Assignment:

ISO–NIST CSF Mapping and Policy Development

Part 1 — ISO 27001 Control Interpretation

ISO 27001:2022 Control 5.17 — Identity Management

This control requires organizations to establish and maintain processes that uniquely identify users, validate their identities, and manage identity lifecycles (creation, modification, suspension, and deletion). Its goal is to ensure that only legitimate, authenticated individuals are granted access to organizational systems and resources.

ISO 27001:2022 Control 5.18 — Access Control

This control requires enforcing access restrictions to information and systems based on business needs and the principle of least privilege. It ensures users only receive the minimum level of access required to perform their duties and that access rights are properly authorized, reviewed, and monitored.

ISO 27001:2022 Controls 5.9 & 5.10 — Asset Management & Asset Inventory

These controls ensure organizations maintain a complete, accurate inventory of information assets and assign ownership responsibilities. They require establishing processes to identify, classify, and track assets such as hardware, software, data, and cloud resources. The purpose is to ensure accountability, proper protection, and lifecycle management.

Part 2 — NIST CSF Mapping Table & Justification

ISO 27001 Control	Mapped NIST CSF Functions / Categories / Subcategories	Reason for Mapping
5.17 Identity Management	**PR.AC-1** (Identities are managed) **PR.AC-4** (Access permissions are managed) **PR.AC-6** (Identities authenticated commensurate with risk)	Both frameworks require formal processes for identity lifecycle management, authentication, and ensuring only authorized users access systems.
5.18 Access Control	**PR.AC-3** (Least privilege enforced) **PR.PT-3** (Access to systems is controlled through mechanisms	NIST and ISO both emphasize access restriction, least privilege, monitoring, and enforcement through technical and administrative controls.

ISO 27001 Control	**Mapped NIST CSF Functions / Categories / Subcategories**	**Reason for Mapping**
	like MFA, segmentation, or physical protections) **PR.AC-5** (Network integrity protected by access controls)	
5.9 & 5.10 Asset Management	**ID.AM-1** (Asset inventory) **ID.AM-2** (Asset ownership defined) **ID.AM-5** (Resources prioritized based on classification, criticality, and business value)	Both require identifying, classifying, and assigning ownership of assets to ensure accountability and appropriate protection measures.

How Mapping Supports the Cybersecurity Analyst Role

- **Improves audit readiness:** Understanding cross-framework alignment helps analysts demonstrate compliance to auditors using either standard.
- **Supports risk assessments:** Mapping highlights what controls mitigate which risks, improving prioritization and security gap analysis.
- **Enhances policy development:** Framework mapping ensures enterprise policies align with recognized best practices.
- **Strengthens security operations:** Analysts can validate identity, access, and asset-related controls during investigations, access reviews, and vulnerability assessments.
- **Facilitates communication:** Mapping enables clearer conversation with compliance officers, auditors, and executives using recognized frameworks.

Part 3 — Enterprise Security Policies (SANS-Style)

Below are three consolidated policies written in a formal enterprise format.

Identity Management Policy

1. Purpose

To define requirements for establishing, managing, and governing user identities to ensure only authorized individuals have access to organizational resources.

2. Scope

This policy applies to all employees, contractors, vendors, interns, and service accounts accessing organizational systems, networks, or data.

3. Policy Statements

1. All users must be assigned a unique digital identity (UID) for system access.
2. Identity creation, modification, and removal must follow documented onboarding and offboarding procedures.
3. Authentication must use approved methods such as passwords, MFA, or certificates.
4. Shared or generic accounts are prohibited unless formally approved and monitored.
5. Service accounts must have documented owners and must not be used interactively by humans.
6. Identity records must reflect accurate user status (active, suspended, terminated).
7. Privileged identities must undergo enhanced monitoring and approval.

4. Responsibilities

- **IT Department:** Manage identity systems, provision and deprovision accounts.
- **Security Team:** Enforce identity security requirements and perform periodic access reviews.
- **HR:** Notify IT/security of user role changes or terminations promptly.
- **Managers:** Approve identity creation and privilege changes.
- **End Users:** Maintain secure credentials and comply with authentication requirements.

5. Compliance

Violations may result in disciplinary action, revoked access, or termination depending on severity. Security incidents resulting from non-compliance may lead to investigation.

6. Related Standards

- **ISO 27001:2022 — Control 5.17**
- **NIST CSF — PR.AC-1, PR.AC-4, PR.AC-6**

Access Control Policy

1. Purpose

To define how access to organizational information systems is authorized, enforced, and reviewed to protect confidentiality, integrity, and availability.

2. Scope

Applies to all systems, applications, databases, networks, cloud services, and users interacting with organizational resources.

3. Policy Statements

1. Access must be granted based on least privilege and business need-to-know.
2. All access must be approved by the system or asset owner.
3. Privileged access requires documented justification and multi-factor authentication.
4. Access rights must be reviewed at least quarterly.
5. Users must not attempt to bypass access controls or escalate privileges.
6. System access logs must be retained and monitored.
7. Network segmentation, firewalls, and filtering must enforce access boundaries.

4. Responsibilities

- **IT:** Implement access controls, maintain logs, and manage technical enforcement.
- **Security:** Monitor access patterns, investigate anomalies, and support access reviews.
- **Managers/Owners:** Approve and periodically validate user access.
- **End Users:** Use granted access responsibly and report suspicious activity.

5. Compliance

Unauthorized access attempts or violations may result in access revocation, disciplinary action, or legal consequences.

6. Related Standards

- **ISO 27001:2022 — Control 5.18**
- **NIST CSF — PR.AC-3, PR.AC-5, PR.PT-3**

Asset Inventory & Management Policy

1. Purpose

To ensure all organizational assets are identified, documented, classified, and managed throughout their lifecycle.

2. Scope

Covers all hardware, software, data assets, cloud resources, virtual machines, mobile devices, and third-party hosted systems.

3. Policy Statements

1. All assets must be recorded in the official Asset Inventory Repository.
2. Each asset must have a designated owner responsible for classification and protection.
3. Assets must be tagged or electronically identified (e.g., barcodes, CMDB entries).
4. Critical and sensitive assets must have enhanced protection controls.
5. Unauthorized or unregistered assets are prohibited from connecting to the network.
6. Asset inventories must be reviewed semi-annually for accuracy.
7. Decommissioned assets must follow secure disposal procedures, including data sanitization.

4. Responsibilities

- **IT:** Maintain inventory systems, label assets, and support lifecycle processes.
- **Security:** Oversee accuracy of asset-related controls and classification standards.
- **Asset Owners:** Ensure data classification, risk evaluation, and appropriate protection.
- **End Users:** Use organizational assets responsibly and report missing or damaged assets.

5. Compliance

Non-compliance (e.g., unauthorized devices, missing inventory data) may lead to disciplinary action or restricted system access.

6. Related Standards

- **ISO 27001:2022 — Controls 5.9 & 5.10**
- **NIST CSF — ID.AM-1, ID.AM-2, ID.AM-5**