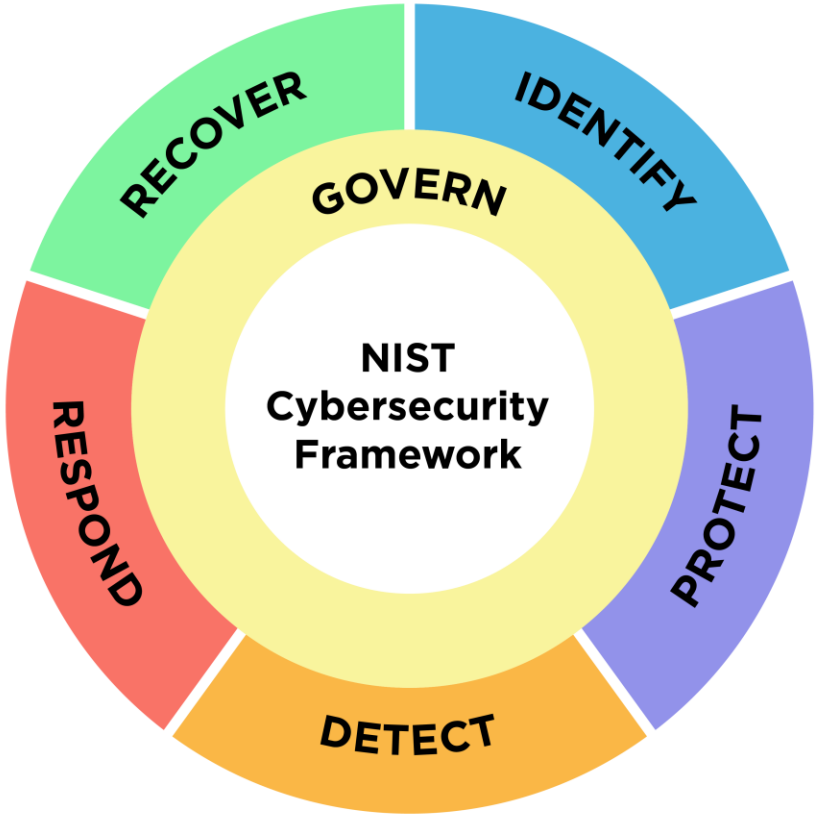
NIST FRAMEWORK



INDEX

Key Components

Identify: Understand and catalog assets, risks, and vulnerabilities within an organization.

Protect: Implement measures to safeguard systems, data, and infrastructure from potential threats.

Detect: Employ methods to recognize and promptly identify security breaches or anomalies.

Respond: Develop and execute response plans to mitigate and address detected cybersecurity incidents.

Recover: Develop strategies to restore capabilities and services after a cybersecurity event, aiming for resilience.

Purpose Of The Framework

Framework Purpose:

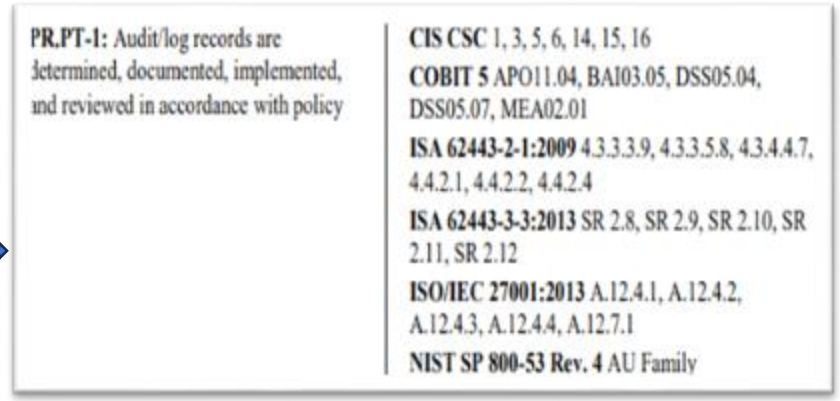
Developed by NIST, it offers guidelines, standards, and best practices for enhancing cybersecurity and managing risk.

Core Functions:

The framework revolves around five primary functions: Identify, Protect, Detect, Respond, and Recover (IPDRR), providing a structured approach to cybersecurity.

Core of the framework

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO



PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**CIS CSC** 1, 3, 5, 6, 14, 15, 16 **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 **NIST SP 800-53 Rev. 4** AU Family

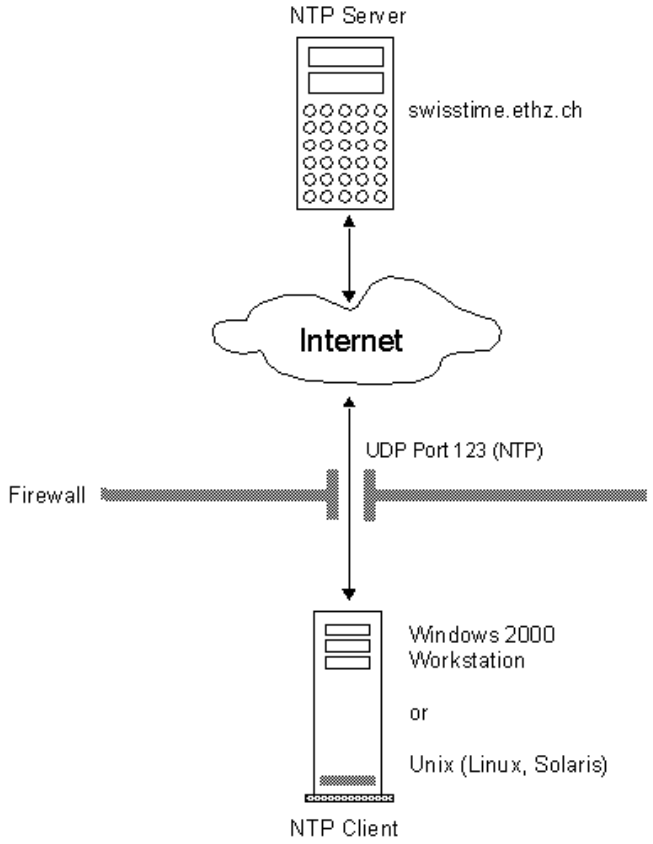
Importance of PR-PT1 Control in NIST Framework:

- Foundational for Incident Investigation.
- Forensic Analysis and Compliance.
- Crucial for forensic analysis, ensuring that digital evidence is reliable and legally admissible.
- Assists in meeting compliance standards that require accurate timestamping for audit trails.
- Coordination and Response.
- Data Integrity and Authenticity.
- Upholds the authenticity of logs and records, preventing manipulation or tampering.
- Operational Continuity.
- Unifies time-sensitive security measures and responses.
- Compliance and Regulatory Requirements.

Importance of Clock Synchronization in Cyber Security.

Log Management and Correlation

- Synchronized clocks ensure timestamps across various system logs are consistent and accurate.
- Accurate timestamps aid in correlating events during forensic investigations.
- Timestamp consistency is vital for reconstructing the sequence of events during a security incident or breach.
- It enables a clear timeline for understanding how an attack unfolded across different systems.
- Inaccurate timestamps due to unsynchronized clocks can hinder incident response and forensic analysis.



Security Protocols and Authentication

- Synchronized clocks in security protocols (e.g., Kerberos, SSL/TLS) are essential for accurate timestamping.

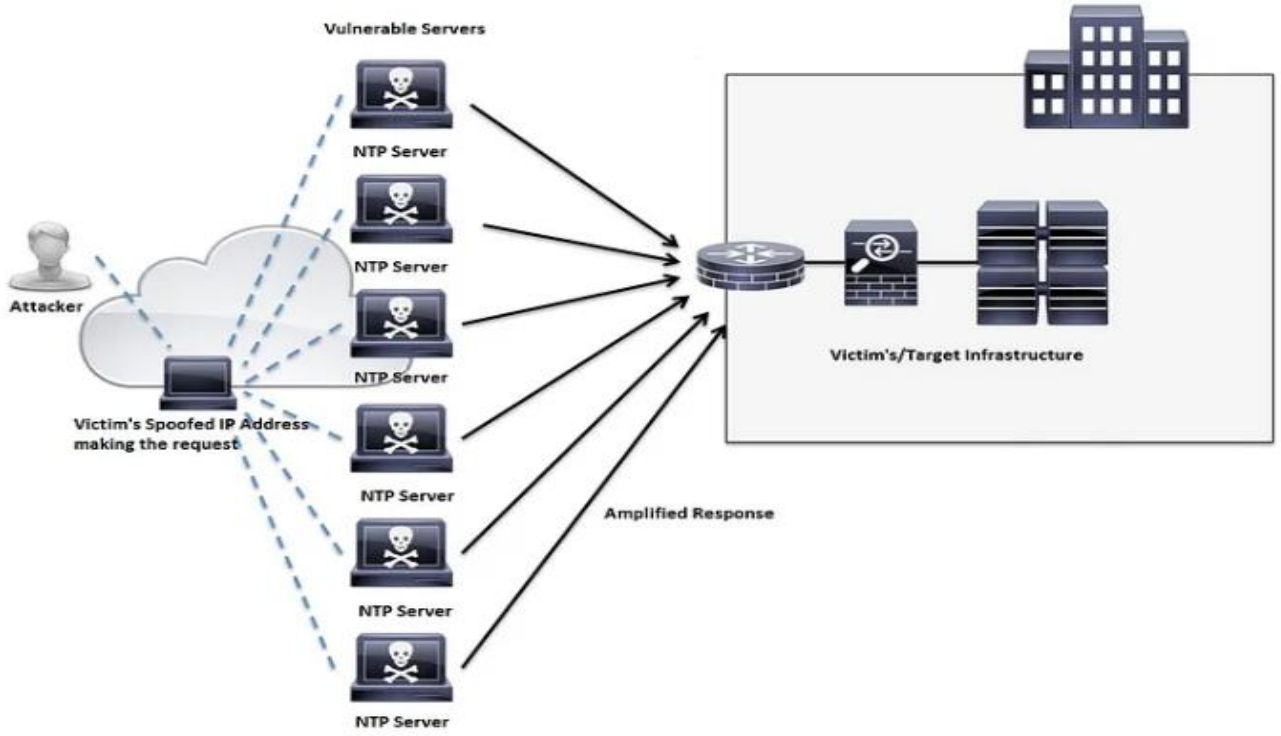
- They guarantee the validity of certificates and tokens.

- Unsynchronized clocks create vulnerabilities that attackers can exploit through time-related weaknesses.

Clock Synchronization- Implementation

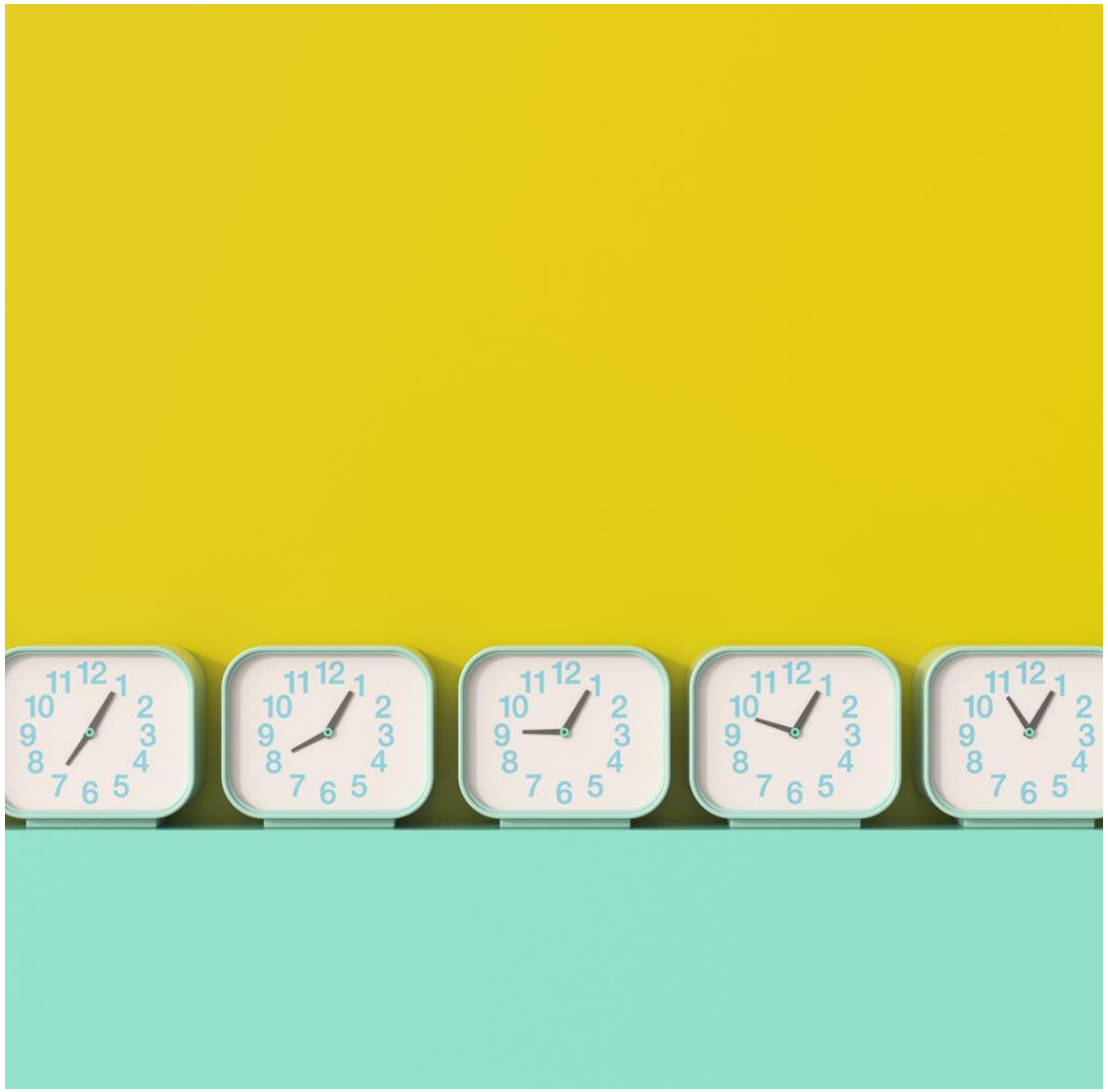
Network Time Protocol (NTP)

- NTP servers facilitate regular clock synchronization across a network.
- Organizations have the option to set up their own NTP servers or use public ones available on the internet.
- Devices synchronize their clocks periodically with these NTP servers.
- Regular synchronization ensures the maintenance of accurate time across the network.



Active Directory Time Service (Windows-based environments)

- Within a Windows domain environment, the Active Directory Time Service is utilized for time synchronization.
- The primary domain controller is designated as the authoritative time source.
- Other devices within the domain are configured to sync their clocks with this primary domain controller.



Case Study And Examples

Financial Sector Frauds:

Example: In financial institutions, synchronized clocks are vital for accurate transaction timestamps.

Impact: In cases of fraudulent activities like unauthorized fund transfers or market manipulations, synchronized clocks help investigators reconstruct timelines accurately. Discrepancies in transaction times can indicate potential tampering or fraudulent activities, aiding in identifying and resolving such incidents.

Data Breaches and Network Intrusions:

Example: During a network breach, synchronized clocks aid in correlating events across multiple systems.

Impact: In incidents involving malware infections or unauthorized access, synchronized clocks help cybersecurity teams track the spread of malware, identify the entry point, and understand the sequence of events. This information is crucial for containment and remediation efforts.

Conclusion

In conclusion, the synchronization of clocks plays a pivotal role in fortifying cybersecurity measures. It forms an integral part of the Protect function within the NIST Cybersecurity Framework, specifically control PR.PT-1, ensuring the safeguarding of physical devices and systems from unauthorized access.