Tishk International University
Faculty of Applied Science
Cybersecurity Department

Lecture 9 : Compliance, Regulatory Frameworks & Risk Management

CBS221/A : Ethics and Legal Issues in Cybersecurity

Week 9 : 07-11/12/2025

Instructor: Prof. Dr. Qaysar Salih Mahdi

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Week 9 – Compliance, Regulatory Frameworks & Risk Management

- Objectives:
- 1. Understand cybersecurity compliance requirements
- 2. Explore key frameworks (NIST, ISO 27001, PCI DSS, GDPR)
- 3. Calculate compliance risk and interpret results
- 4. Apply frameworks to real-world scenarios

Introduction to Compliance & Regulatory Frameworks

- - Definition of compliance and regulatory frameworks
- - Importance in cybersecurity governance
- - - Explanation: Policies → Standards → Procedures → Audits

Definition of compliance and regulatory frameworks

Understanding Cybersecurity Compliance:

Key Regulations.

Is your business compliant with relevant laws and safe from cyber threats? Dive into our guide on cyber security compliance to uncover the essential steps and regulations that will keep your data secure and your organisation compliant, avoiding legal consequences.

We'll explore theimportance of cyber security compliance and the common regulations businesses need to adhere to, such as GDPR, HIPAA, and PCI DSS.

Discover practical steps to achieve compliance, including conducting risk assessments, implementing strong password policies, and monitoring security incidents.

What is cyber security compliance?

Cyber security compliance refers to adhering to and implementing regulations, standards, and practices to safeguard sensitive data and information systems within organisations.

Ensuring cyber security compliance is necessary to protect your organisation against cyber threats and data breaches. By aligning with industry-specific regulations such as PCI DSS, organisations can uphold data privacy and build customer trust. Effective compliance management also helps mitigate risk by identifying vulnerabilities and implementing controls to prevent unauthorised access.

Maintaining a solid security posture through regular audits and assessments helps your organisation stay resilient against evolving cyber threats. However, non-compliance can lead to financial penalties, reputational damage, and legal consequences.

Why is cyber security compliance important for your organisation?

By aligning with relevant regulatory standards, you can enhance your organisation's defensive mechanisms and establish a robust cyber security framework. This proactive approach protects sensitive data, avoids legal consequences, and builds customers trust.

Protect sensitive data

One of the primary benefits of cyber security compliance is protecting sensitive data from unauthorised access, breaches, and misuse, ensuring data privacy and integrity. Data privacy regulations, such as GDPR, require your organisation to protect personal information through measures like encryption and secure access controls.

If there is a security incident, having stringent incident response protocols can minimise the impact and mitigate potential damages. By integrating these data protection and security measures, your organisation can foster trust among your customers and stakeholders.

Avoid legal consequences

When your organisation complies with cyber security regulations, you avoid legal consequences such as fines, penalties, and lawsuits resulting from non-compliance with data protection laws and regulations.

Non-compliance can lead to severe repercussions, including hefty financial penalties. In addition to immediate financial implications, organisations may face reputational damage, loss of customer trust, and potential lawsuits from individuals affected by data breaches.

Build trust with customers

Maintaining cyber security compliance enhances your organisation's credibility. It builds customer trust by demonstrating a commitment to data protection, security, and regulatory compliance.

By adhering to industry best practices and obtaining compliance certifications such as ISO 27001 or SOC 2, your organisation signals its dedication to maintaining high levels of security and confidentiality.

Transparency in data handling practices also conveys confidence among customers, as they value knowing how their data is collected, processed, and protected.

What are the common cyber security compliance regulations you need to know?

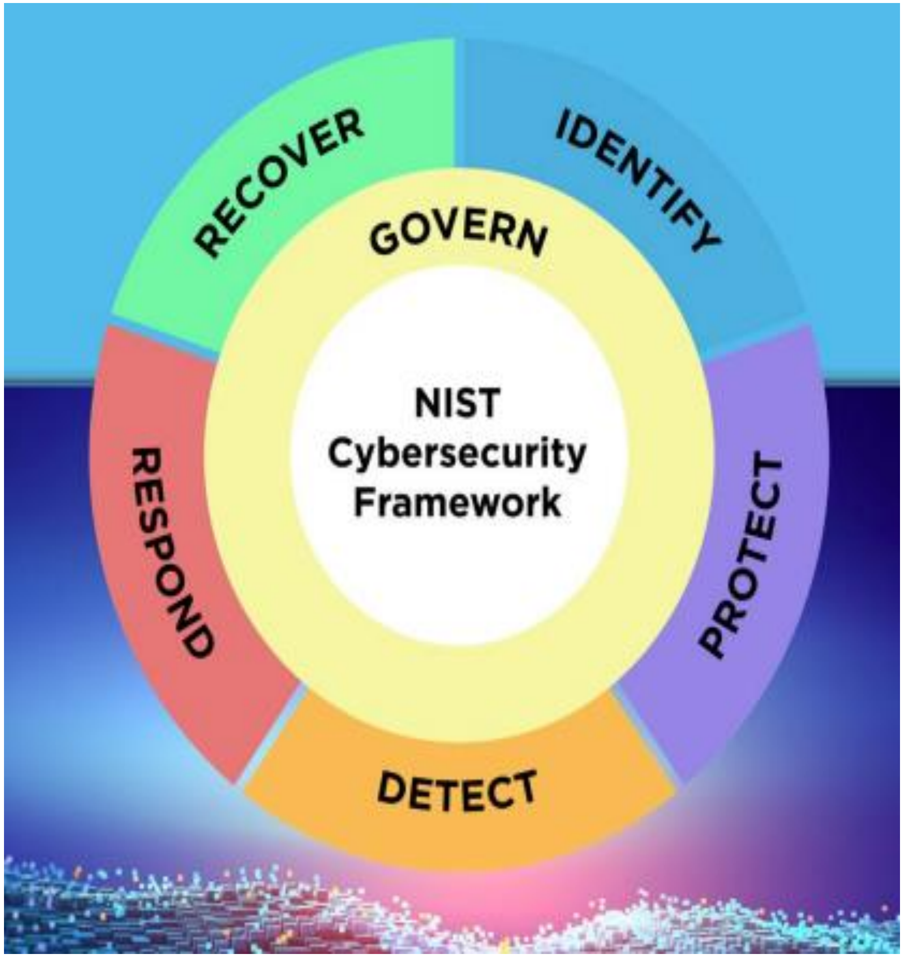
There are many different cyber security regulations. But which ones should you really know about? Common cyber security compliance regulations include the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS), among others, that outline specific requirements for data protection and security measures.

- GDPR focuses on protecting personal data and applies to organisations that handle or process data of EU residents. It mandates companies to obtain explicit consent for data collection and specifies fines for non-compliance.
- HIPAA safeguards patients' medical records and health information, requiring healthcare entities to implement safeguards to protect sensitive data. While HIPAA is a US regulation, private providers from the UK operating in the US must also adhere to it.
- PCI DSS ensures secure payment card transactions and mandates compliance for any organisation that accepts, processes, stores, or transmits cardholder data.

Compliance with these regulations safeguards organisations from data breaches and financial penalties and builds trust with customers, partners, and regulatory authorities.

NIST Cybersecurity Framework Core

- NIST CSF Core functions (Identify, Protect, Detect, Respond, Recover)
- - Explanation: Interaction of five functions to manage cybersecurity risk
- - Example: Mapping internal IT processes to NIST CSF



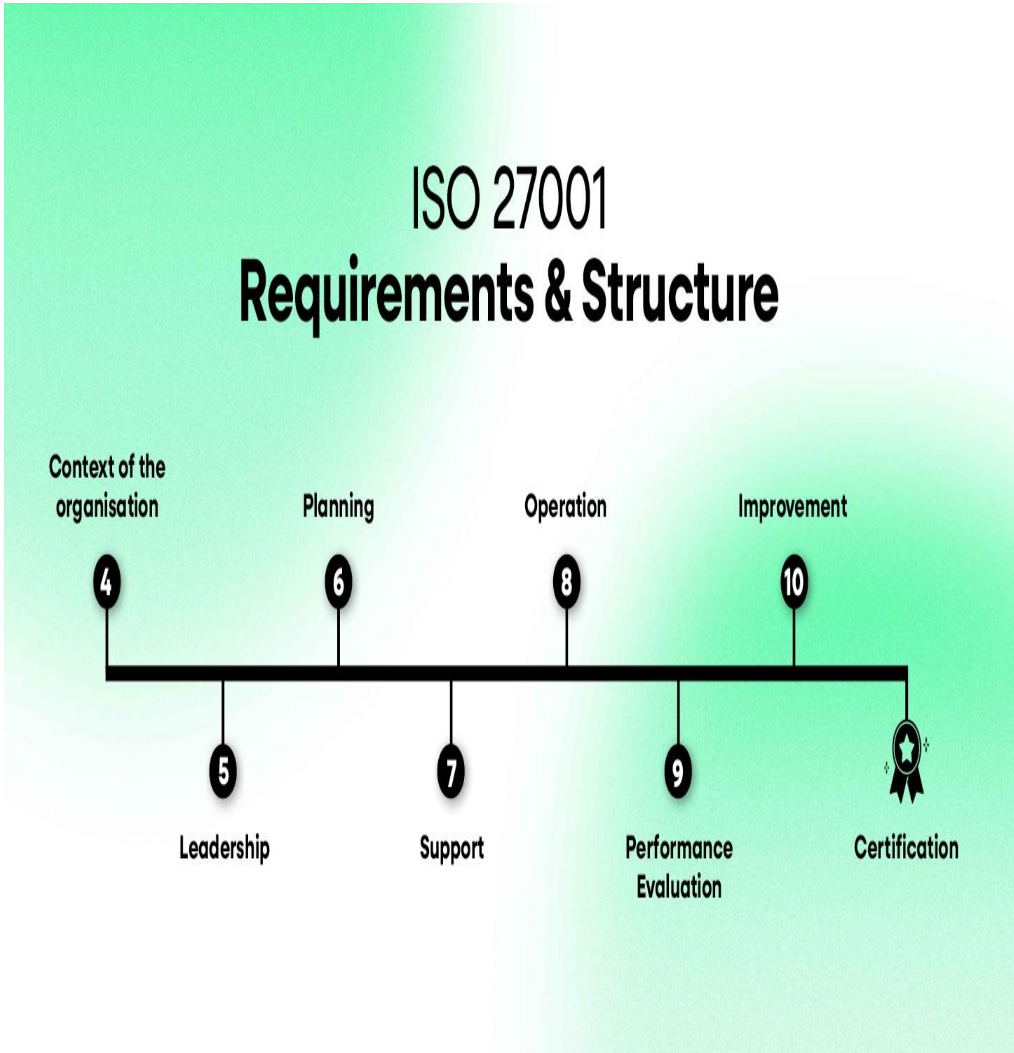
What is the Cybersecurity Framework and what was it created to accomplish?

AVM: The Framework for Improving Critical Infrastructure Cybersecurity, or the Cybersecurity Framework as many of us refer to it, is voluntary guidance for organizations to better manage and reduce their cybersecurity risk. NIST developed the Framework at the direction of the White House with the active participation of industry, academia and multiple levels of government. It's designed to be a "common language" that spans the entirety of cybersecurity risk management and that can be easily understood by people with all levels of cybersecurity expertise. Five functions comprise the core of the Framework: Identify, Protect, Detect, Respond and Recover. Under these overarching functions, the Framework provides a catalog of cybersecurity outcomes based on existing standards, guidelines and practices that organizations can customize to better manage and reduce their cybersecurity risk.

Although we designed the Framework specifically for companies that are part of the U.S. critical infrastructure, many other organizations in the private and public sectors are using and gaining value from the approach. A 2017 Executive Order requires federal agencies to use it, but the Cybersecurity Framework remains voluntary for industry. Twenty-one states are using it, and we have also seen an increase in the use and adaptation of the Framework internationally.

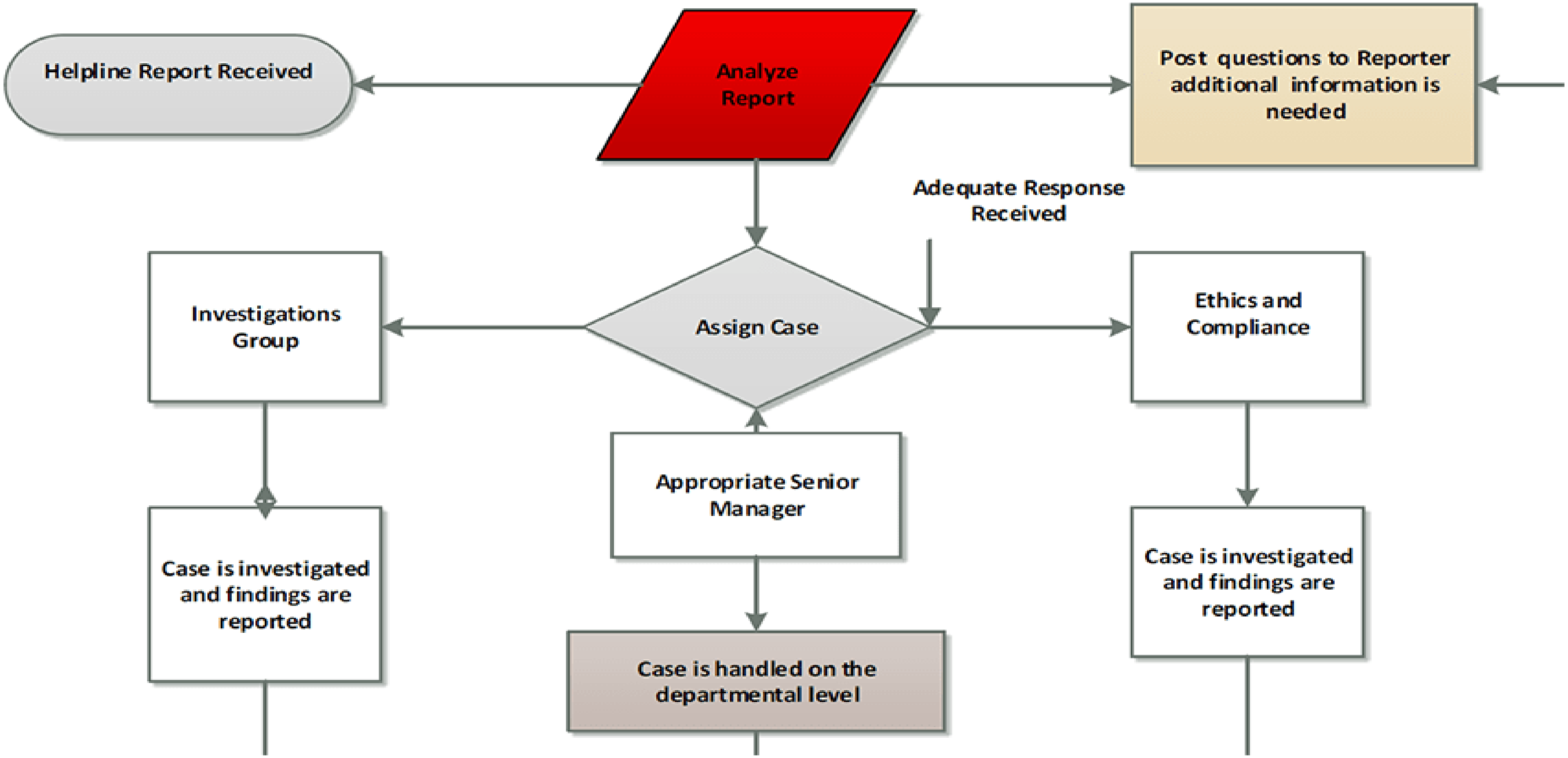
ISO 27001 ISMS Structure

- ISMS structure and certification cycle
- - Link: https://www.iso.org/isoiec-27001-information-security.html
- - Explanation: PDCA (Plan-Do-Check-Act) cycle for continuous security improvement
- - Example: Implementation in a mid-size IT company



Tishk International University
Faculty of Applied Science
Cybersecurity Department

Risk Compliance Policy Management Flow Chart


Helpline Report Received
Analyze Report
Post questions to Reporter additional information is needed
Adequate Response Received
Investigations Group
Assign Case
Ethics and Compliance
Appropriate Senior Manager
Case is investigated and findings are reported
Case is handled on the departmental level
Case is investigated and findings are reported

Compliance Risk Formula & Calculation Example

- - Formula: $CR = (I \times V) / C$
- - I = Impact, V = Vulnerability, C = Controls
- - Example Problem: I=8, V=6, C=4 → CR=12

PCI Security

The PCI Security Standards Council touches the lives of hundreds of millions of people worldwide. A global organization, it maintains, evolves and promotes Payment Card Industry standards for the safety of cardholder data across the globe.

Who We Serve

We serve those who work with and are associated with payment cards. This includes: merchants of all sizes, financial institutions, point-of-sale vendors, and hardware and software developers who create and operate the global infrastructure for processing payments.

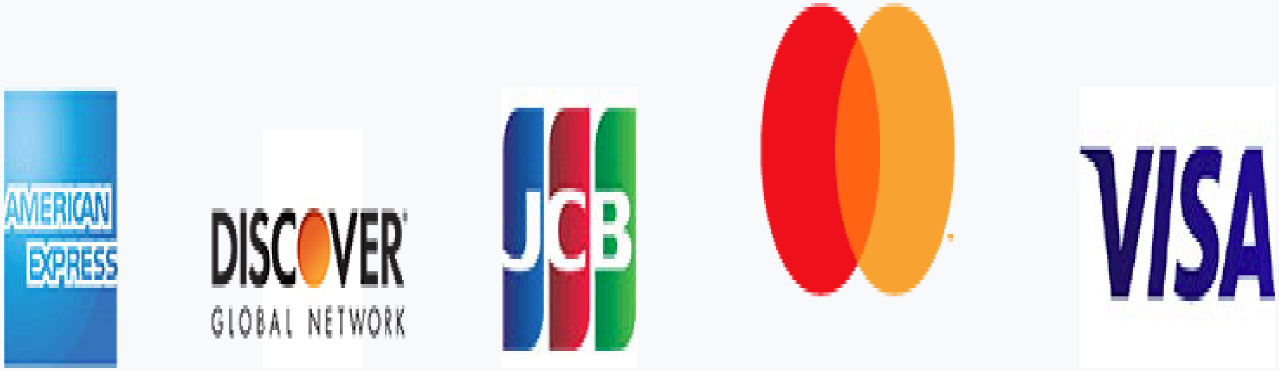
What We Do

There are two priorities for our work:

- Helping merchants and financial institutions understand and implement standards for security policies, technologies and ongoing processes that protect their payment systems from breaches and theft of cardholder data.

- Helping vendors understand and implement standards for creating secure payment solutions.

The Council was founded in 2006 by American Express, Discover, JCB International, Mastercard and Visa Inc. They share equally in ownership, governance, and execution of the Council's work.



Security Matters

From customers to merchants and financial institutions, the security of cardholder data affects everybody. Discover how securing cardholder data can help preserve customer trust, ensure compliance, and benefit your organization in the long term.

The PCI Security Standards

Maintaining payment security is required for all entities that store, process or transmit cardholder data. Guidance for maintaining payment security is provided in PCI security standards. These set the technical and operational requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.

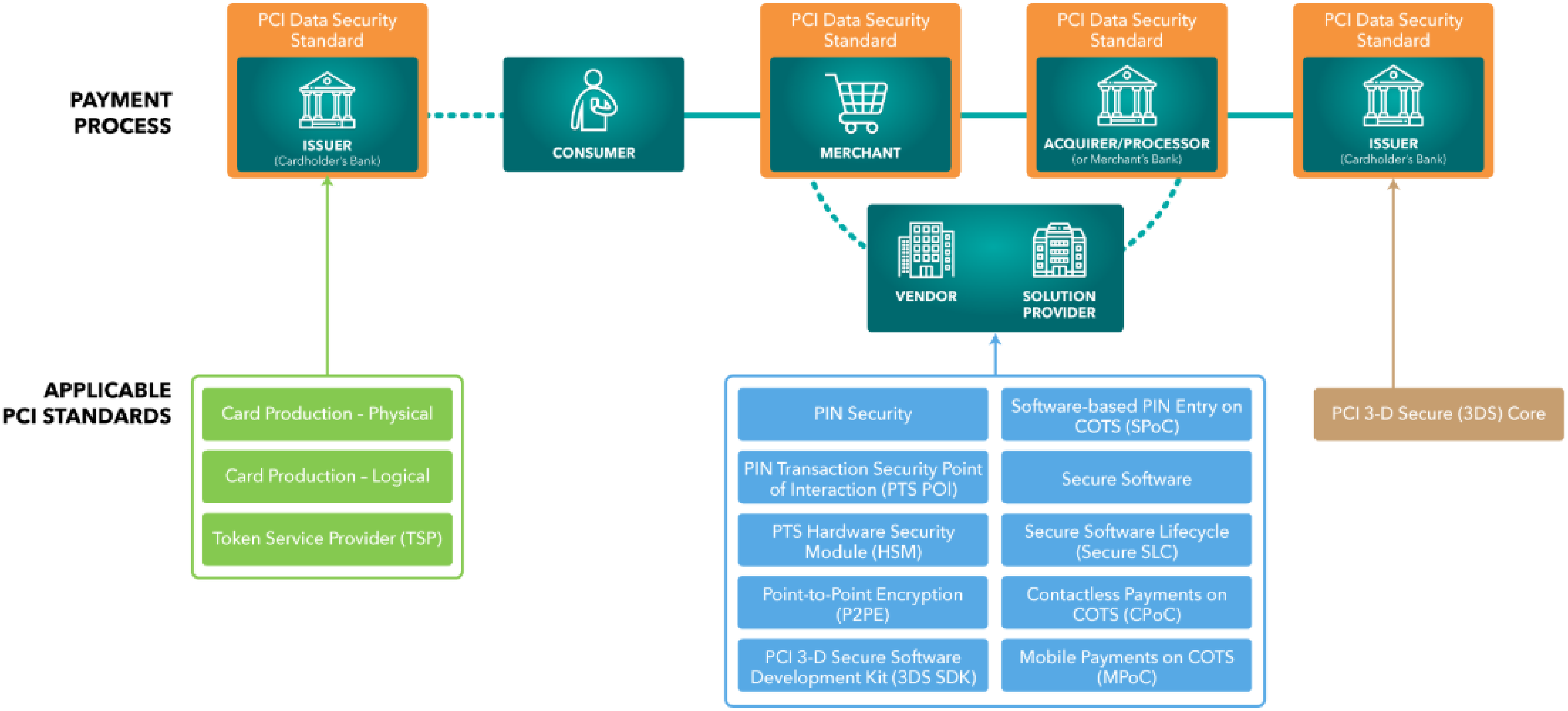
How to Secure

Following guidance in the PCI Data Security Standard helps keep your cyber defenses primed against attacks aimed at stealing cardholder data.

Assessing the Security of Your Cardholder Data

Most small merchants can use a self-validation tool to assess their level of cardholder data security. The Self-Assessment Questionnaire includes a series of questions for each applicable PCI Data Security Standard requirement. There are different SAQs available for a variety of merchant environments.

The PCI Security Standards Ecosystem


PAYMENT PROCESS
PCI Data Security Standard
ISSUER (Cardholder's Bank)
CONSUMER
PCI Data Security Standard
MERCHANT
PCI Data Security Standard
ACQUIRER/PROCESSOR (or Merchant's Bank)
PCI Data Security Standard
ISSUER (Cardholder's Bank)
VENDOR
SOLUTION PROVIDER
APPLICABLE PCI STANDARDS
Card Production - Physical
Card Production - Logical
Token Service Provider (TSP)
PIN Security
Software-based PIN Entry on COTS (SPoC)
PIN Transaction Security Point of Interaction (PTS POI)
Secure Software
PTS Hardware Security Module (HSM)
Secure Software Lifecycle (Secure SLC)
Point-to-Point Encryption (P2PE)
Contactless Payments on COTS (CPoC)
PCI 3-D Secure Software Development Kit (3DS SDK)
Mobile Payments on COTS (MPoC)
PCI 3-D Secure (3DS) Core

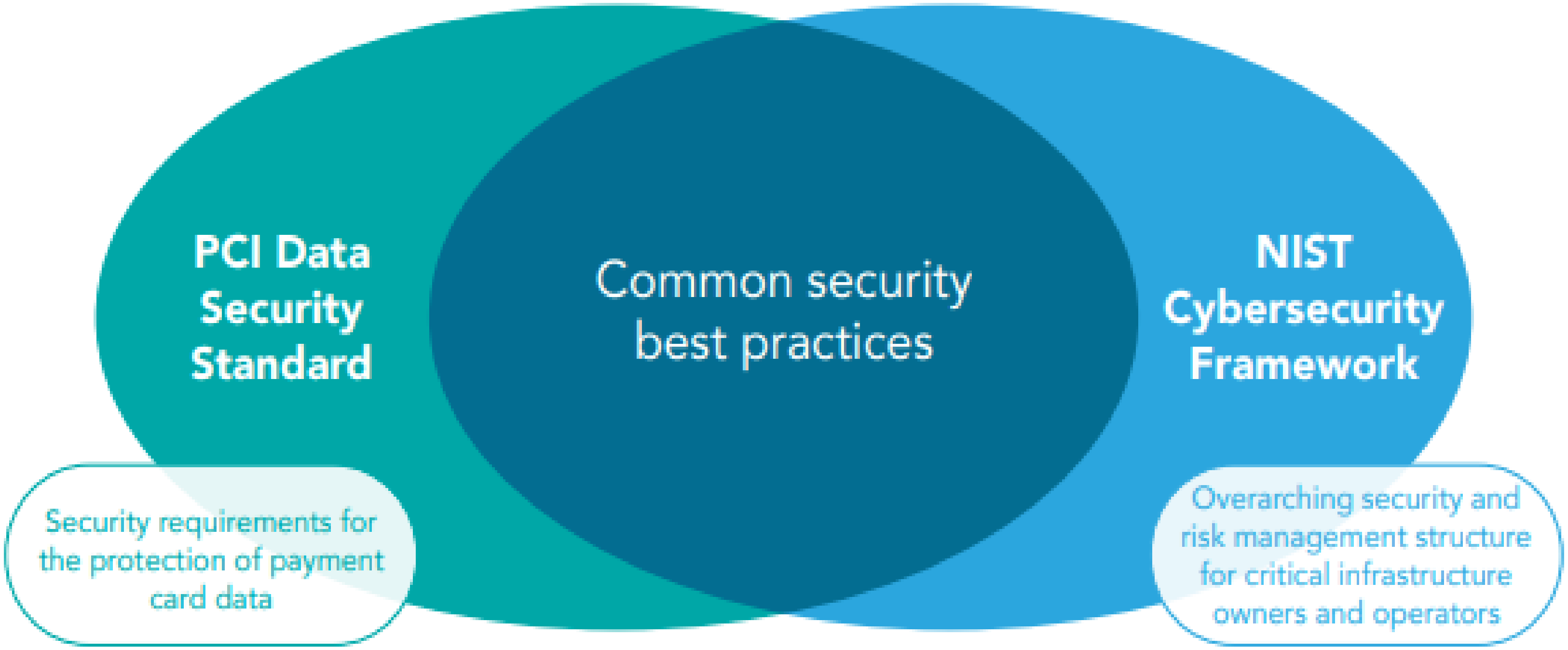
This diagram notes applicable PCI Security Standards. Contact payments brands for any related compliance programs.

- **HW1 : NIST vs ISO vs PCI DSS vs GDPR**

- Links:

- **NIST: https://www.nist.gov/cyberframework**
- **ISO: https://www.iso.org/isoiec-27001-information-security.html**
- **PCI DSS: https://www.pcisecuritystandards.org**
- **GDPR: https://gdpr-info.eu**
- **HW2 : Explanation: Differences in scope, enforcement, approach**

The PCI Data Security Standard (PCI DSS) and the NIST Cybersecurity Framework share the common goal of enhancing data security. The Mapping of PCI DSS to the NIST Cybersecurity Framework provides a resource for stakeholders to use in understanding how to align security efforts to meet objectives in both PCI DSS and the NIST Framework.



PCI Data Security Standard

Common security best practices

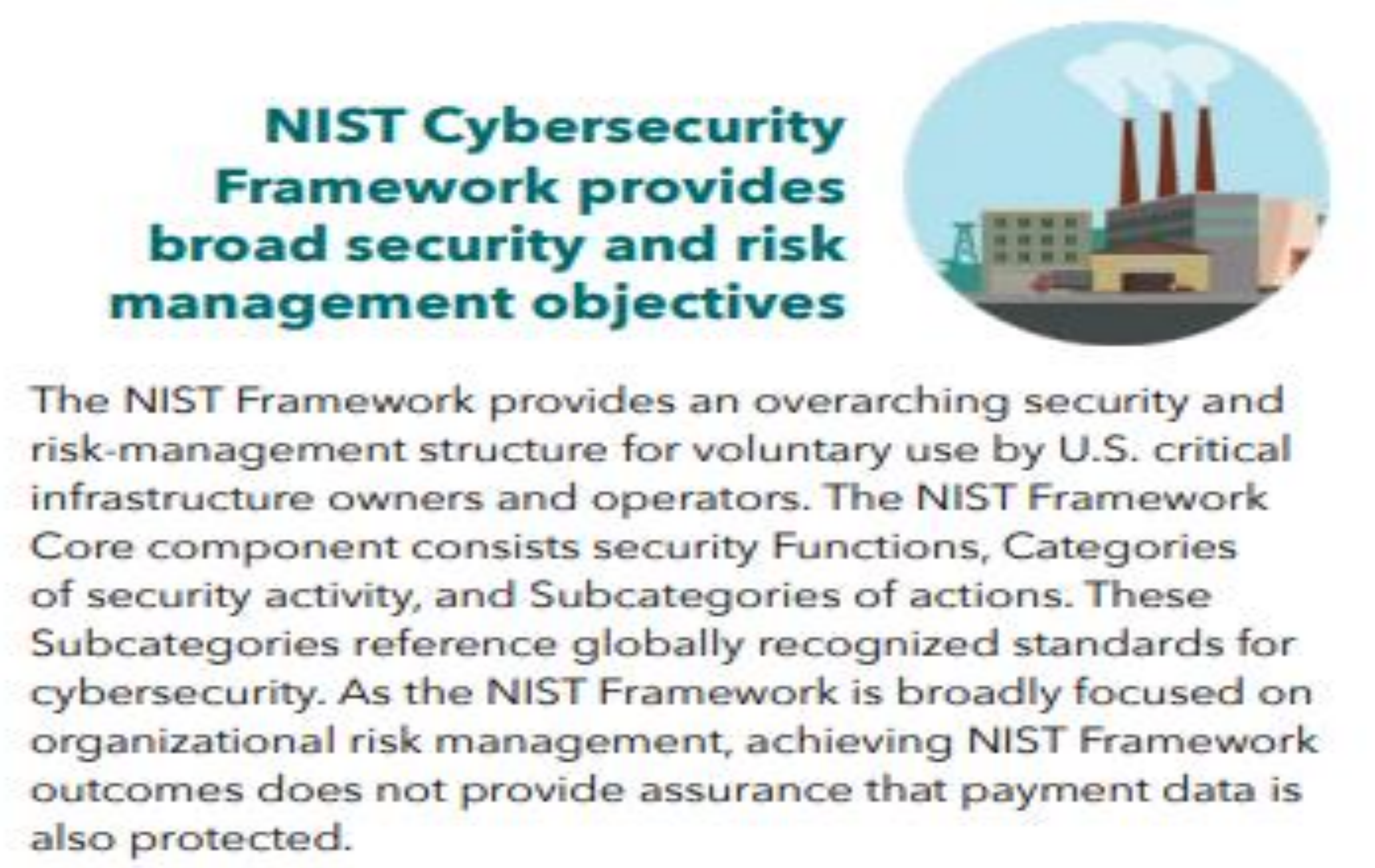
NIST Cybersecurity Framework

Security requirements for the protection of payment card data

Overarching security and risk management structure for critical infrastructure owners and operators

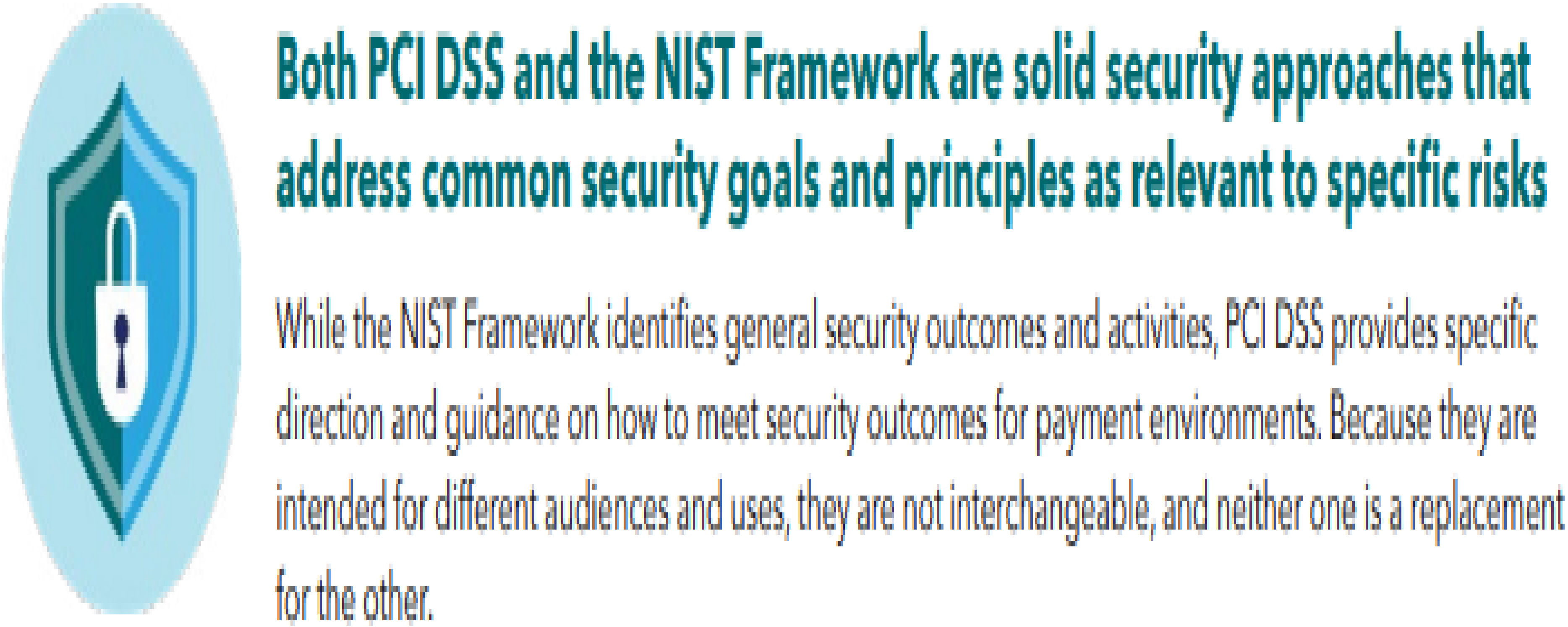
PCI DSS provides specific security requirements for payment card data

PCI DSS defines security requirements for the protection of payment card data, as well as validation procedures and guidance to help organizations understand the intent of the requirements. Rapid changes in threats require more detailed standards for payment security. PCI DSS is focused on the unique threats and risks present in the payments industry. It is intended for all entities involved in storing, processing, or transmitting payment card data, and provides foundational security requirements across twelve main security objectives to protect payment environments.



NIST Cybersecurity Framework provides broad security and risk management objectives

The NIST Framework provides an overarching security and risk-management structure for voluntary use by U.S. critical infrastructure owners and operators. The NIST Framework Core component consists security Functions, Categories of security activity, and Subcategories of actions. These Subcategories reference globally recognized standards for cybersecurity. As the NIST Framework is broadly focused on organizational risk management, achieving NIST Framework outcomes does not provide assurance that payment data is also protected.

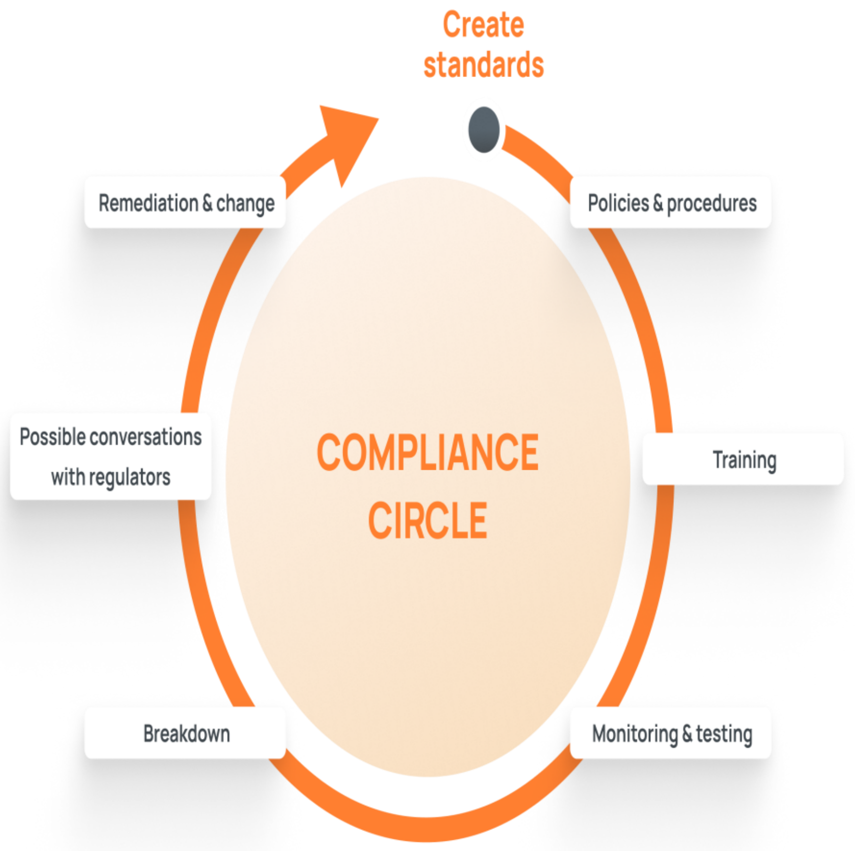


Both PCI DSS and the NIST Framework are solid security approaches that address common security goals and principles as relevant to specific risks

While the NIST Framework identifies general security outcomes and activities, PCI DSS provides specific direction and guidance on how to meet security outcomes for payment environments. Because they are intended for different audiences and uses, they are not interchangeable, and neither one is a replacement for the other.

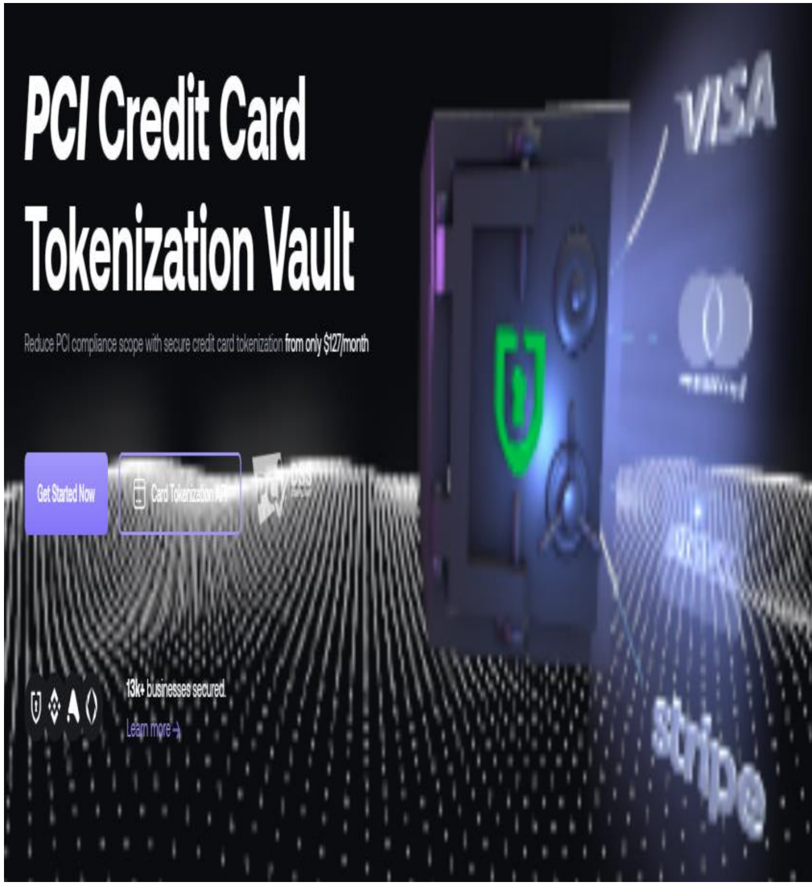
Real-World Case Study 1

- - GDPR compliance in a European financial company
- - Steps taken, challenges faced, outcomes
- - Diagram showing compliance process
- - Link: https://gdpr-info.eu



Real-World Case Study 2

- - PCI DSS implementation in a retail payment system
- - Lessons learned and key metrics
- - Diagram: Payment security controls
- - Link: https://www.pcisecuritystandards.org



PCI Credit Card Tokenization Vault

Reduce PCI compliance scope with secure credit card tokenization **from only $127/month**

13k+ businesses secured.

https://pcivault.io/?gad_source=1&gad_campaignid=1749394532&gbraid=0AAAAAD0KWCg7sfpLyDZ3dTwoHcYTWRKyh&gclid=CjwKCAjwmNLHBhA4EiwA3ts3mQ461FVxYRLge38Dq74UYWBbLfFxydrD8HwQiT2jAnqd94k_36TuPRoCME0QAvD_BwE

Practice Problems / Step-by-Step Solutions

- - Problem 1: Calculate CR for I=8, V=6, C=4 → Solution: 12
- - Problem 2: Map an internal control process to NIST CSF → Step-by-step solution

Key Takeaways & Conclusion

- - Regulatory frameworks ensure governance, risk management, legal compliance
- - NIST, ISO 27001, PCI DSS, GDPR complement each other
- - Compliance risk scoring prioritizes security measures
- - Continuous monitoring and audit are critical
- - Diagram: Continuous Compliance Cycle

References (IEEE Style)

- 1. NIST Cybersecurity Framework: https://www.nist.gov/cyberframework
- 2. ISO/IEC 27001: https://www.iso.org/isoiec-27001-information-security.html
- 3. PCI DSS: https://www.pcisecuritystandards.org
- 4. GDPR: https://gdpr-info.eu