

NIST CYBERSECURITY FRAMEWORK

Prepared By: Shriya roi



CYBERSECURITY FRAMEWORK

A collection of finest practices that an organization must follow to manage its cybersecurity risk.

Goal of the framework:

- Reduce company's exposure to cyberattacks
- Identify areas at higher risk for data breaches
- Monitor the compromising activities of cyber criminals



TYPES OF SECURITY FRAMEWORK



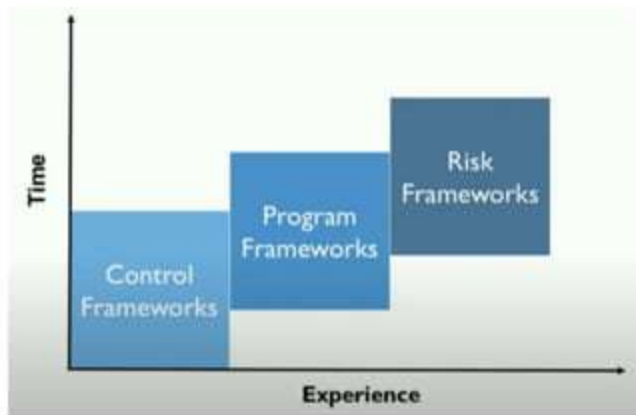
Control Framework



Program Framework



Risk Framework



Purpose	Control Framework	Program Framework	Risk Framework
<p>Use of the Framework</p> 	<ul style="list-style-type: none"> • Identify baseline of controls • Assess state of technical capabilities • Prioritize implementation of controls • Develop an initial roadmap for the security team 	<ul style="list-style-type: none"> • Assess state of the overall security program • Build a comprehensive security program • Measure maturity and conduct industry comparisons • Simplify communication with business leaders 	<ul style="list-style-type: none"> • Define key process steps for assessing and managing risk • Structure risk management program • Identify, measure and quantify risk • Prioritize security activities

NIST CYBERSECURITY FRAMEWORK



Program Framework

- Assess state of the overall security program
- Build a comprehensive security program
- Measure maturity and conduct industry comparisons
- Simplify communication with business leaders



There are two frameworks defined under Program Framework:

- ISO 27001
- **NIST Cyber Security Framework**

DEEP DIVE INTO: NIST CYBERSECURITY FRAMEWORK

Identify

Protect

Detect

Respond

Recover



- Composed of three parts:
 - Core
 - Implementation Tiers
 - Profiles
- Defines a common language for managing risk
 - Core has five functions that provide a high-level, strategic view of security lifecycle

HELPS ORGANIZATIONS ASK:



What are we doing today ?



How are we doing today ?



Where do we want to go ?






When do we want to go there ?

FRAMEWORK CATEGORIES

Function	Category
Identify 	Asset Management Business Environment Governance Risk Assessment Risk Management Strategy Supply Chain Risk Management
Protect 	Identify management, Authentication and Access Control Awareness Training Data Security Information Protection Processes and Procedures Maintenance Protective Technology

FRAMEWORK CATEGORIES

Function	Category
Detect 	Anomalies and events Security continuous monitoring Detection Processes
Respond 	Response Planning Communications Analysis Mitigation Improvements
Recover 	Recover Planning Improvements Communications

Thank You