**INFORMATION SECURITY**



**Session 2023 - 2027**

**Submitted by:**

Sumaira Hafeez 2023-CS-1

**Supervised by:**

Mam Faiza Iqbal

**Course:**

Information Security

Department of Computer Science

**University of Engineering and Technology**

**Lahore Pakistan**

Contents

[Information Security Policy Development 3](#_Toc191637542)

[TASK 1 3](#_Toc191637543)

[**1.** **Case Scenario:** 3](#_Toc191637544)

[**2.** **Issue-Specific Security Policy: Acceptable and Prohibited use of IT resources** 3](#_Toc191637545)

[**d.** **Prohibited Use of Equipment** 3](#_Toc191637546)

[**3.** **System-Specific Security Policy(SysSP): Endpoint and Network Security Configuration:** 4](#_Toc191637547)

[**4.** **Enterprise Information Security Policy:** 5](#_Toc191637548)

[TASK 2 6](#_Toc191637549)

[**1.** **Comparison of** ISO/IEC 27001 and the NIST Cybersecurity Framework 6](#_Toc191637550)

[**2.** **Solution aligning ISO/IEC and NIST:** 7](#_Toc191637551)

[ **Hybrid Framework Integration** 8](#_Toc191637552)

[ **Unique Security Management Policy** 8](#_Toc191637553)

[**3. Integrated Information Security and Cybersecurity Management Policy** 8](#_Toc191637554)

# Information Security Policy Development

# TASK 1

## **Case Scenario:**

You have been hired as an Information Security Officer at a navy federal credit union which serves for military personal’s financial tasks. The organization recently faced a security breach due to employees accessing unauthorized websites, leading to malware infections on several workstations. Following are the policies for the required tasks.

## **Issue-Specific Security Policy: Acceptable and Prohibited use of IT resources**

* + - 1. **Definition:**

It is a policy that addresses a specific issue or area of concern within an organization’s IT environment

* + - 1. **Purpose:**

It defines acceptable and prohibited use of NFCU’s IT resources, ensuring protection of sensitive data.

* + - 1. **Scope:**

It is applicable on all employees, contractors and third parties accessing the system.

* + - 1. **Authorized Access and Usage of System:**
* Access to systems and data is granted based on job roles and responsibilities, following the principle of least privilege.
* Employees may use IT resources for work-related tasks and limited personal use (e.g., checking personal email during breaks) that does not compromise security.
  + - 1. **Prohibited Use of Equipment:**
* Accessing unauthorized websites, including social media, gambling, or streaming platforms, is prohibited.
* Downloading or installing unapproved software or applications is strictly forbidden.
* Sharing login credentials or allowing unauthorized individuals to access NFCU systems is prohibited.
* Using NFCU resources for illegal activities, harassment, or unethical behavior is not allowed.
  + - 1. **Management Responsibilities:**
* Management is responsible for ensuring up to date software.
* Regular penetration testing and vulnerability tests should be conducted to identify and reduce risks.
* Employees must any technical issues to the IT department immediately.
  + - 1. **Reporting policy violations:**
* Employees must report suspected violations to their supervisor or the IT department.
* Anonymous reports can be made through NFCU’s whistleblower hotline or email.
* The IT team will investigate and take necessary action, which may include discipline or legal steps.
  + - 1. **Rules for Violations:**
* First offense: Written warning and mandatory security training.
* Second offense: Suspension of IT access and further disciplinary action.
* Third offense: Termination of employment and potential legal action.

## **System-Specific Security Policy(SysSP): Endpoint and Network Security Configuration:**

* + - 1. **Definition:**

It is a security policy focusing on the protection of a specific IT system, application, or network.

* + - 1. **Purpose:**

It will establish secure configurations for endpoint devices protecting the system infrastructure.

* + - 1. **Scope:**

It applies to all company-owned workstations, laptops, mobile devices, and network systems.

* + - 1. **Antivirus and Firewall settings:**
* All devices must have approved antivirus software with automatic updates enabled.
* Real-time scanning must be on, and a full system scan should run weekly.
* Firewalls must be active, blocking unauthorized traffic.
  + - 1. **Access control Mechanisms:**
* Multi-factor authentication (MFA) is required for sensitive systems and data.
* Role-based access control (RBAC) ensures employees access only what they need.
* Passwords must be at least 12 characters long, include a mix of characters, and be changed every 90 days.
  + - 1. **Encryption Requirements:**
* All sensitive data, including member and financial records, must be encrypted at rest and in transit.
* Endpoint devices must have full-disk encryption (e.g., BitLocker for Windows, FileVault for macOS).
* Emails and file transfers with sensitive data must use encryption protocols like TLS or PGP.

## **Enterprise Information Security Policy:**

* + - 1. **Definition:**

It is a high level security policy that sets the overall direction and framework of the organization’s information security program.

* + - 1. **Purpose:**

The ISSP and SysSP support NFCU’s EISP by ensuring a consistent and thorough approach to information security. The EISP sets the overall framework for protecting information assets, while the ISSP and SysSP focus on specific operational and technical controls.

* + - 1. **Risk Management:**

The ISSP and SysSP mitigate risks identified in the EISP, such as unauthorized access and malware infections.

* + - 1. **Compliance:**

Both policies help maintain compliance with regulations like GLBA and NCUA and follow industry best practices.

* + - 1. **Awareness and Training:**

The ISSP requires security training for employees, reinforcing the EISP’s goal of building a security-conscious culture.

* + - 1. **Continuous Improvement:**

Regular reviews and updates keep the ISSP and SysSP effective and aligned with evolving threats and organizational goals.

# TASK 2

## **Comparison of ISO/IEC 27001 and the NIST Cybersecurity Framework**

* + - * 1. **Similarity:**
* **Risk-Based Approach:** Both frameworks focus on identifying, assessing, and mitigating risks to information assets.
* **Comprehensive Coverage:** They provide guidelines for implementing and maintaining an effective information security management system (ISMS).
* **Continuous Improvement:** Emphasize ongoing monitoring and adaptation to evolving threats and organizational changes.
* **Widely Adopted:** Internationally recognized and used across industries, including healthcare.

**b)**  **Differences:**

a. **Scope:**

* ISO/IEC 27001 focuses on establishing an **Information Security Management System (ISMS)** and achieving certification.
* NIST CSF is designed for **cybersecurity risk management** without requiring certification.

b. **Structure:**

* ISO/IEC 27001 follows the **Plan-Do-Check-Act (PDCA)** cycle and includes specific clauses and annexes.
* NIST CSF is organized into **five core functions**: Identify, Protect, Detect, Respond, and Recover.

c. **Certification:**

* ISO/IEC 27001 offers **formal certification** through accredited bodies.
* NIST CSF does not provide certification but serves as a **voluntary framework** for self-assessment and improvement.

d. **Audience:**

* ISO/IEC 27001 is mainly for organizations looking for **formal compliance and certification**.
* NIST CSF is designed for **organizations of all sizes**, including those in **critical infrastructure**.

e. **Control Set:**

* ISO/IEC 27001 includes a **detailed set of controls** in Annex A, aligned with ISO/IEC 27002.
* NIST CSF offers a **flexible framework**, referencing **NIST SP 800-53** for specific controls.

**f. Regulatory Alignment:**

* ISO/IEC 27001 aligns with **international standards and regulations**.
* NIST CSF aligns with **U.S. federal requirements** and is widely used in **government and critical infrastructure**.

## **Solution aligning ISO/IEC and NIST:**

To enhance compliance and security governance in a healthcare organization, a **hybrid approach** combining **ISO/IEC 27001** and the **NIST Cybersecurity Framework (CSF)** can be implemented. This strategy utilizes ISO/IEC 27001’s **structured certification process** while integrating NIST CSF’s **flexible, outcome-based approach** to build a customized and effective security program.

### **Hybrid Framework Integration**

#### **Map ISO/IEC 27001 and NIST CSF**

* Create a mapping between ISO/IEC 27001 controls (Annex A) and the NIST CSF's five core functions (Identify, Protect, Detect, Respond, Recover).
* Use this mapping to identify gaps and overlaps in the organization's current security practices.

#### **Adopt a Unified Risk Management Approach**

* Use the NIST CSF's **Identify** function to catalog assets, assess risks, and prioritize them.
* Apply ISO/IEC 27001's risk treatment methodology to implement controls and mitigate risks.

#### **Leverage NIST CSF for Flexibility and ISO/IEC 27001 for Certification**

* Use the NIST CSF's **Protect, Detect, Respond, and Recover** functions to design flexible, outcome-based security measures.
* Use ISO/IEC 27001's structured framework to achieve formal certification, demonstrating compliance to stakeholders.

### **Unique Security Management Policy**

**Policy Title:** Integrated Information Security and Cybersecurity Management Policy

**Purpose:** This policy establishes a unified approach to information security and cybersecurity by aligning with **ISO/IEC 27001** and the **NIST Cybersecurity Framework (CSF)**. It aims to protect patient data, enhance security governance, and ensure compliance with regulatory requirements.

## **3. Integrated Information Security and Cybersecurity Management Policy**

**1. Purpose**  
This policy establishes a unified approach to information security and cybersecurity by aligning with **ISO/IEC 27001** and the **NIST Cybersecurity Framework (CSF)**. It aims to protect patient data, enhance security governance, and ensure compliance with regulatory requirements.

**2. Risk Management Practices**

* **Unified Risk Register:** Maintain a single risk register integrating risks identified through ISO/IEC 27001 and NIST CSF methodologies.
* **Threat Intelligence Integration:** Use threat intelligence feeds to enhance risk assessments, aligning with NIST CSF’s Identify function.
* **Third-Party Risk Management:** Extend risk assessments to third-party vendors, ensuring compliance with both frameworks.

**3. Security Control Implementation**

* **Control Selection:** Choose controls from **ISO/IEC 27002 Annex A** and **NIST SP 800-53** based on the organization’s risk profile and regulatory requirements.
* **Zero Trust Architecture:** Implement a **Zero Trust** model for strict access control and continuous verification, aligning with NIST CSF’s Protect function.
* **Automated Incident Response:** Utilize **Security Orchestration, Automation, and Response (SOAR)** tools to automate incident response processes, supporting NIST CSF’s Respond function.

**4. Performance Monitoring and Continuous Improvement**

* **Unified Metrics:** Develop key performance indicators (KPIs) and key risk indicators (KRIs) aligned with both frameworks.
* **Continuous Monitoring:** Deploy a **Security Information and Event Management (SIEM)** system to analyze security events in real-time.
* **Integrated Audits:** Conduct audits to assess compliance with **ISO/IEC 27001** and **NIST CSF**.
* **Feedback Loop:** Apply the **Plan-Do-Check-Act (PDCA)** cycle from ISO/IEC 27001 to drive continuous improvement, integrating lessons learned from NIST CSF’s Recover function.

**5. Specific Security Controls for Protecting Patient Data**  
From **ISO/IEC 27002**:

* **A.12.6.1 - Management of Technical Vulnerabilities:**
  + Implement a vulnerability management program with automated scanning and risk-based remediation.
* **A.18.1.4 - Privacy and Protection of Personally Identifiable Information (PII):**
  + Conduct privacy impact assessments (PIAs) and implement data masking and anonymization techniques.
* **A.10.1.1 - Cryptographic Controls:**
  + Encrypt patient data at rest and in transit using **AES-256** and **TLS 1.3**.
  + Secure cryptographic key management practices.

From **NIST SP 800-53**:

* **AC-4 - Information Flow Enforcement:**
  + Implement **Data Loss Prevention (DLP)** solutions and use **network segmentation** to restrict access to sensitive data.
* **SI-4 - Information System Monitoring:**
  + Deploy **Endpoint Detection and Response (EDR)** tools and use **behavioral analytics** to detect anomalies.
* **IR-4 - Incident Handling:**
  + Establish an **incident response team** with a playbook for data breach response.
  + Conduct regular **tabletop exercises** to test the incident response plan.

**6. Implementation Roadmap**

* **Phase 1: Assessment and Planning (0-3 Months)**
  + Conduct a **gap analysis** against ISO/IEC 27001 and NIST CSF.
  + Develop a **unified risk management framework** and select security controls.
* **Phase 2: Control Implementation (3-12 Months)**
  + Implement **encryption, access control, and monitoring tools**.
  + Train employees on new policies and procedures.
  + Conduct initial internal audits for compliance assessment.
* **Phase 3: Certification and Continuous Improvement (12+ Months)**
  + Prepare for **ISO/IEC 27001 certification** by addressing audit findings.
  + Utilize **NIST CSF’s Recover function** to enhance incident response and business continuity.
  + Establish a **continuous improvement program** using the PDCA cycle.

**7. Benefits of the Hybrid Approach**

* **Comprehensive Coverage:** Combines **ISO/IEC 27001’s structured certification process** with **NIST CSF’s flexible, risk-based approach**.
* **Regulatory Compliance:** Meets international standards (**ISO/IEC 27001**) and U.S. federal requirements (**NIST CSF**).
* **Improved Resilience:** Strengthens detection, response, and recovery capabilities.
* **Stakeholder Trust:** Demonstrates commitment to security and compliance, building confidence among patients, regulators, and partners.