PCI-DSS, ISO 27001, NIST

Name: Ammar Yasser Mohamed
Enterprise Security Department - Summer 2025

Date: August 3, 2025

Overview of PCI-DSS

The **Payment Card Industry Data Security Standard (PCI-DSS)** is a globally accepted set of policies and procedures created to optimize the security of credit, debit, and cash card transactions. It aims to protect cardholders against misuse of their personal information. PCI-DSS is maintained by the *PCI Security Standards Council*, which was founded by Visa, MasterCard, American Express, Discover, and JCB.

Why PCI-DSS Exists

Organizations that store, process, or transmit cardholder data are required to comply with PCI-DSS to prevent data breaches and payment fraud. Compliance ensures the protection of sensitive cardholder data such as PAN (Primary Account Number), CVV, and expiration dates.

The 6 Goals and 12 Requirements

PCI-DSS consists of 6 major security goals, broken into 12 key requirements:

- **Goal 1: Build and Maintain a Secure Network and Systems**
  - Requirement 1: Install and maintain a firewall configuration
  - Requirement 2: Do not use vendor-supplied defaults for system passwords and settings
- **Goal 2: Protect Cardholder Data**
  - Requirement 3: Protect stored cardholder data

  - Requirement 4: Encrypt transmission of cardholder data across open networks
- **Goal 3: Maintain a Vulnerability Management Program**
  - Requirement 5: Protect all systems against malware
  - Requirement 6: Develop and maintain secure systems and applications
- **Goal 4: Implement Strong Access Control Measures**
  - Requirement 7: Restrict access to cardholder data by business need-to-know
  - Requirement 8: Identify and authenticate access to system components
  - Requirement 9: Restrict physical access to cardholder data
- **Goal 5: Regularly Monitor and Test Networks**
  - Requirement 10: Track and monitor all access to network resources and cardholder data
  - Requirement 11: Regularly test security systems and processes
- **Goal 6: Maintain an Information Security Policy**
  - Requirement 12: Maintain a policy that addresses information security

How to Read the PCI-DSS Standard

Each of the 12 requirements is broken down into:

- **Control Objective** – The security goal to achieve
- **Testing Procedures** – What assessors check during an audit
- **Guidance** – Explanation and rationale behind each requirement

Example: Requirement 4

Encrypt transmission of cardholder data across open networks

- Use strong cryptography (TLS 1.2 or higher)
- Never send PANs via email, instant messaging, or unencrypted channels
- Verify certificates and avoid expired or self-signed ones

Who Must Comply with PCI-DSS?

Any organization, regardless of size or number of transactions, that accepts, transmits, or stores cardholder data must comply. There are 4 merchant levels based on transaction volume; each has different validation requirements.

Compliance Levels:

- **Level 1:** Over 6 million card transactions annually – must pass an annual QSA audit
- **Level 2–4:** Lower volumes – may use a Self-Assessment Questionnaire (SAQ)

How to Implement PCI-DSS in Your Environment

1. **Determine the scope:** Identify all systems that interact with cardholder data.
2. **Segment networks:** Isolate the cardholder data environment (CDE).
3. **Use strong encryption:** Encrypt PAN during transmission and storage.
4. **Enforce access control:** Grant least privilege access and use strong authentication.
5. **Keep software updated:** Patch systems and monitor for vulnerabilities.
6. **Maintain logs and monitoring:** Track access to cardholder data.
7. **Train employees:** Educate staff on secure data handling and policies.
8. **Complete SAQ or QSA audit:** Submit proof of compliance to your acquirer bank.

Real-World Example of PCI-DSS Violation

Target (2013) – Hackers accessed network via a third-party HVAC vendor. Malware was used to steal 40 million credit and debit card numbers. Failure to segment the network and lack of sufficient monitoring contributed to the breach.

Relation to Other Standards

PCI-DSS is often cross-referenced with standards such as:

- **ISO 27001** – Information Security Management
- **GDPR** – Data protection regulations for EU citizens
- **NIST** – Cybersecurity frameworks

Overview of ISO/IEC 27001

ISO/IEC 27001 is an international standard for establishing, implementing, maintaining, and continually improving an **Information Security Management System (ISMS)**. Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), it helps organizations manage the security of information assets.

Purpose of ISO 27001

The main goal of ISO 27001 is to protect the **confidentiality, integrity, and availability** (CIA) of information by applying a risk management process and giving confidence to stakeholders that risks are adequately managed.

It is applicable to organizations of all sizes, sectors, and geographies and provides a comprehensive approach to information security.

Core Structure of ISO 27001

ISO 27001 follows the Plan-Do-Check-Act (PDCA) model and consists of:

- **Clauses 4 to 10:** The main requirements (mandatory)
- **Annex A:** A list of 93 security controls grouped into 4 themes

Main Clauses (Mandatory)

1. **Clause 4:** Context of the organization
2. **Clause 5:** Leadership
3. **Clause 6:** Planning
4. **Clause 7:** Support
5. **Clause 8:** Operation
6. **Clause 9:** Performance evaluation
7. **Clause 10:** Improvement

Annex A Themes and Control Sets (2022 Revision)

- **A.5 Organizational controls** – e.g., information security policies, roles, and responsibilities
- **A.6 People controls** – e.g., screening, training, disciplinary processes
- **A.7 Physical controls** – e.g., physical entry controls, asset management

- **A.8 Technological controls** – e.g., access control, malware protection, backups

How to Read ISO 27001

The standard is split into management system clauses and control objectives:

- **Clauses 4–10:** Tell you how to set up and operate an ISMS.
- **Annex A:** Provides optional security controls selected based on risk assessment.
- **Implementation guidance:** Found in ISO/IEC 27002 (used alongside ISO 27001).

Example: Clause 6 – Planning

Clause 6.1.2: Information security risk assessment

- Define criteria for accepting risks
- Identify and evaluate risks
- Decide how to treat the risks (avoid, reduce, share, accept)

Who Should Use ISO 27001?

- Organizations handling sensitive information (banks, hospitals, IT companies, etc.)
- Companies seeking to win client trust or comply with other regulations
- Businesses aiming to get certified to stand out in the market

How to Implement ISO 27001

1. **Define scope and objectives of the ISMS**
2. **Conduct a risk assessment and treatment plan**
3. **Develop necessary policies and procedures**
4. **Implement security controls from Annex A (based on risk)**
5. **Train employees and raise awareness**
6. **Conduct internal audits and management review**
7. **Pursue external certification (optional)**

Real-World Example: ISO 27001 Usage

Microsoft Azure is certified under ISO/IEC 27001, which proves its structured and internationally recognized approach to information security management.

Relation to Other Standards

- **PCI-DSS** – Focused on cardholder data security, while ISO 27001 is broader.
- **NIST CSF** – Offers a flexible cybersecurity framework often used together with ISO 27001.
- **SOC 2** – Covers similar security principles but is based on the AICPA trust service criteria.

Overview of NIST

The **National Institute of Standards and Technology (NIST)** is a U.S. government agency that develops cybersecurity guidelines, including the widely adopted **NIST Cybersecurity Framework (CSF)**. Originally developed for critical infrastructure, it is now used globally by organizations of all types to manage and reduce cybersecurity risks.

Purpose of the NIST Cybersecurity Framework

NIST CSF helps organizations:

- Identify and prioritize cybersecurity risks
- Strengthen defenses through best practices
- Align security initiatives with business needs

The framework is **voluntary**, risk-based, and technology-neutral, enabling customization for diverse environments.

Core Structure of the NIST Framework

The framework has three main components:

1. **Framework Core:** The main body of the CSF with 5 high-level functions
2. **Implementation Tiers:** Levels of organizational maturity and risk management practices
3. **Profiles:** Tailored cybersecurity outcomes based on specific business needs

Framework Core Functions

NIST CSF consists of 5 continuous, concurrent functions:

- **Identify** – Understand the business context, assets, and risks
- **Protect** – Develop safeguards to ensure service delivery
- **Detect** – Identify the occurrence of a cybersecurity event
- **Respond** – Take action regarding detected events
- **Recover** – Maintain plans for resilience and restore operations

How to Read the NIST Framework

Each function is broken down into categories and subcategories with:

- **Outcomes** – What the organization should achieve

- **Informative References** – Related controls from ISO, COBIT, and NIST SP 800-53

Example: Protect Function

Category: Access Control

- Subcategory PR.AC-1: Identities and credentials are managed for authorized devices and users
- Subcategory PR.AC-4: Access permissions are managed, incorporating the principle of least privilege

Who Should Use NIST CSF?

- U.S. federal and critical infrastructure organizations (original target)
- Private companies and global enterprises seeking structured cybersecurity management
- Organizations adopting a flexible, scalable, and adaptable framework

How to Implement the NIST Framework

1. **Set objectives and identify risks**
2. **Create a Current Profile** (your current state)
3. **Create a Target Profile** (desired security posture)
4. **Perform a gap analysis and prioritize actions**
5. **Implement improvements and monitor progress**

Real-World Example: NIST Adoption

U.S. Federal Agencies – Required to follow NIST standards (e.g., NIST SP 800-53). Large enterprises like Intel and Bank of America also map their security programs to the NIST CSF to align with industry best practices.

Relation to Other Standards

- **ISO 27001** – Compatible and often mapped to the NIST CSF for international adoption
- **PCI-DSS** – NIST provides a broader framework, PCI-DSS focuses on cardholder data
- **COBIT, CIS Controls** – Often used in conjunction with NIST to enhance security governance