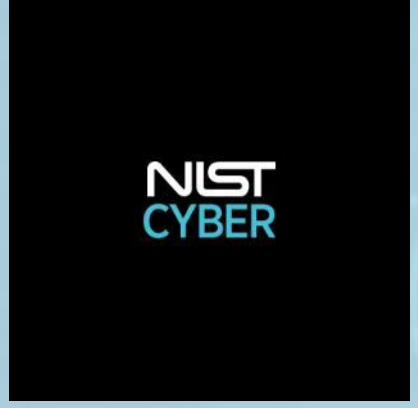



# The Cybersecurity Framework Version 1.1

October 2019

# Cybersecurity Framework History

- February 2013 - Executive Order 13636: *Improving Critical Infrastructure Cybersecurity*

- December 2014 - *Cybersecurity Enhancement Act of 2014 (P.L. 113-274)*

- May 2017 - Executive Order 13800: *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

# The Cybersecurity Framework

*Three Primary Components*

## Core

Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls

## Profiles

Alignment of an organization's requirements and objectives, risk appetite and resources ***using*** the desired outcomes of the Framework Core

## Implementation Tiers

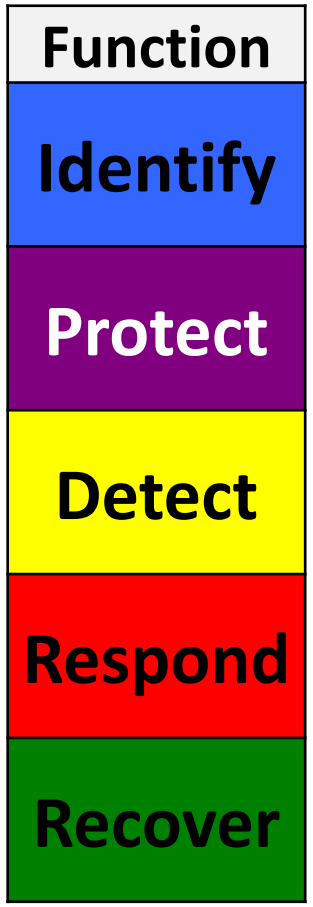
A qualitative measure of organizational cybersecurity risk management practices

# Key Framework Attributes

*Principles of Current and Future Versions of the Framework*

# The Framework Core

*Establishes a Common Language*




- Describes desired outcomes
- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

# An Excerpt from the Framework Core

*The Connected Path of Framework Outcomes*

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| PROTECT (PR) | **Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. | **PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions | **CIS CSC**, 16<br>**COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03<br>**ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4<br>**ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1<br>**ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1<br>**NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3 |
| | | **PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) | **CIS CSC** 1, 12, 15, 16<br>**COBIT 5** DSS05.04, DSS05.10, DSS06.10<br>**ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9<br>**ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10<br>**ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4<br>**NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 |

5 Functions 23 Categories 108 Subcategories 6 Informative References

# Implementation Tiers

*The Cybersecurity Framework Version 1.1*

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| | **Partial** | **Risk Informed** | **Repeatable** | **Adaptive** |
| **Risk Management Process** | The functionality and repeatability of cybersecurity risk management | | | |
| **Integrated Risk Management Program** | The extent to which cybersecurity is considered in broader risk management decisions | | | |
| **External Participation** | The degree to which the organization:<br>• **monitors and manages supply chain risk**[1.1]<br>• benefits my sharing or receiving information from outside parties | | | |
| | | | | |

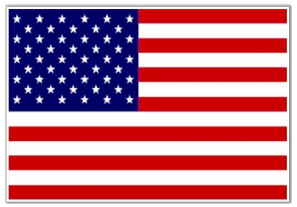
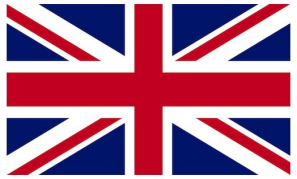
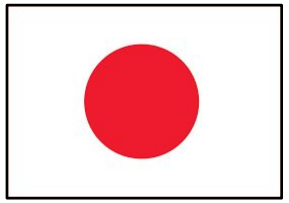
# Framework Update

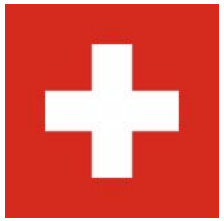
*The Cybersecurity Framework Version 1.1*

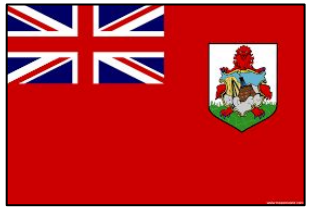
- Applicability for all system lifecycle phases
- Enhanced guidance for managing cybersecurity within supply chains and for buying decisions
- New guidance for self-assessment
- Better accounts for Authorization, Authentication, and Identity Proofing
- Incorporates emerging vulnerability information (a.k.a., Coordinated Vulnerability Disclosure)
- Administratively updates the Informative References

# International Use

*Translations, Adaptations, and Other References World-Wide*





# Sample Resources

*www.nist.gov/cyberframework/framework-resources*

**Manufacturing Profile**

*NIST Discrete Manufacturing Cybersecurity Framework Profile*

**Financial Services Profile**

*Financial Services Sector Specific Cybersecurity "Profile"*

**Maritime Profile**

*Bulk Liquid Transport Profile*

# Success Stories

*https://www.nist.gov/cyberframework/success-stories*

University of Chicago Biological Sciences Division

Japan's Cross-Sector Forum

ISACA

University of Pittsburgh

University of Kansas Medical Center

Multi-State Information Sharing & Analysis Center

# STAYING IN TOUCH

NIST.gov/cyberframework

cyberframework@nist.gov

CSRC.NIST.gov

NCCoE.NIST.gov

NIST.gov/topics/cybersecurity

@NISTcyber