ISO 27001 - NIST CSF Mapping and Policy Development

This document serves as a comprehensive analysis demonstrating the practical application of cybersecurity frameworks. It interprets key controls from ISO 27001:2022, maps them directly to the NIST Cybersecurity Framework (CSF), and operationalizes these requirements into three robust, SANS-inspired enterprise security policies.

ISO Control Interpretation: The Building Blocks

To build a strong Information Security Management System (ISMS), we need solid foundational controls. I have selected three critical areas from ISO/IEC 27001:2022 Annex A that are non-negotiable for any organization serious about security.

ISO 27001 Control 5.17: Authentication Information (Identity Management)

This control, titled **Authentication Information**, is all about proving who you are. It is the gatekeeper for our systems. The core idea is to manage and protect every piece of data used to verify an identity, passwords, tokens, biometrics etc.This is not just about having a password; it is about the entire **Identity Management** process: making sure the credentials are secure when stored (think hashing and salting), requiring strong methods like Multi-Factor Authentication (MFA), and having a clear process for issuing and, crucially, revoking them. If the authentication information is compromised, the entire security perimeter fails.

ISO 27001 Control 5.18: Access Rights (Access Control)

Once an identity is proven (Control 5.17), we move to **Access Control** with Control 5.18, titled **Access Rights**. This control dictates who gets to see and touch what. It demands a formal, documented process for defining and authorizing access to all assets. The guiding philosophy here is the **Principle of Least Privilege (PoLP)**: users should only have the absolute minimum access required to do their job no more, no less. This control ensures that access is not just handed out arbitrarily; it must be requested, approved, and regularly reviewed to make sure it is still necessary.

ISO 27001 Controls 5.9 & 5.10: Asset Inventory / Asset Management

You can't protect what you don't know you have. These two controls are the bedrock of **Asset Management**.

- **Control 5.9 (Inventory of Information and Other Associated Assets):** This simply requires us to keep a complete, up to date list of every asset that stores, processes, or transmits information hardware, software, data, and services. This inventory is the essential first step for any risk assessment.
- **Control 5.10 (Acceptable Use of Information and Other Associated Assets):** This control is the human element. It sets the ground rules for how people can actually use those inventoried assets. It's about making sure every employee understands their responsibility to use company resources securely and appropriately, preventing accidental or malicious misuse.

ISO to NIST CSF Mapping

As a cybersecurity analyst, my job is not just to follow one standard; it is to build a cohesive security program. Mapping ISO 27001 to the NIST CSF is how we create that bridge, translating the ISO's specific controls into the NIST CSF's risk-based, outcome-focused language.

Mapping ISO 5.17 (Authentication Information)

ISO 5.17 lands squarely in the **Protect (PR)** Function of the NIST CSF, specifically within the **Identity Management, Authentication, and Access Control (PR.AC)** Category.

- **NIST CSF Subcategories: PR.AC-1** (Identities are managed) and **PR.AC-4** (Authentication mechanisms are managed).
- **Reason for Mapping:** ISO 5.17 is the technical backbone of identity verification. PR.AC-1 covers the entire lifecycle of an identity, while PR.AC-4 directly addresses the technical requirements for securing the credentials themselves, such as requiring MFA and strong passwords exactly what ISO 5.17 mandates.
- **Analyst Value:** This mapping is invaluable for **Policy Creation and Auditing**. It gives me the specific, measurable NIST subcategories to anchor our policy statements to (e.g., "MFA is required" is a direct response to PR.AC-4), which makes compliance checks straightforward and defensible.

Mapping ISO 5.18 (Access Rights)

ISO 5.18 also falls under the **Protect (PR)** Function and the **Identity Management, Authentication, and Access Control (PR.AC)** Category.

- **NIST CSF Subcategories: PR.AC-3** (Access permissions are managed) and **PR.AC-5** (Access is managed).
- **Reason for Mapping:** ISO 5.18 is the procedural definition of access rules. PR.AC-3 focuses on the formal process the request, approval, and revocation of permissions.

PR.AC-5 is about the technical enforcement of those rules across all systems, which is the practical outcome of the Least Privilege principle in the ISO control.

- **Analyst Value:** This knowledge is vital for **Risk Assessment**. By focusing on these NIST subcategories, I can systematically identify and assess the risk of "privilege creep" and ensure that our access review and recertification processes are robust and effective.

Mapping ISO 5.9 & 5.10 (Asset Management)

The Asset Management controls are the starting point, so they map to the **Identify (ID)** Function, specifically the **Asset Management (ID.AM)** Category.

- **NIST CSF Subcategories: ID.AM-1** (Physical devices and systems are inventoried) and **ID.AM-3** (Information is classified).
- **Reason for Mapping:** ISO 5.9 is a perfect match for ID.AM-1, which requires a comprehensive inventory of all assets. ISO 5.10 (Acceptable Use) is strongly supported by ID.AM-3, as the rules for acceptable use are fundamentally dependent on how sensitive or critical the information (and thus the asset) is classified.
- **Analyst Value:** This mapping is foundational for **Compliance and Governance**. It ensures that every asset is accounted for and classified, which is the necessary first step for any major compliance effort (like GDPR or HIPAA). It allows me to directly link security controls to the specific business assets they are meant to protect.

Final Security Policies (SANS-Inspired)

The following three policies are designed to be practical, consolidated, and easily understood, following a structure inspired by the SANS Security Policy Templates.

1. Identity Management Policy

Purpose

The goal of this policy is to establish mandatory requirements for the entire lifecycle of user and system identities and their associated authentication information. This is our primary defense against unauthorized access to company assets.

Scope

This policy applies to everyone all employees, contractors, vendors, and any automated process that uses an identity or credentials to access our systems, networks, or data.

Policy Statements (Practical Rules)

1. **Unique Identity:** Every person and every automated process must have a unique, non-shared identity. We do not permit generic or shared accounts unless explicitly approved by the Information Security Team for a specific, documented business need.
2. **Multi-Factor Authentication (MFA):** MFA is a must-have. It is mandatory for all remote access, all privileged accounts, and access to any system containing data classified as Confidential or Secret.
3. **Credential Protection:** Passwords must be strong at least 12 characters, using a mix of cases, numbers, and symbols. They must never be written down, shared, or stored in unencrypted files.
4. **Credential Lifecycle:** When an employee leaves or a contract ends, their account must be disabled immediately. Passwords for service accounts must be changed at least once a year.

Responsibilities

- **Information Security Team:** They own the policy, manage the central identity system, and audit authentication logs regularly.
- **HR Department:** They are responsible for notifying the Information Security Team immediately when an employee's status changes (e.g., termination).
- **End Users:** They are personally responsible for safeguarding their credentials and reporting any suspected compromise immediately.

Compliance (Consequences for Violations)

Any violation of this policy, such as sharing a password or bypassing MFA, will be treated as a serious security breach. Consequences can range from immediate access revocation to termination of employment or contract, and potential legal action.

Related Standards

- ISO 27001:2022 Control 5.17 (Authentication Information)
- NIST CSF PR.AC-1, PR.AC-4

2. Access Control Policy

Purpose

This policy defines the formal process for granting, modifying, and revoking access to all organizational systems and data, ensuring we strictly adhere to the Principle of Least Privilege.

Scope

This policy covers all access granted to information, applications, operating systems, network devices, and physical facilities owned or managed by the organization.

Policy Statements (Practical Rules)

1. **Least Privilege:** Access rights will only be granted to the minimum level required for a user to perform their current job duties. Access must be justified by the user's role.
2. **Formal Authorization:** Every access request must be formally documented, approved by the user's manager *and* the system owner, and logged before any access is provisioned.
3. **Role-Based Access Control (RBAC):** We will manage access primarily through defined roles and groups, rather than granting permissions directly to individuals.
4. **Periodic Review:** All user access rights, especially for privileged accounts, must be reviewed and recertified by the system owner at least every quarter to confirm they are still necessary.

Responsibilities

- **System Owners:** They are responsible for defining the correct access roles for their systems and ensuring the quarterly access reviews are completed.
- **IT Operations:** They handle the technical side: implementing and enforcing the access controls (e.g., provisioning accounts, managing firewall rules).
- **End Users:** They must never attempt to access systems or data for which they have not been explicitly authorized.

Compliance (Consequences for Violations)

Unauthorized access attempts, attempts to bypass access controls, or failure by system owners to complete required access reviews will be treated as a serious security violation, subject to disciplinary action up to and including termination.

Related Standards

- ISO 27001:2022 Control 5.18 (Access Rights)
- NIST CSF PR.AC-3, PR.AC-5

3. Asset Inventory & Management Policy

Purpose

The purpose of this policy is to ensure that all company assets are formally identified, inventoried, classified, and used in an acceptable manner to protect their confidentiality, integrity, and availability.

Scope

This policy applies to all assets, including information (data), software, hardware (laptops, servers, mobile devices), and services, regardless of whether they are company owned or personally owned devices used for work.

Policy Statements (Practical Rules)

1. **Comprehensive Inventory:** We must maintain a complete and accurate inventory of all assets. This inventory must include the asset owner, location, classification, and last update date. The inventory must be reviewed and updated at least monthly.
2. **Asset Ownership:** Every single asset must have a designated Asset Owner who is accountable for its protection and compliance with this policy.
3. **Information Classification:** All information must be classified (e.g., Public, Internal, Confidential, Secret) and handled strictly according to its classification level.
4. **Acceptable Use:** Company assets are to be used primarily for business purposes. Personnel are strictly prohibited from installing unauthorized software, engaging in illegal activities, or using assets in any way that compromises security or violates company policy.

Responsibilities

- **Asset Owners:** They are responsible for ensuring their assets are accurately recorded, correctly classified, and securely disposed of when retired.
- **IT Operations:** They maintain the central asset inventory system and deploy inventory tools.
- **End Users:** They must follow the acceptable use guidelines and report any loss, theft, or suspected compromise of an asset immediately.

Compliance (Consequences for Violations)

Failure to maintain an accurate asset inventory or any violation of the acceptable use guidelines may result in disciplinary action, financial penalties for the department, and potential legal liability for the organization.

Related Standards

- ISO 27001:2022 Controls 5.9 & 5.10 (Asset Management)
- NIST CSF ID.AM-1, ID.AM-3

References

[1] ISO/IEC 27001:2022, Annex A, Control 5.17: Authentication Information.
[2] ISO/IEC 27001:2022, Annex A, Control 5.18: Access Rights.
[3] ISO/IEC 27001:2022, Annex A, Control 5.9: Inventory of Information and Other Associated Assets.

[4] ISO/IEC 27001:2022, Annex A, Control 5.10: Acceptable Use of Information and Other Associated Assets.
[5] National Institute of Standards and Technology (NIST).*Cybersecurity Framework (CSF)*.
[6] SANS Institute.*Security Policy Templates*. (Used as inspiration for policy structure and content).