departmental leads collaborate on high-risk role assignments

**M.17 – Securing Organisational Assets Upon Termination (System-Based Perspective)**

**Control Description**  
Establish and enforce a formal policy and workflow to secure **all organisational assets and information access rights** when an individual’s employment or contractual engagement ends. The offboarding process must be **automated where possible** and include coordinated efforts between **HR, IT, Information Security, and line management** to ensure:

* Immediate or scheduled **revocation of logical access** (e.g., accounts, VPN, SaaS platforms)
* Collection of **physical assets** (e.g., laptops, phones, ID cards, security tokens)
* Deactivation of **building and system access credentials**
* Retrieval or secure transfer of **business-critical data** and intellectual property
* Enforced awareness of **post-employment obligations** (e.g., non-disclosure, data handling)

Processes should be supported by **role-based termination checklists**, **identity governance tools**, and **endpoint management platforms**, ensuring no residual access remains and all assets are recovered or accounted for.

**Risk Statement**  
Failure to effectively offboard departing personnel may leave critical systems and information exposed to unauthorized access or misuse, leading to potential data breaches, sabotage, or regulatory non-compliance.

**Business Impact**

* Unauthorized post-employment access to sensitive systems or data
* Loss, theft, or misuse of physical or digital corporate assets
* Compliance failures due to incomplete access revocation
* Reputational damage and legal liability from insider-driven incidents
* Increased costs from manual investigations, remediation, and legal claims

**ISO/IEC 27001:2022 Alignment**

**Primary ISO Control:**

* **A.6.4 – Termination and Change of Employment**  
  Requires timely removal of access and recovery of organizational assets when a person leaves or changes roles.

**Supporting ISO Controls and Clauses:**

* **A.8.18 – Access Rights**  
  Mandates immediate review and revocation of user privileges based on employment status changes.
* **A.5.2 – Information Security Roles and Responsibilities**  
  Assigns accountability for termination procedures across departments.
* **Clause 7.3 – Awareness and Training**  
  Ensures users understand their offboarding obligations, including data return and confidentiality.

**Implementation Recommendations (System and Workflow View)**

✅ **Automate Offboarding with IAM and HR Integration**

* Connect HRIS (e.g., Workday, BambooHR) with Identity & Access Management (IAM) systems
* Automatically trigger account deactivation and access revocation workflows upon status change
* Remove access to internal systems, cloud apps (e.g., M365, Salesforce), VPNs, and MFA tokens

✅ **Implement Role-Based Exit Checklists**

* Create customized checklists for full-time staff, contractors, and third-party vendors
* Include checkpoints for:  
  • IT and security teams (account revocation, device wipe)  
  • HR (policy acknowledgment, final pay)  
  • Line managers (handover and knowledge transfer)  
  • Facilities (badge and physical access return)

✅ **Recover and Audit Physical and Logical Assets**

* Track asset assignment and recovery through your asset management system (e.g., JAMF, Intune, ServiceNow)
* Require physical return or verification of secure destruction for all issued devices
* Conduct spot checks and reconciliation for high-value or sensitive asset categories

✅ **Secure Retention or Transfer of Critical Business Data**

* Ensure email and file access is **redirected or archived** (e.g., mailbox handover, data export from shared folders)
* Transfer ownership of key systems, workflows, or repositories before disabling accounts
* Monitor for large outbound data transfers prior to termination

✅ **Enforce Post-Employment Obligations and Acknowledgment**

* Include reminders of non-disclosure agreements (NDAs) or regulatory requirements in the exit process
* Retain signed termination acknowledgments for legal or audit readiness
* Monitor ex-employee identities for potential re-entry via third-party systems or VPN

✅ **Review and Audit Offboarding Performance**

* Maintain offboarding logs and audit trails for each user
* Periodically test for “ghost accounts” or orphaned access (e.g., via access review campaigns)
* Report metrics (e.g., average time to deprovision, asset recovery rate) as part of Clause 9.1 and 9.3 reviews

**L.17 – Incident Management Policy (Detection, Resolution, Recovery) – System-Based Perspective**

**Control Description**  
Establish and maintain a formal **Incident Management Policy** that governs the end-to-end lifecycle of information security incidents—**from detection and reporting to resolution, recovery, and post-incident review**. This policy must define:

* **Roles and responsibilities** (e.g., Security Operations, IT, Legal, Communications)
* **Detection mechanisms** such as SIEMs, EDRs, anomaly detection, IDS/IPS, and user reporting
* **Incident classification and escalation criteria**
* **Containment, eradication, and remediation procedures**
* **Recovery plans** to restore systems and data integrity
* **Communication protocols** including internal updates and external notifications (e.g., regulatory, contractual)
* **Forensic and evidence collection procedures** for legal, compliance, or disciplinary needs
* **Lessons learned analysis** to feed into risk treatment, awareness training, and control enhancement

The policy should be supported by **automated playbooks**, **ticketing systems**, and **runbooks** integrated into your **Security Incident Response Platform (SIRP)** or **SIEM**, ensuring a repeatable, audit-ready process aligned with regulatory obligations and business continuity goals.

**Risk Statement**  
If the organization does not define and implement an incident management policy covering detection, resolution, and recovery, it risks delayed or ineffective response, non-compliance with reporting requirements, increased damage from incidents, and missed opportunities to improve resilience.

**Business Impact**

* Slower containment and eradication of cyber threats
* Missed breach reporting deadlines under laws like GDPR, HIPAA, or NIS2
* Increased system downtime and lost productivity
* Customer and partner dissatisfaction due to unclear communication or prolonged outages
* Legal liability and reputational damage following poorly managed incidents

**ISO/IEC 27001:2022 Alignment**

**Primary ISO Controls:**

* **A.5.25 – Response to Information Security Incidents**  
  Requires documented, communicated, and tested incident response procedures.
* **A.5.26 – Learning from Information Security Incidents**  
  Mandates structured post-incident analysis and continuous improvement.
* **A.5.27 – Collection of Evidence**  
  Ensures digital forensics is handled lawfully and appropriately.
* **Clause 6.1.2 – Risk Assessment (supporting)**  
  Informs planning and prioritization of incident response based on risk scenarios.

**Implementation Recommendations (System and Operational View)**

✅ **Establish an Incident Response Framework**

* Define severity levels, categories (e.g., data breach, malware, phishing), and escalation paths
* Use **NIST 800-61**, **SANS**, or **ISO/IEC 27035** frameworks as structure
* Develop **incident response plans** for high-risk scenarios (e.g., ransomware, insider attack, cloud misconfiguration)

✅ **Integrate Detection and Alerting Systems**

* Implement and tune **SIEM**, **EDR/XDR**, **IDS/IPS**, and **UEBA** tools
* Define correlation rules and alert thresholds that align with your risk appetite
* Ensure alert triage integrates into **ticketing systems** (e.g., ServiceNow, Jira) or **SOCs**

✅ **Coordinate Response and Communication**

* Define roles for Incident Manager, Technical Lead, Legal, HR, PR, and Executive Sponsors
* Maintain **contact rosters**, **call trees**, and **communications templates**
* Create predefined **external notification plans** (e.g., regulators, DPOs, partners, affected users)

✅ **Document and Practice Recovery Procedures**

* Link incident response to **Business Continuity (BCP)** and **Disaster Recovery (DR)** plans
* Ensure critical assets and systems have defined **Recovery Time Objectives (RTOs)** and **Recovery Point Objectives (RPOs)**
* Test technical recovery processes regularly via **tabletop exercises** and **red/blue team simulations**

✅ **Capture Evidence and Support Investigations**

* Follow chain-of-custody procedures and log access controls when collecting forensic data
* Secure logs and artifacts to support root cause analysis and legal action, if needed
* Engage third-party forensic specialists when necessary

✅ **Conduct Post-Incident Reviews and Improve Continuously**

* Use structured **lessons learned sessions** after major or repeat incidents
* Feed findings into:  
  • Awareness programs  
  • Control enhancements  
  • Risk register updates  
  • Policy revisions
* Track metrics: MTTR (mean time to respond), incident volume by type, root causes, response SLAs

**H.10 – Proactive Verification of Security Controls (System-Based Perspective)**

**Control Description**  
Establish and maintain a formal process to **proactively verify the effectiveness of security controls** through continuous testing, monitoring, and assurance activities. This verification ensures that **technical, physical, and procedural controls** operate as intended and continue to align with the organization’s **risk appetite, regulatory obligations, and business needs**.

Control validation may include:

* **Automated security control assessments** (e.g., CSPM, GRC toolsets, SCAP-based scans)
* **Vulnerability scanning and remediation tracking**
* **Internal audits and technical configuration reviews**
* **Penetration testing and red/purple team simulations**
* **Tabletop exercises** and **incident response walk-throughs**

This control should be supported by **control owners**, **audit/compliance teams**, and **automated assurance platforms** to ensure validation activities are **timely, traceable, and risk-prioritized**.

**Risk Statement**  
If security controls are not proactively verified, the organization may unknowingly operate with ineffective, misconfigured, or outdated controls—exposing critical systems and data to unmitigated risk.

**Business Impact**

* Unseen control weaknesses leave critical assets vulnerable
* Failure to detect control degradation following system changes or updates
* Inability to prove control effectiveness during audits or due diligence
* Greater likelihood of compliance violations or fines
* Reputational damage following a preventable breach or misconfiguration

**ISO/IEC 27001:2022 Alignment**

**Primary Control:**

* **A.10 – Validation of Controls**  
  Requires organizations to validate security controls at planned intervals or upon significant changes to ensure they remain effective.

**Supporting Clauses and Controls:**

* **Clause 9.1 – Monitoring, Measurement, Analysis and Evaluation**  
  Ensures control performance is regularly evaluated and supported by metrics.
* **Clause 10.1 – Nonconformity and Corrective Action**  
  Facilitates formal corrective action when controls fail to perform as intended.
* **A.5.16 – Monitoring Activities**  
  Supports ongoing oversight of control operations across technical and organizational layers.
* **A.5.26 – Learning from Information Security Incidents**  
  Drives validation updates following incident findings.

**H.11 – Ensuring Availability of Critical Assets During a Crisis (System-Based Perspective)**

**Control Description**  
Develop and enforce a **Business Continuity and Crisis Resilience Policy** that ensures the **availability of critical systems, data, and services** during disruptive events such as cyberattacks, infrastructure failures, pandemics, or natural disasters.

The policy must establish a **continuity assurance framework** that includes:

* **Identification of critical assets** and business processes (via BIA – Business Impact Analysis)
* **Redundancy, high availability (HA), and failover mechanisms** (e.g., clustering, geo-redundant cloud)
* **Data backup and recovery strategies**, including Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)
* Clearly defined **roles and responsibilities** for crisis response
* **Crisis communication protocols** for internal and external stakeholders
* **Periodic testing**, simulation, and refinement of business continuity and disaster recovery (BC/DR) plans
* Alignment with **incident response**, **risk treatment**, and **change management** procedures

This ensures minimal disruption to essential operations and sustains trust with stakeholders during adverse conditions.

**Risk Statement**  
If the organization does not implement a structured policy to ensure critical asset availability during crises, it may suffer prolonged outages, data loss, reputational damage, and non-compliance with business or regulatory requirements.

**Business Impact**

* Inability to operate mission-critical services or meet SLAs
* Reputational damage from perceived unpreparedness or failure to respond
* Financial losses due to prolonged downtime or contract breaches
* Fines or enforcement actions for non-compliance with availability requirements (e.g., under DORA, NIS2, GDPR, etc.)

**ISO/IEC 27001:2022 Alignment**

**Primary Control:**

* **A.5.31 – Validation of Information Security Controls**  
  Requires that controls (e.g., continuity safeguards) are regularly reviewed to ensure they remain effective and aligned with risk and availability requirements.

**Supporting Clauses and Controls:**

* **Clause 9.1 – Monitoring, Measurement, Analysis, and Evaluation**  
  Ensures continuity controls are monitored for effectiveness and reported on.
* **A.8.9 – Configuration Management**  
  Supports validation of HA and DR settings following infrastructure or software changes.
* **A.8.28 – Protection of Log Information**  
  Reinforces monitoring of critical system events and availability-related anomalies.
* **A.6.3 – Information Security in Business Continuity Management** (Directly relevant to continuity planning)

**Implementation Recommendations (Operational Resilience View)**

✅ **Identify and Classify Critical Assets**

* Conduct a **Business Impact Analysis (BIA)** to determine asset criticality
* Map systems to business functions, RTOs/RPOs, and dependency trees
* Label Tier 1 assets for priority protection and recovery

✅ **Deploy Resilience Architecture**

* Use solutions like:  
  • Active-passive or active-active failover  
  • Multi-cloud or hybrid backup strategies  
  • Offline/offsite storage for ransomware resilience
* Test resilience of: DNS, VPN, identity platforms (e.g., SSO), communication tools, backup infrastructure

✅ **Integrate DR with Incident and Change Management**

* Include disaster recovery (DR) steps in incident response plans
* Link availability risks to change approvals (via CAB) and test rollback/failover post-deployment
* Conduct **tabletop exercises** and **live DR tests** at least annually

✅ **Define and Test Crisis Communication Plans**

* Pre-approve messaging templates for internal teams, regulators, and the public
* Establish communication escalation paths and fallback methods (e.g., SMS alerts, satellite phones)
* Simulate communication breakdowns in crisis exercises

✅ **Monitor Continuity Metrics and Automate Reporting**

* Track:  
  • % of critical assets covered by DR/BCP  
  • Time to recovery (actual vs. RTO targets)  
  • Success rate of DR tests  
  • Control uptime and failure rates
* Feed results into **Clause 9.3 – Management Review** and **Clause 10.1 – Continual Improvement**