# CTRL THE FUTURE LLC

## NIST CYBERSECURITY FRAMEWORK 2.0

## EXECUTIVE OVERVIEW

**A practical introduction to organizing cybersecurity governance and risk-management outcomes**

**What is CSF 2.0?** The NIST Cybersecurity Framework (CSF) 2.0 provides a flexible structure for helping organizations understand, assess, prioritize, and communicate cybersecurity risk. Its Core organizes high-level cybersecurity outcomes into six Functions: GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER. The framework can be used by organizations of any size, sector, or maturity level.

## Why Organizations Use the CSF

CSF 2.0 can help leadership and practitioners establish a common language for cybersecurity risk, understand current practices, define desired outcomes, prioritize improvements, communicate with internal and external stakeholders, and connect cybersecurity activities with broader enterprise risk management.

CSF 2.0 is outcome-oriented rather than a prescriptive implementation checklist. Organizations determine how to achieve relevant outcomes based on their mission, risk environment, resources, legal and contractual obligations, technologies, and business needs.

## The Six CSF 2.0 Functions

| FUNCTION | PRACTICAL PURPOSE |
|---|---|
| GOVERN | Establish and monitor cybersecurity risk-management strategy, expectations, policy, roles, responsibilities, authorities, and oversight. |
| IDENTIFY | Understand the organization's current cybersecurity risks, including assets, suppliers, vulnerabilities, threats, and opportunities for improvement. |
| PROTECT | Use safeguards to manage cybersecurity risks, including identity and access, awareness and training, data security, platform security, and infrastructure resilience. |
| DETECT | Find and analyze possible cybersecurity attacks and compromises through monitoring and adverse-event analysis. |
| RESPOND | Take action regarding detected cybersecurity incidents through incident management, analysis, reporting and communication, and mitigation. |
| RECOVER | Restore assets and operations affected by cybersecurity incidents and communicate recovery activities. |

## Understanding the CSF Core

The CSF Core is organized hierarchically. Functions provide the broadest view. Each Function contains Categories, which group related cybersecurity outcomes. Categories contain Subcategories that describe more specific technical and management outcomes. Informative References can help connect CSF outcomes to other standards, guidelines, regulations, and practices.

| LEVEL | WHAT IT DOES | EXAMPLE |
|---|---|---|
| Function | Organizes cybersecurity outcomes at the highest level. | GOVERN |
| Category | Groups related outcomes within a Function. | Risk Management Strategy |
| Subcategory | Expresses a more specific cybersecurity outcome. | A particular risk-management outcome |
| Informative References | Maps outcomes to external standards and guidance. | Cross-references to relevant resources |

## Profiles: Current State and Target State

**CSF Organizational Profiles** can be used to describe an organization's current and target cybersecurity posture in terms of selected CSF outcomes. Comparing a Current Profile with a Target Profile can help identify gaps and prioritize improvement activities.

A practical approach is to document which outcomes are currently achieved, which are partially achieved, which are priorities for the future, and what actions, owners, resources, and timelines are needed to close important gaps.

## CSF Tiers

CSF Tiers characterize the rigor of an organization's cybersecurity risk governance and management practices. The four Tiers are **Tier 1: Partial**, **Tier 2: Risk Informed**, **Tier 3: Repeatable**, and **Tier 4: Adaptive**. Tiers provide context for how an organization views and manages cybersecurity risk; they should not be treated as simple compliance grades.

## A Practical CSF 2.0 Adoption Path

| | | |
|---|---|---|
| **01** | **Establish Context** | Identify mission, stakeholders, obligations, risk appetite/tolerance, and the scope of the cybersecurity effort. |
| **02** | **Understand Current State** | Review relevant assets, risks, practices, dependencies, and existing CSF outcomes. |
| **03** | **Define Target Outcomes** | Determine which CSF outcomes are important for the organization's desired cybersecurity posture. |
| **04** | **Analyze Gaps** | Compare current and target outcomes and identify gaps, risks, dependencies, and resource needs. |
| **05** | **Prioritize Actions** | Create a risk-informed improvement plan with accountable owners, resources, and target dates. |
| **06** | **Monitor & Improve** | Measure progress, reassess risk, update Profiles, and adapt as the organization and threat environment change. |

## Questions Leadership Can Ask

• How is cybersecurity risk incorporated into enterprise risk-management and business decisions?

• Who is accountable for cybersecurity risk, policy, oversight, and reporting?

• Which assets, services, data, suppliers, and dependencies are most important to organizational objectives?

• Which safeguards reduce the organization's most significant cybersecurity risks?

• How will the organization detect, respond to, and recover from cybersecurity incidents?

• What cybersecurity outcomes should be prioritized over the next 6–12 months?

• How is progress measured and communicated to leadership?

## Using CSF 2.0 With Other Requirements

The CSF can complement regulatory, contractual, sector-specific, and organizational requirements. It does not replace obligations that apply to an organization. Instead, organizations can use the CSF to organize cybersecurity outcomes and connect them with relevant policies, controls, standards, assessments, and improvement activities.

## Recommended Next Steps

**1.** Select a manageable scope such as a business service, system environment, location, or organizational unit.

**2.** Build a Current Profile using relevant CSF outcomes and available evidence.

**3.** Establish a Target Profile based on mission needs, risk, obligations, and business priorities.

**4.** Identify and prioritize gaps based on risk rather than attempting to implement every outcome equally.

**5.** Assign owners, timelines, resources, and measures for priority improvements.

**6.** Revisit the Profile as business conditions, technology, suppliers, threats, and organizational priorities change.

**Ready to put CSF 2.0 into practice?**
**CTRL The Future LLC can help organizations evaluate current cybersecurity practices, develop CSF Profiles, identify governance and control gaps, establish a risk-informed improvement roadmap, and strengthen ongoing cybersecurity oversight.**

**Framework note:** This overview is based on the NIST Cybersecurity Framework (CSF) 2.0 structure and terminology. Organizations should consult NIST's official CSF 2.0 publication and related resources when implementing the framework.

**Disclaimer:** This resource is provided for general informational and educational purposes. It is not a certification, formal audit, legal advice, or determination of cybersecurity compliance or security effectiveness.