NIST Cybersecurity Framework (CSF) Summary

The NIST Cybersecurity Framework (CSF) is a voluntary set of standards, best practices, and guidelines developed to help organizations manage cybersecurity risks. Initially created in 2014 to protect U.S. critical infrastructure, the CSF has evolved into a flexible framework applicable across all industries--including small businesses and large enterprises.

Framework Components

1. Core

The CSF core outlines desired cybersecurity outcomes across six key functions:

- Identify: Understand and manage cybersecurity risks to systems and assets.
- Protect: Implement safeguards to ensure delivery of critical services.
- Detect: Enable timely discovery of cybersecurity events.
- Respond: Take appropriate actions regarding a detected cybersecurity event.
- Recover: Restore capabilities or services affected by cybersecurity incidents.
- Govern (added in 2024): Emphasizes leadership, accountability, and decision-making in cybersecurity risk management.

2. Tiers

The CSF tiers assess an organization's cybersecurity maturity on a scale from Tier 1 (Partial) to Tier 4 (Adaptive). They help organizations understand the sophistication of their practices and identify opportunities for improvement.

3. Profiles

CSF profiles are tailored templates developed by industry experts. They help organizations benchmark their current state against desired outcomes and create a roadmap to enhance their cybersecurity posture.

Implementation Strategy

According to guidance from CISA (Cybersecurity and Infrastructure Security Agency), organizations should follow these steps when implementing the CSF:

1. Create a current profile: Evaluate existing security operations and business needs.
2. Perform a risk assessment: Identify gaps and determine alignment with business goals and regulations.
3. Analyze and prioritize: Focus on areas that pose the greatest risk.
4. Develop and implement an action plan: Address gaps and align with objectives.

Key Benefits

- Applicable to any industry
- Supports compliance with regulatory requirements
- Aligns with industry best practices
- Improves visibility into cybersecurity maturity
- Helps manage financial and reputational risk