Three's Company: Unpacking and Settling in with Three NIST Frameworks

Dave Weitzel

Policy and Standards Principal

Julie Snyder

Principal Cybersecurity and Privacy Engineer/National Cybersecurity FFRDC Privacy Lead

Christina Sames

Principal Cybersecurity Engineer

October 26, 2022

**The authors' affiliation with MITRE is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the authors.*

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. CASE NUMBER 21-1450

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

About Us

- MITRE operates federally funded R&D centers (FFRDCs). FFRDCs are unique organizations that assist the United States government with scientific research and analysis; development and acquisition; and systems engineering and integration.
- As a not-for-profit organization, MITRE works in the public interest across federal, state and local governments, as well as industry and academia to tackle challenges to the safety, stability, and well-being of our nation.

Source: MITRE, Corporate Overview | The MITRE Corporation

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Agenda

- Foundational Overview of Three NIST Frameworks
  - Cybersecurity Framework
  - Privacy Framework
  - Risk Management Framework
- Setting Up Framework Profiles
- Assembling Security and Privacy Controls
- Bringing Together the Frameworks

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

CliffsNotes©

- Work is underway to clarify how the NIST Cybersecurity Framework, Privacy Framework, and Risk Management Framework (RMF) should be used together
  - Complement each other
  - Distinct benefits
  - Collective power

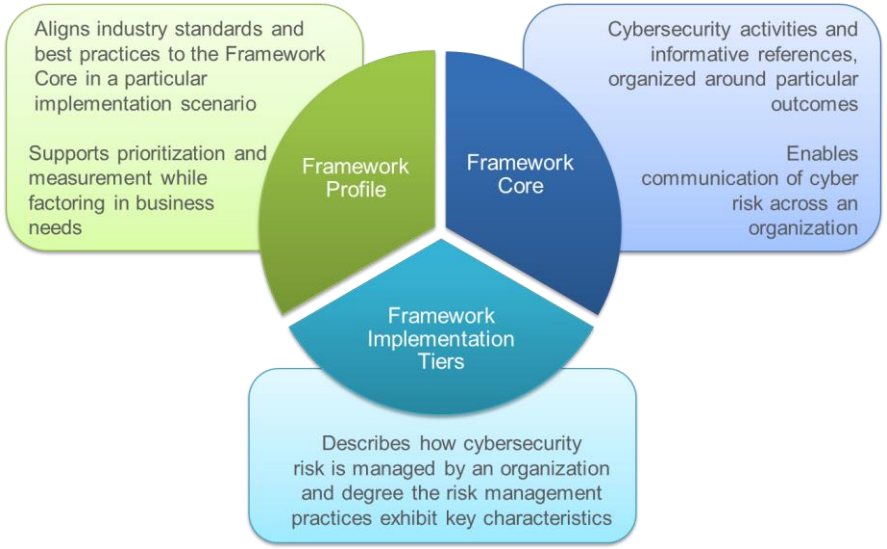
© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Foundational Overview of Three NIST Frameworks

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

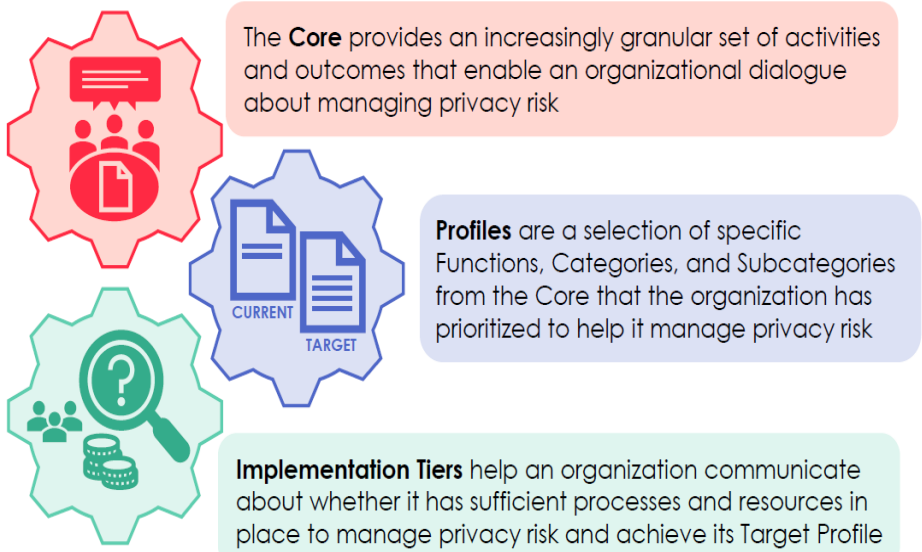
Overview of the Three NIST Frameworks

Cybersecurity Framework



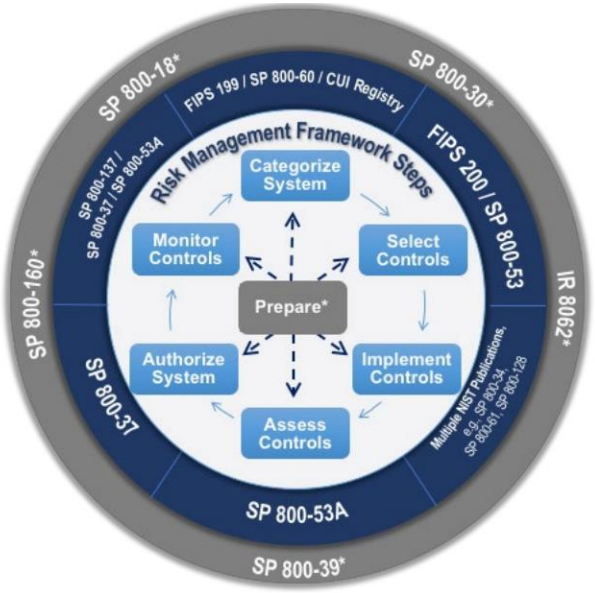
Source: *The Framework for Improving Critical Infrastructure Cybersecurity, April 2018, https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview*

Privacy Framework



Source: NIST Privacy Framework website, New to Framework | NIST

Risk Management Framework



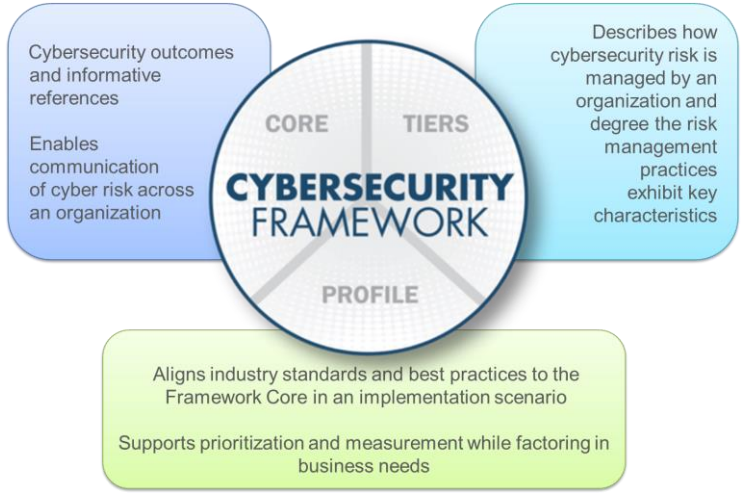
Source: NIST RMF Webcast: A Flexibility Methodology to Manage Information Security and Privacy Risk, February 2019, NIST RMF Webcast: A Flexible Methodology to Manage Information Security and Privacy Risk | CSRC

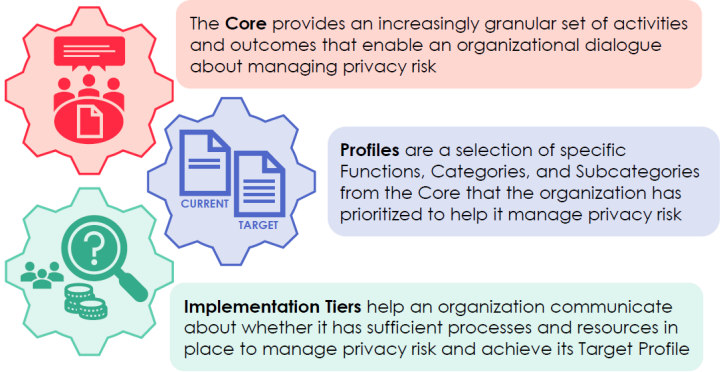
MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Cybersecurity and Privacy Framework Components

- **Core:**
  Increasingly granular set of activities and outcomes that enable an organization dialogue about managing risk
  - **Informative References:**
    Optional resources to support implementation of the Core (e.g., technical guidance, standards)
- **Profiles:**
  Prioritized subset of the Core that addresses risk in alignment with organizational objectives
- **Implementation Tiers:**
  Helps an organization determine whether it has sufficient risk management practices and resources in place to achieve its Target Profile(s)



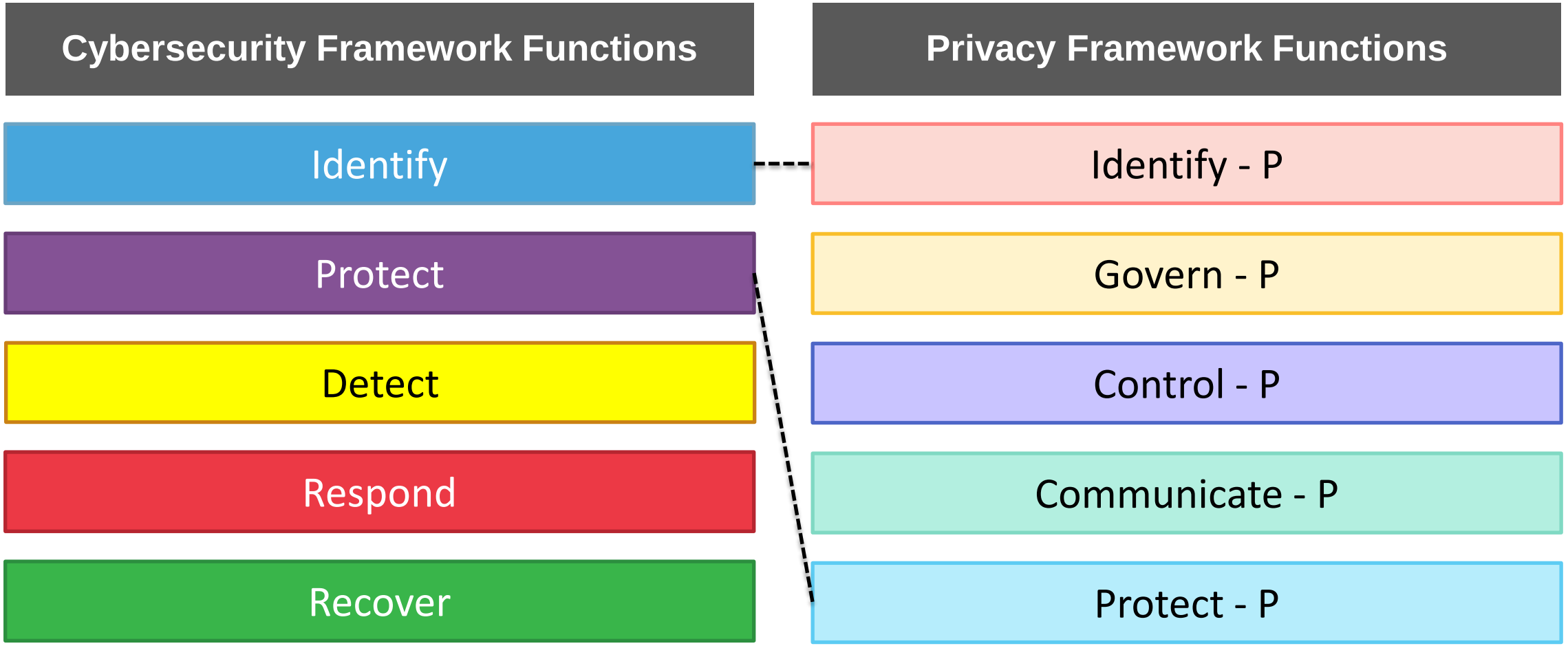


Sources (adapted): *The Framework for Improving Critical Infrastructure Cybersecurity, April 2018, https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview, The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, https://doi.org/10.6028/NIST.CSWP.01162020 , Version 1.0 (January 2020)*

MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Cybersecurity and Privacy Framework Cores

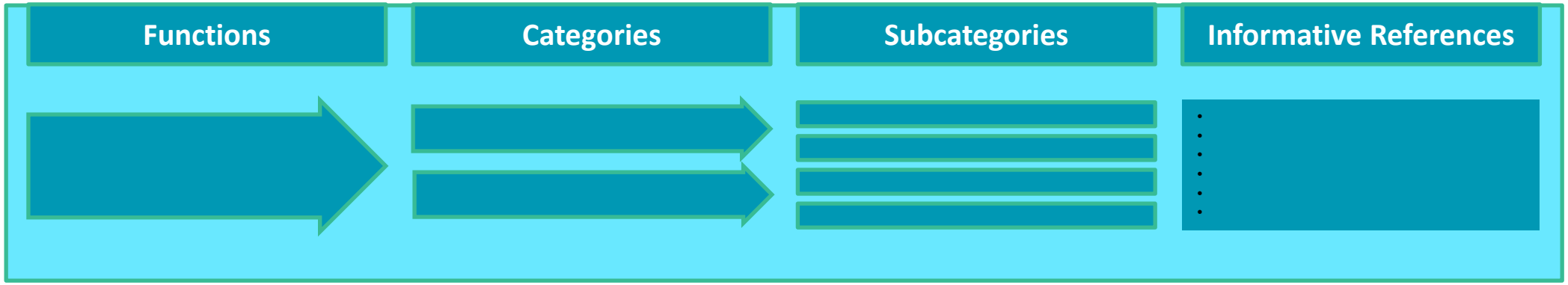


Sources (adapted): *The Framework for Improving Critical Infrastructure Cybersecurity, April 2018, https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview, The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, https://doi.org/10.6028/NIST.CSWP.01162020 , Version 1.0 (January 2020)*

MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Cybersecurity and Privacy Framework Cores



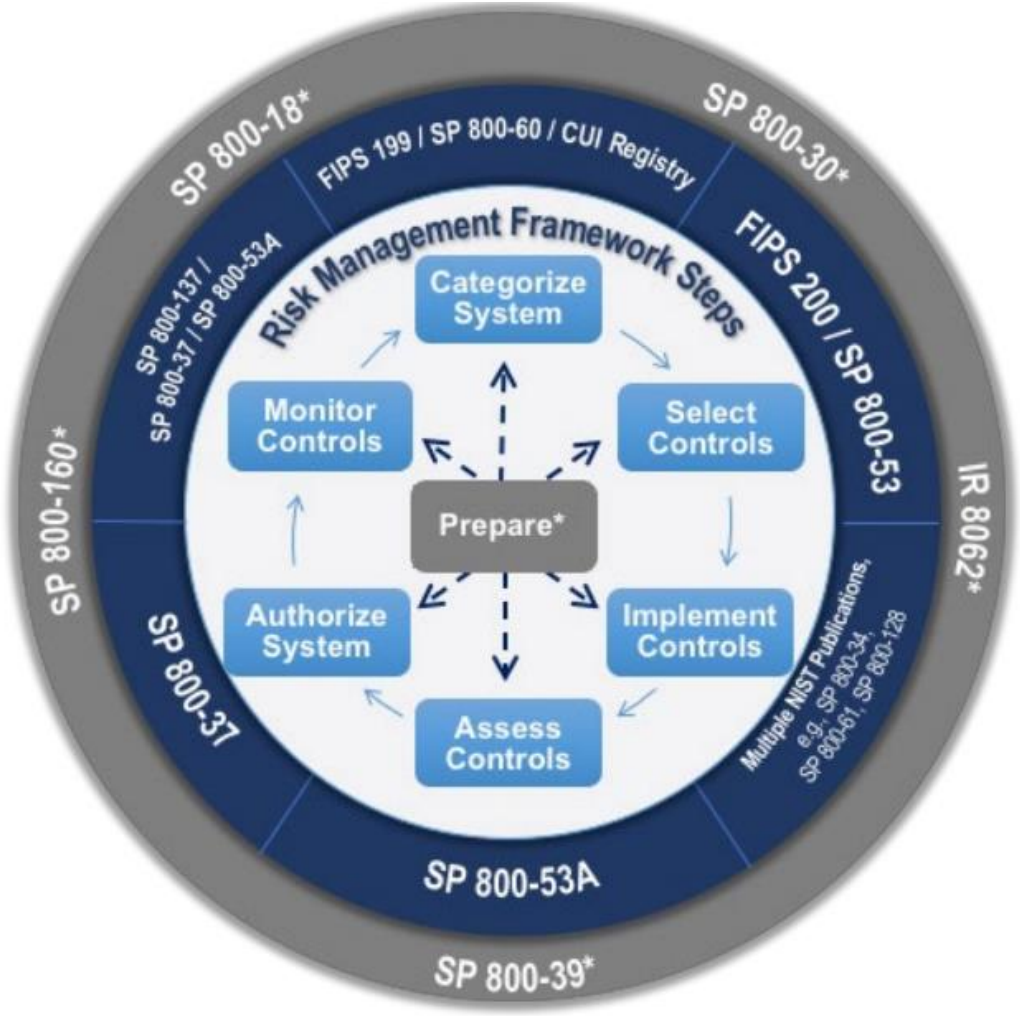
	Function	Category	Subcategory	Informative References
Cybersecurity Framework	**IDENTIFY**	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	• COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 • ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7 • ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3 • NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM-9
Privacy Framework	**IDENTIFY-P**	**Business Environment (ID.BE-P):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.	**ID.BE-P1:** The organization's role(s) in the data processing ecosystem are identified and communicated.	• NIST SP 800-37 Rev. 2: Section 2.8 Supply Chain Risk Management, Task P-9 • NIST SP 800-53 Rev. 5 (IPD): CP-2, SA-12 • NIST SP 800-161 • NISTIR 7622

Sources (adapted): *The Framework for Improving Critical Infrastructure Cybersecurity, April 2018, https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview, The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, https://doi.org/10.6028/NIST.CSWP.01162020, Version 1.0 (January 2020)*

MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Risk Management Framework (RMF)

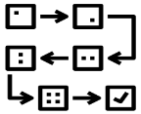


Source: NIST RMF Webcast: A Flexibility Methodology to Manage Information Security and Privacy Risk, February 2019, NIST RMF Webcast: A Flexible Methodology to Manage Information Security and Privacy Risk | CSRC

MITRE

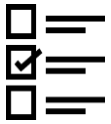
© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

RMF Steps

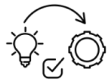


Prepare to execute the RMF from an organization- and system-level perspective by establishing a context and priorities for managing security and privacy risks.

Categorize the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.



Select an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk



Implement the controls and describe how the controls are employed within the system and its environment of operation

Assess the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements

Authorize the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.

Monitor the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system

Source: NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 2018, SP 800-37 Rev. 2, RMF: A System Life Cycle Approach for Security and Privacy | CSRC (nist.gov)

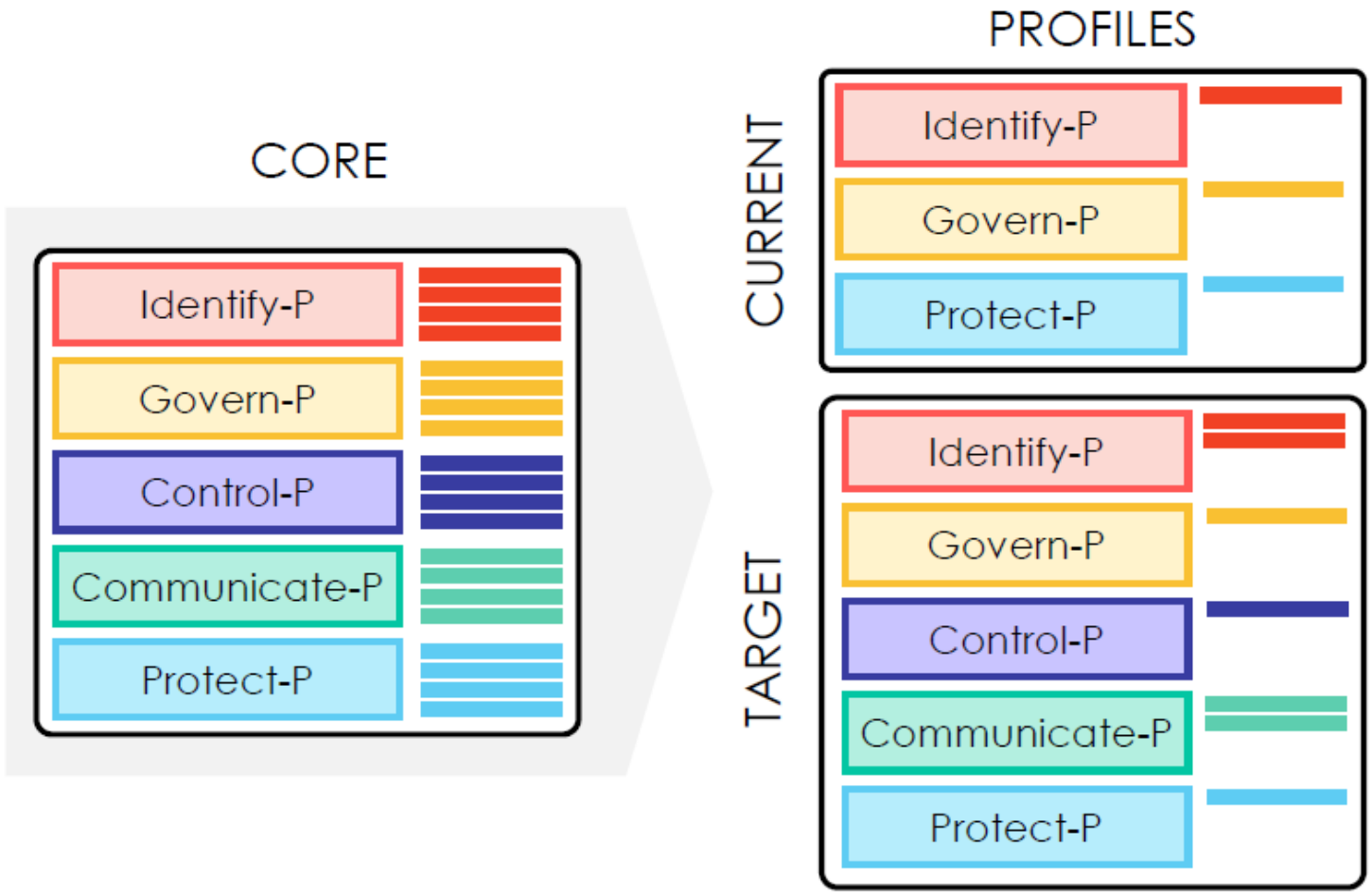
MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Setting up Framework Profiles

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

What is a Framework Profile?



Consider:

- Organizational goals
- Role(s) in the data processing ecosystem or industry sector
- Legal/regulatory requirements & industry best practices
- Organization's risk management priorities
- Privacy needs of individuals

Reference: *NIST Privacy Framework Webinar: Ready. Set. Adopt Version 1.0, January 29, 2020*

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Understanding How to Draft Mission Objectives: Terminology

Business/Mission Objective

The fundamental purposes and operations of an industry/subsector or organization that the processes and systems support.

Mission Priority

The relative importance of one item versus another

Mission Dependency

A requirement to fulfill Mission or a Mission Objective that lives outside of the subsector

Source (adapted): NIST

MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

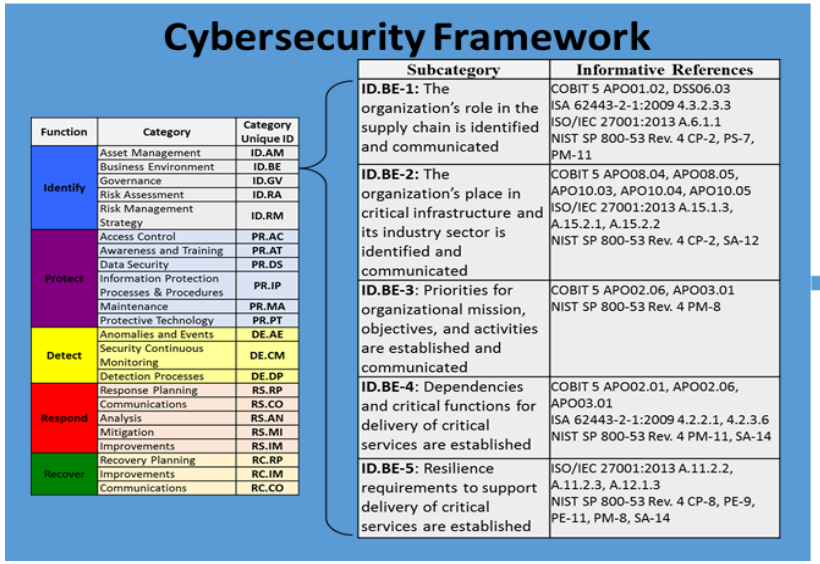
Example: Maritime Bulk Liquids Transfer (MBLT) Profile

Source: *USCG Maritime Bulk Liquids Transfer Profile, http://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/*

MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

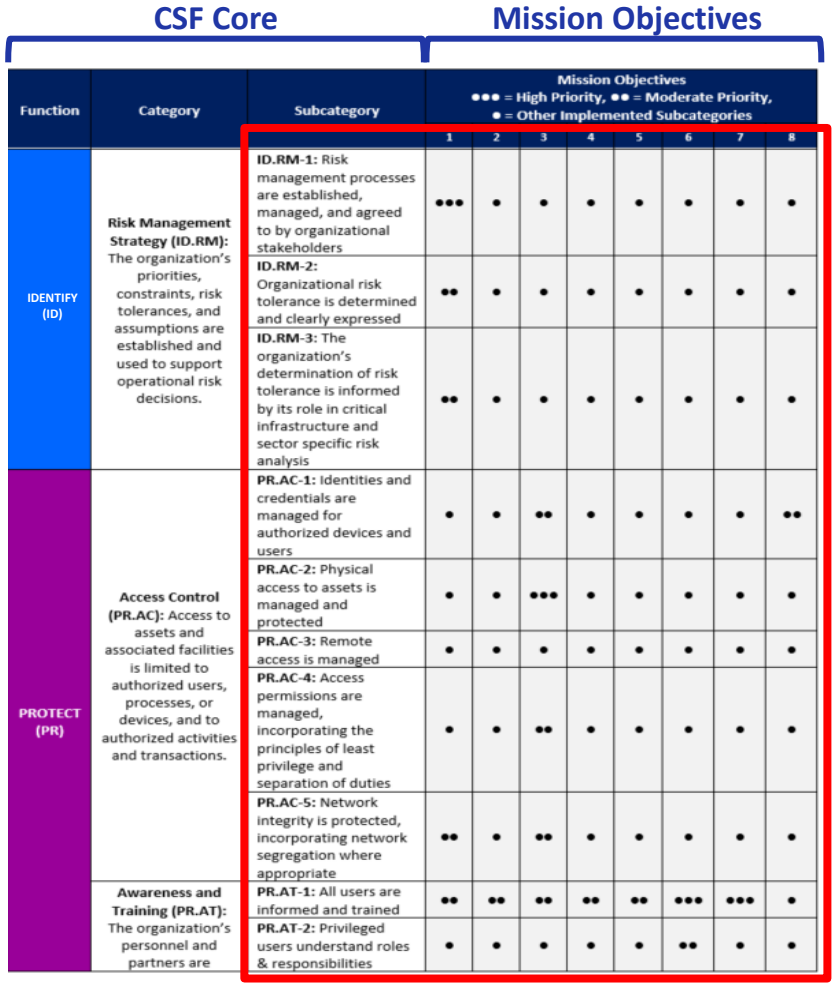
Example: MBLT Profile



Source: *USCG Maritime Bulk Liquids Transfer Profile,* http://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/

MITRE
© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Understanding the Dot Chart



CSF Core | Mission Objectives

Function	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Implemented Subcategories							
			1	2	3	4	5	6	7	8
IDENTIFY (ID)	**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	●●●	●	●	●	●	●	●	●
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	●●	●	●	●	●	●	●	●
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	●●	●	●	●	●	●	●	●
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	●	●	●●	●	●	●	●	●●
		PR.AC-2: Physical access to assets is managed and protected	●	●	●●●	●	●	●	●	●
		PR.AC-3: Remote access is managed	●	●	●	●	●	●	●	●
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	●	●	●●	●	●	●	●	●
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	●●	●	●●	●	●	●	●	●
	Awareness and Training (PR.AT): The organization's personnel and partners are	**PR.AT-1:** All users are informed and trained	●●	●●	●●	●●	●●	●●●	●●●	●
		PR.AT-2: Privileged users understand roles & responsibilities	●	●	●	●	●	●●	●	●

- Mission/business contexts will inform priority Categories and Subcategories
  - Suggests areas of focus for cybersecurity needs or requirements
  - Provides crosswalk among programs to demonstrate their capabilities
- Levels are:
  - ●●● = High Priority
  - ●● = Moderate Priority
  - ● = Other Implemented Subcategories
  - ✕ = Subcategories to NOT Implement
- Intent is to strive to conduct activities in support of all relevant Categories and Subcategories
- Use the Profile's flexibility to determine how and in what order to address High and Moderate Priority Categories and Subcategories
- Implementation details may differ but priority cybersecurity activities and outcomes will be consistent

Source: *USCG Maritime Bulk Liquids Transfer Profile,* http://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/

MITRE

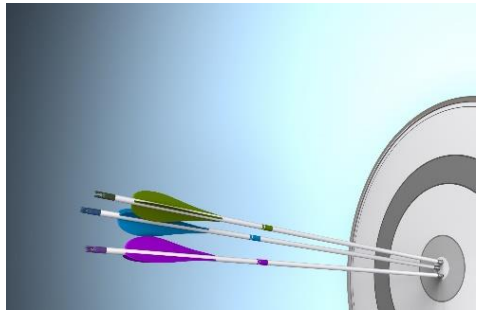
© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Ways to Use a Profile

Customization of the Core for a given sector, subsector, or organization

Fusion of business/mission logic and cybersecurity outcomes

Alignment of cybersecurity requirements with operational methodologies



Basis for **assessment** and expressing **target state**

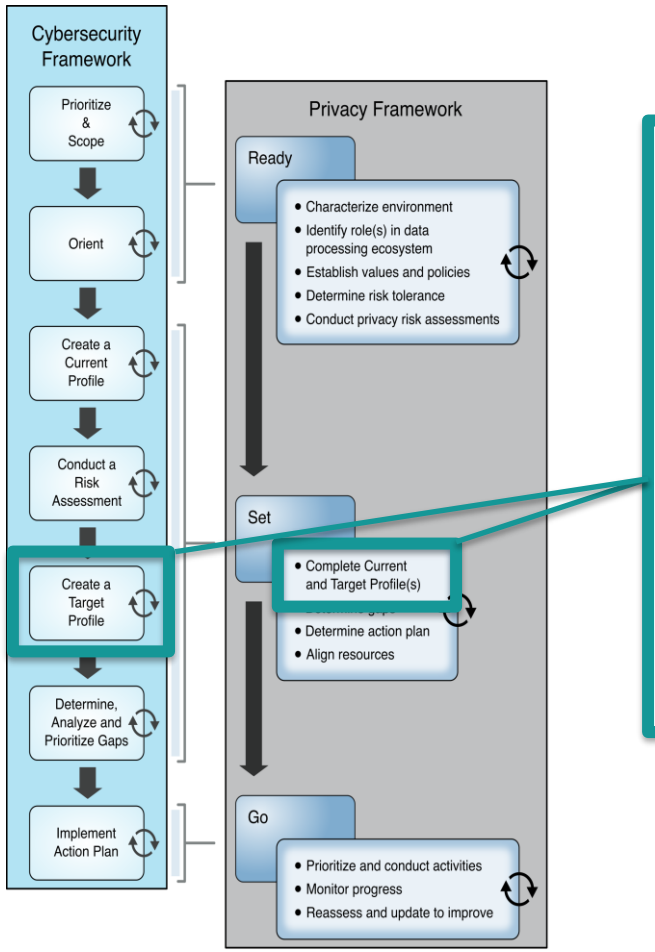
Decision support tool for cybersecurity risk management

Source (adapted): *The Framework for Improving Critical Infrastructure Cybersecurity, April 2018,* https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview

MITRE

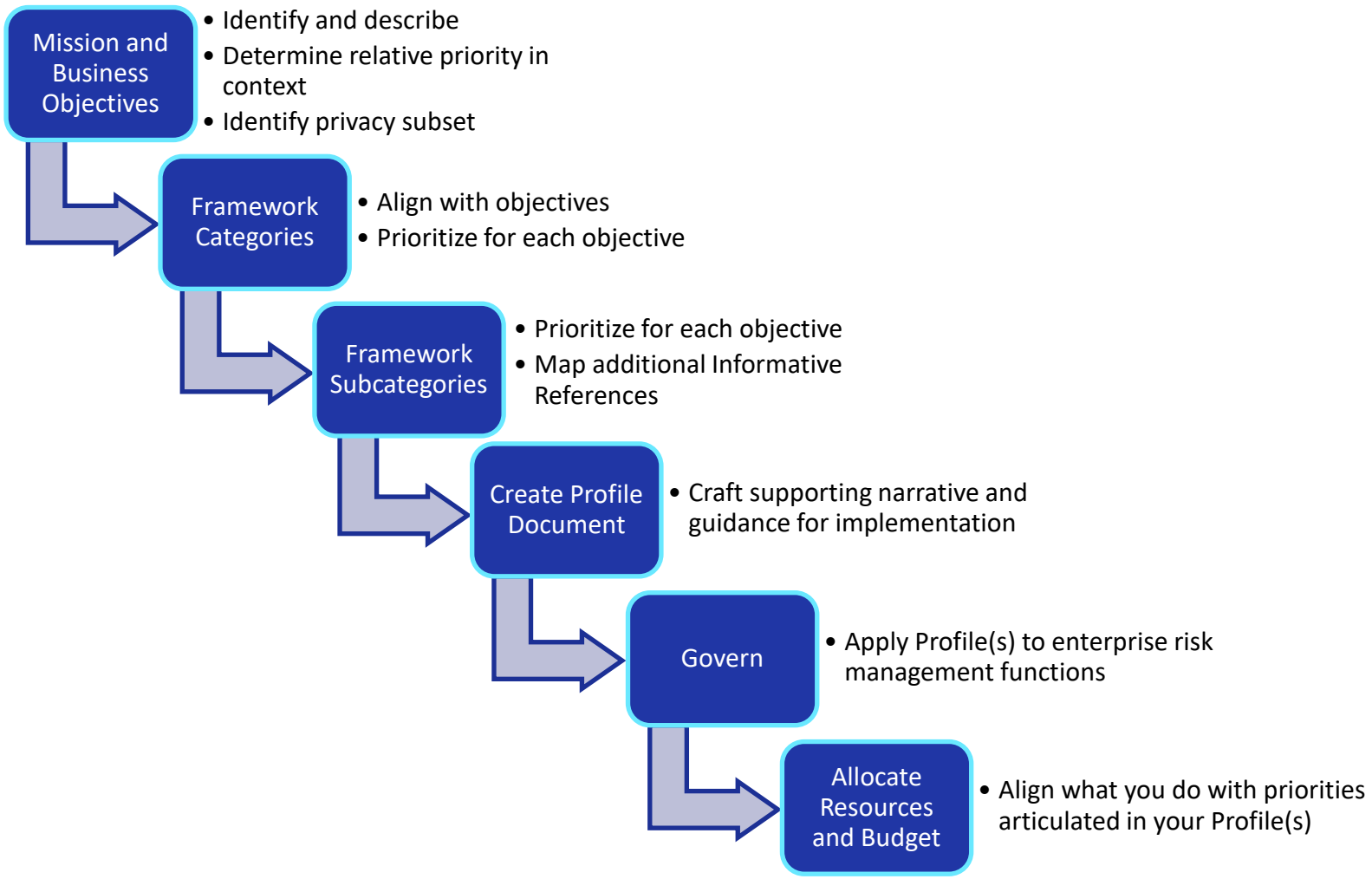
© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Framework Profile Development Process



© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Profile Development Approach



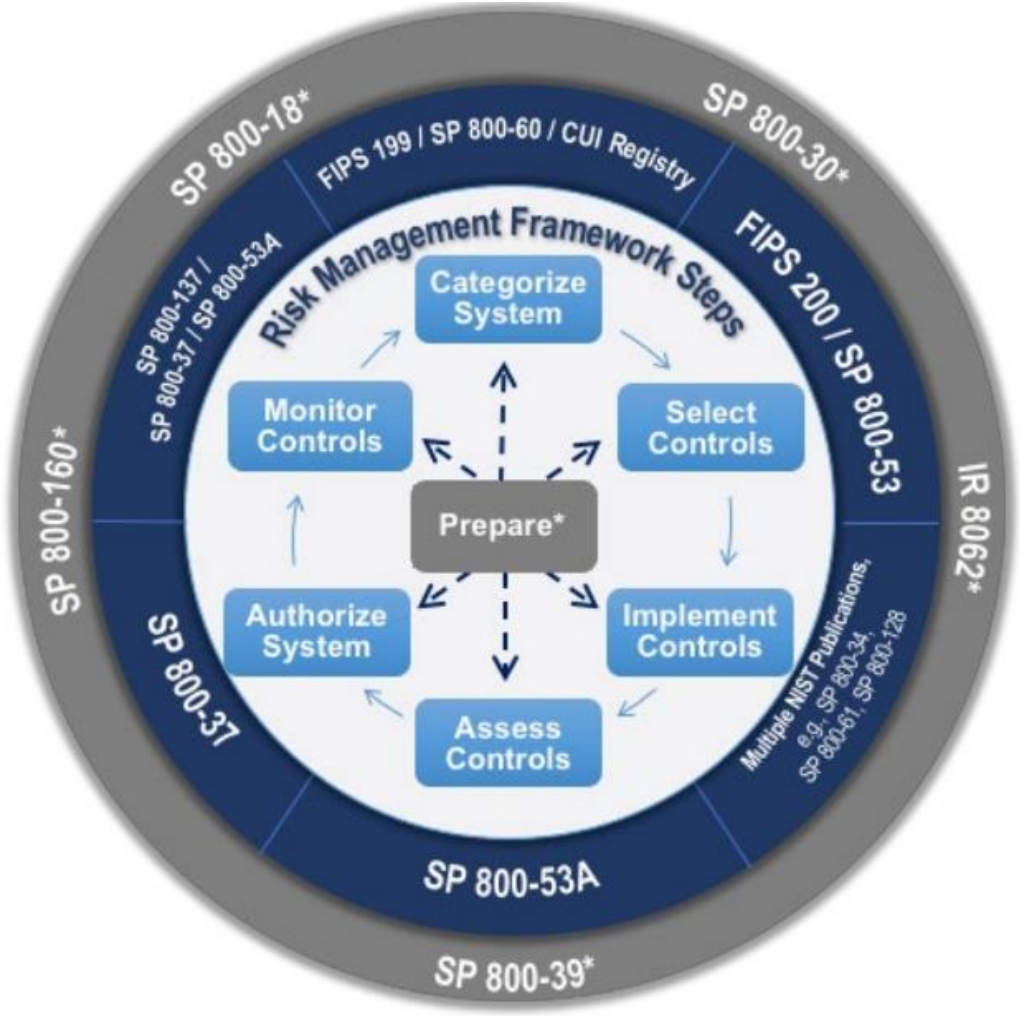
MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Assembling Security and Privacy

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

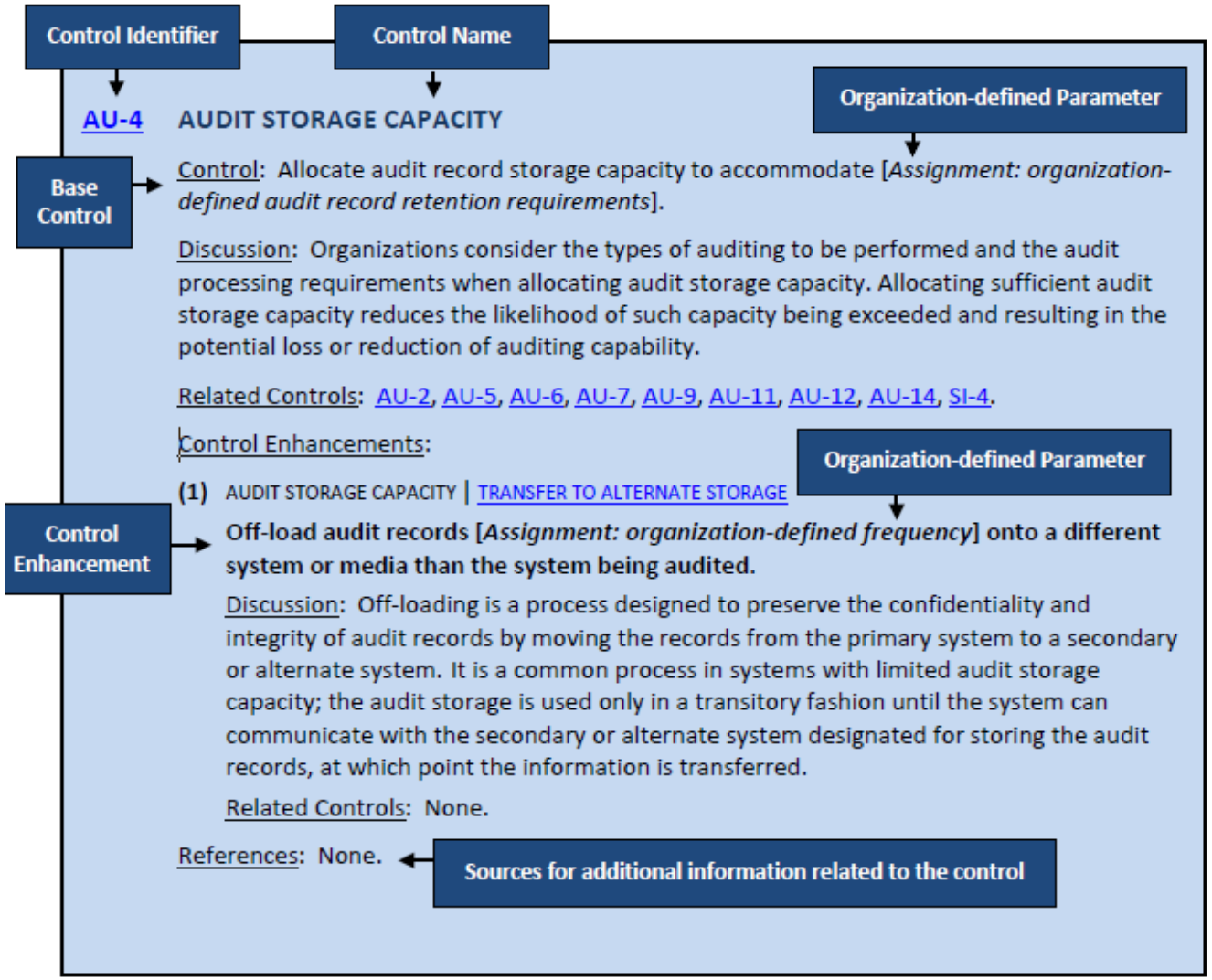
Risk Management Framework (RMF)



Source: NIST RMF Webcast: A Flexibility Methodology to Manage Information Security and Privacy Risk, February 2019, NIST RMF Webcast: A Flexible Methodology to Manage Information Security and Privacy Risk | CSRC

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

NIST Controls: Example



Source: Figure 1: Control Structure, NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020 (with December 2020 errata updates)

MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

NIST Baselines: Example

TABLE 3-2: AWARENESS AND TRAINING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AT-1	**Policy and Procedures**	x	x	x	x
AT-2	**Literacy Training and Awareness**	x	x	x	x
AT-2(1)	PRACTICAL EXERCISES				
AT-2(2)	INSIDER THREAT		x	x	x
AT-2(3)	SOCIAL ENGINEERING AND MINING			x	x
AT-2(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR				
AT-2(5)	ADVANCED PERSISTENT THREAT				
AT-2(6)	CYBER THREAT ENVIRONMENT				
AT-3	**Role-Based Training**	x	x	x	x
AT-3(1)	ENVIRONMENTAL CONTROLS				
AT-3(2)	PHYSICAL SECURITY CONTROLS				
AT-3(3)	PRACTICAL EXERCISES				
AT-3(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR	W: Incorporated into AT-2(4).			
AT-3(5)	ACCESSING PERSONALLY IDENTIFIABLE INFORMATION	x			
AT-4	**Training Records**	x	x	x	x
AT-5	Contacts with Security Groups and Associations	W: Incorporated into PM-15.			
AT-6	**Training Feedback**				

Source: NIST Special Publication 800-53B, *Control Baselines for Information Systems and Organizations*, October 2020 (with December 2020 errata updates)

MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Overlays: Example

An overlay provides the following for each control it contains:

- Justification for inclusion in overlay
- Applicable control specifications:
  - Selection indicator (+, --, or blank with other specifications)
  - Guidance (G)
  - Parameter Value (V)
  - Control Extensions (E)
  - Reference to the applicable requirement(s) (R)
- Table 3 provides an example summary of all four Privacy Overlays

Table 3: Privacy Overlays Security and Privacy Controls

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
	LOW	MODERATE	HIGH	PHI
AC-1	+GR	+GR	+GR	+ER
AC-2	+EGVR	+EGVR	+EGVR	+EGR
AC-2(8)		--R	--R	
AC-2(9)	GVR	GVR	GVR	R
AC-2(13)	+R	+R	+R	+R
AC-3	+EGR	+EGR	+EGR	+GR
AC-3(9)		+EVR	+EVR	+R
AC-3(10)	GVR	GVR	GVR	
AC-4		+GR	+GR	+R
AC-4(8)			+VR	
AC-4(12)				+GR
AC-4(15)		+GR	+GR	+R
AC-4(17)		+GVR	+GVR	
AC-4(18)		+GR	+GR	+R
AC-5		+GR	+GR	+GR

Source: CNSSI No. 1253, *Security Categorization and Control Selection for National Security Systems*, Appendix F, Privacy Overlays, April 2015.

MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

How Framework Profiles May Influence the RMF Steps

RMF Step	Examples of How Profiles May Influence RMF Decisions
Prepare (SP 800-37, Rev2)	• Shapes planning tasks related to all other RMF steps • Profile development process facilitates communication and alignment within the organization
Categorize	• Understanding of relative importance and correlation of security objectives (Confidentiality, Integrity, Availability) to mission/business objectives
Select	• Prioritization input for baseline selection, overlay selection/implementation, and system-specific tailoring decisions • Appropriateness of risk acceptance and what can be addressed later through a Plan of Action and Milestones (POA&M)
Implement	• Inform risk-based trades during systems acquisition, development, design, and engineering • Techniques used (e.g., automated tools vs. policies and procedures)
Assess	• Rigor of assessment techniques for controls supporting higher priority Subcategories, Categories, and Functions
Authorize	• Set and convey risk tolerance based on mission/business priorities • Understanding and acceptance of risk posture in terms of mission/business objectives and priorities
Monitor	• Drives criticality of controls (in the continuous monitoring strategy) supporting priority Subcategories, Categories, and Functions • Drives frequency, method, reporting, and tracking of controls

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

How the Cybersecurity and Privacy Frameworks can help RMF activities

- Provide closer linkage and communication between leadership's risk management processes and activities and those at the system level
- Profiles can provide a link between cybersecurity and privacy activities and organizational mission/business objectives
  - Supports risk-based decision-making throughout the RMF
  - While Profiles may be used as a starting point to inform control selection and tailoring activities, further evaluation is needed to ensure the appropriate controls are selected.
- Identify, align, and deconflict requirements
  - And to subsequently inform the selection of controls for an organization.

Source (Adapted): NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 2018, SP 800-37 Rev. 2, RMF: A System Life Cycle Approach for Security and Privacy | CSRC (nist.gov)

MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Bringing Together the Frameworks

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Worked Example: RMF Categorize and Select Results

Example of a CNSSI No. 1253 baseline - “only” 450 controls to prioritize….

	C	I	A
ID	L	H	M
AC-1	X	X	X
AC-2	X	X	
AC-2(1)		X	
AC-2(2)		X	
AC-2(3)		X	
AC-2(4)	+	X	
AC-2(5)	+	X	+
AC-2(7)	+	+	
AC-2(9)	+	+	
AC-2(10)	+	+	
AC-2(11)		X	
AC-2(12)	+	X	
AC-2(13)	+	X	
AC-3	X	X	
AC-3(4)	+	+	
AC-4		X	
AC-5	+	X	
AC-6	+	X	
AC-6(1)	+	X	
AC-6(2)	+	X	
AC-6(3)		X	
AC-6(5)	+	X	
AC-6(7)	+	+	
AC-6(8)	+	+	
AC-6(9)	+	X	
AC-6(10)	+	X	
AC-7	X	X	X
AC-8	X	X	
AC-10		X	+
AC-11	+	X	
AC-11(1)	+		
AC-12		X	
AC-12(1)		+	
AC-14	X	X	
AC-16		+	
AC-16(6)		+	
AC-17	X	X	
AC-17(1)	+	X	
AC-17(2)	+	X	
AC-17(3)	+	X	
AC-17(4)	+	X	
AC-17(6)	+		
AC-17(9)	+	+	
AC-18	X	X	
AC-18(1)	+	X	

	C	I	A
ID	L	H	M
AC-18(3)	+	+	
AC-18(4)	+	X	
AC-18(5)		X	
AC-19	X	X	
AC-19(5)		X	
AC-20	X	X	
AC-20(1)	+	X	
AC-20(2)	+		
AC-20(3)	+	+	
AC-22	X		
AT-1	X	X	X
AT-2	X	X	X
AT-2(1)			
AT-2(2)	+	X	X
AT-3	X	X	X
AT-3(2)	+	+	+
AT-3(4)	+	+	+
AT-4	X	X	X
AU-1	X	X	X
AU-2	X	X	
AU-2(3)	+	X	
AU-3	X	X	
AU-3(1)	+	X	
AU-3(2)		X	
AU-4			X
AU-4(1)	+	+	+
AU-5			X
AU-5(1)			+
AU-6	X	X	
AU-6(1)	+	X	
AU-6(3)	+	X	
AU-6(4)	+	+	
AU-6(5)		X	
AU-6(6)		X	
AU-6(10)	+	+	
AU-7		X	
AU-7(1)		X	
AU-8		X	
AU-8(1)		X	
AU-9	X	X	X
AU-9(3)		X	
AU-9(4)	+	X	
AU-10		X	
AU-11			X
AU-11(1)			+

	C	I	A
ID	L	H	M
AU-12	X	X	
AU-12(1)		X	
AU-12(3)	+	X	
AU-14	+	+	
AU-14(1)	+	+	
AU-14(2)	+	+	
AU-14(3)	+		
CA-1	X	X	X
CA-2	X	X	X
CA-2(1)	+	X	X
CA-2(2)		X	
CA-3	X	X	
CA-3(1)	+		
CA-3(5)	+	X	
CA-4			
CA-5	X	X	X
CA-6	X	X	X
CA-7	X	X	X
CA-7(1)		X	X
CA-8		X	
CA-9	X	X	
CM-1	X	X	
CM-2		X	
CM-2(1)		X	
CM-2(2)		X	
CM-2(3)		X	
CM-2(7)		X	
CM-3		X	
CM-3(1)		X	
CM-3(2)		X	
CM-3(4)		+	
CM-3(5)		+	
CM-3(6)		+	
CM-4		X	
CM-4(1)		X	
CM-5		X	
CM-5(1)		X	
CM-5(2)		X	
CM-5(3)		X	
CM-5(5)		+	
CM-5(6)		+	
CM-6		X	
CM-6(1)		X	
CM-6(2)		X	
CM-7	X	X	

	C	I	A
ID	L	H	M
CM-7(1)	+	X	
CM-7(2)	+	X	
CM-7(3)	+	+	
CM-7(5)	+	X	
CM-8		X	
CM-8(1)		X	
CM-8(2)		X	
CM-8(3)		X	
CM-8(4)		X	
CM-8(5)		X	
CM-9		X	
CM-9(1)			
CM-10		X	
CM-10(1)		+	
CM-11	X	X	
CM-11(1)		+	
CM-11(2)	+	+	
CP-1	X	X	X
CP-2			X
CP-2(1)			X
CP-2(3)			X
CP-2(8)			X
CP-3			X
CP-4			X
CP-4(1)			X
CP-6			X
CP-6(1)			X
CP-6(3)			X
CP-7		X	X
CP-7(1)			X
CP-7(2)			X
CP-7(3)			X
CP-8			X
CP-8(1)			X
CP-8(2)			X
CP-9	X	X	X
CP-9(1)		X	X
CP-9(5)			+
CP-10			X
CP-10(2)		X	X
CP-10(4)		X	
IA-1	X	X	
IA-2	X	X	
IA-2(1)	X	X	
IA-2(2)	+	X	

	C	I	A
ID	L	H	M
IA-2(3)		X	
IA-2(4)		X	
IA-2(5)	+	+	
IA-2(8)	+	X	
IA-2(9)		X	
IA-2(11)	+	X	
IA-2(12)	X	X	
IA-3	+	X	
IA-3(1)		+	
IA-4	X	X	
IA-4(4)	+	+	
IA-5	X	X	
IA-5(1)	X	X	
IA-5(2)		X	
IA-5(3)		X	
IA-5(4)	+	+	
IA-5(7)	+		
IA-5(8)	+	+	
IA-5(11)		X	
IA-5(13)	+	+	
IA-5(14)	+	+	
IA-6	X		
IA-7	X	X	
IA-8	X	X	
IA-8(1)	X	X	
IA-8(2)		X	
IA-8(3)		X	
IA-8(4)		X	
IA-10		+	
IA-11		+	
IR-1	X	X	X
IR-2	X	X	X
IR-2(1)		X	
IR-2(2)		X	
IR-3	+	X	X
IR-3(2)		X	X
IR-4	X	X	X
IR-4(1)		X	X
IR-4(3)		+	+
IR-4(4)	+	X	+
IR-4(6)	+	+	+
IR-4(7)	+	+	+
IR-4(8)	+	+	+
IR-5	X	X	X
IR-5(1)		X	

	C	I	A
ID	L	H	M
IR-6	X	X	X
IR-6(1)		X	X
IR-6(2)	+	+	+
IR-7	X	X	X
IR-7(1)		X	X
IR-7(2)	+	+	+
IR-8	X	X	X
IR-9	+		
IR-9(1)	+		
IR-9(2)	+		
IR-9(3)			+
IR-9(4)	+		
IR-10		+	+
MA-1	X	X	X
MA-2	X	X	X
MA-2(2)		X	
MA-3		X	
MA-3(1)		X	
MA-3(2)		X	
MA-3(3)	+		
MA-4		X	
MA-4(1)		+	
MA-4(2)		X	
MA-4(3)	+	X	
MA-4(6)	+	+	
MA-4(7)		+	
MA-5	X	X	X
MA-5(1)		X	
MA-6			X
MP-1	X	X	
MP-2	X	X	
MP-4		X	
MP-5		X	
MP-5(4)		X	
MP-6	X		
MP-7	X	X	
MP-7(1)		X	
PE-1	X	X	X
PE-2	X	X	X
PE-3	X	X	X
PE-3(1)	+	X	
PE-4		X	
PE-6	X	X	X
PE-6(1)		X	X
PE-6(4)		X	

	C	I	A
ID	L	H	M
PE-8	X	X	X
PE-8(1)		X	
PE-9			X
PE-10			X
PE-11			X
PE-12			X
PE-13			X
PE-13(3)			X
PE-14			X
PE-15			X
PE-16	X	X	X
PE-17		X	X
PL-1	X	X	X
PL-2	X	X	X
PL-2(3)		X	X
PL-4	X	X	X
PL-8	+	X	X
PL-8(1)	+	+	+
PL-8(2)	+	+	+
PS-1	X	X	X
PS-2	X	X	X
PS-3	X	X	
PS-4	X	X	X
PS-4(1)	+		
PS-4(2)		X	
PS-5	X	X	X
PS-6	X	X	
PS-6(3)	+		
PS-7	X	X	
PS-8	X	X	X
RA-1	X	X	X
RA-2	X	X	X
RA-3	X	X	X
RA-5	X	X	X
RA-5(1)	+	X	X
RA-5(2)	+	X	X
RA-5(4)	+	X	+
RA-5(5)	+	X	X
RA-5(10)		+	
SA-1	X	X	X
SA-2	X	X	X
SA-3	X	X	X
SA-4	X	X	X
SA-4(1)		X	X
SA-4(2)		X	X

	C	I	A
ID	L	H	M
SA-4(3)		+	
SA-4(5)		+	
SA-4(7)		+	
SA-4(9)	+	X	X
SA-4(10)	X	X	
SA-5	X	X	X
SA-8	+	X	X
SA-9	X	X	X
SA-9(1)		+	
SA-9(2)	+	X	X
SA-10		X	
SA-10(1)		+	
SA-11		X	X
SA-12	+	X	+
SA-12(1)		+	
SA-12(5)		+	
SA-12(8)		+	
SA-12(9)		+	
SA-12(11)		+	
SA-14		+	
SA-15	+	X	+
SA-15(3)		+	
SA-15(4)		+	
SA-15(7)		+	
SA-15(9)	+		
SA-16		X	
SA-17		X	
SA-19		+	
SA-22		+	
SC-1	X	X	X
SC-2		X	
SC-3		X	
SC-5			X
SC-5(1)			+
SC-5(2)			+
SC-5(3)			+
SC-7	X	X	
SC-7(3)	+	X	
SC-7(4)	+	X	
SC-7(5)	+	X	
SC-7(7)	+	X	
SC-7(8)	+	X	
SC-7(9)		+	
SC-7(10)	+		
SC-7(11)		+	

	C	I	A
ID	L	H	M
SC-7(12)	+	+	+
SC-7(13)	+	+	
SC-7(14)	+	+	
SC-7(18)		X	
SC-7(21)		X	
SC-8	+	X	
SC-8(1)	+	X	
SC-8(2)		+	
SC-10		X	
SC-12	X	X	
SC-13	X	X	
SC-15	X		
SC-17	+	X	
SC-18		X	
SC-18(1)		+	
SC-18(2)		+	
SC-18(3)		+	
SC-18(4)		+	
SC-19	+	X	
SC-20		X	
SC-21		X	
SC-22	X	X	X
SC-23		X	
SC-23(1)		+	
SC-23(3)		+	
SC-23(5)		+	
SC-24		X	
SC-28	+	X	
SC-28(1)	+	+	
SC-38	+	+	+
SC-39	X	X	
SI-1	X	X	X
SI-2		X	
SI-2(1)		X	
SI-2(2)		X	
SI-2(3)		+	
SI-2(6)		+	
SI-3		X	
SI-3(1)		X	
SI-3(2)		X	
SI-3(10)		+	
SI-4	X	X	X
SI-4(1)	+	+	+
SI-4(2)		X	X
SI-4(4)	+	X	X

	C	I	A
ID	L	H	M
SI-4(5)	+	X	X
SI-4(10)		+	+
SI-4(11)	+	+	+
SI-4(12)	+	+	+
SI-4(14)	+	+	+
SI-4(15)	+	+	+
SI-4(16)	+	+	+
SI-4(19)	+	+	+
SI-4(20)	+	+	+
SI-4(22)	+	+	+
SI-4(23)	+	+	+
SI-5		X	
SI-5(1)		X	
SI-6		X	
SI-6(3)		+	
SI-7		X	
SI-7(1)		X	
SI-7(2)		X	
SI-7(5)		X	
SI-7(7)		X	
SI-7(8)		+	
SI-7(14)		X	
SI-8		X	X
SI-8(1)		X	X
SI-8(2)		X	X
SI-10		X	
SI-10(3)		+	
SI-11		X	
SI-12	X	X	
SI-16		X	
PM-1	X	X	X
PM-2	X	X	X
PM-3	X	X	X
PM-4	X	X	X
PM-5	X	X	X
PM-6	X	X	X
PM-7	X	X	X
PM-8	X	X	X
PM-9	X	X	X
PM-10	X	X	X
PM-11	X	X	X
PM-12	X	X	X
PM-13	X	X	X
PM-14	X	X	X
PM-15	X	X	X
PM-16	X	X	X

Source: CNSS Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, 27 March 2014

MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

But lucky you, you have a Target Profile!

Function	Category	Subcategory	Maintain Continuity & Integrity of Operations
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	●●●
		ID.AM-2: Software platforms and applications within the organization are inventoried	●●●
		ID.AM-3: Organizational communication and data flows are mapped	●
		ID.AM-4: External information systems are catalogued	●●
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	●●●
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	●●●

Function	Category	Subcategory	Maintain Consistent Consumer Experience
PROTECT-P (PR-P): Develop and implement appropriate data processing safeguards.	**Data Protection Policies, Processes, and Procedures (PR.PO-P):** Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.	**CT.DP-P1:** Data are processed to limit observability and linkability (e.g., data actions take place on local devices, privacy-preserving cryptography).	●●
		CT.DP-P2: Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization).	●●●
		CT.DP-P3: Data are processed to limit the formulation of inferences about individuals' behavior or activities (e.g., data processing is decentralized, distributed architectures).	✕
		CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.	●●
		CT.DP-P5: Attribute references are substituted for attribute values.	●●●

MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Traceability from Mission Objective Priorities to Controls

The Framework Informative References map to a subset of NIST SP 800-53 controls that support implementation of the prioritized Subcategories. Through the priorities articulated in the Framework Profile, we have information that helps us justify, prioritize, and tailor the 450 controls in the baseline.

High Priority Subcategories	Moderate Priority Subcategories	Related NIST SP 800-53 Controls
Cybersecurity Framework - IDENTIFY: Asset Management		
ID-AM-1		CM-8, PM-5
ID.AM-2		CM-8
	ID.AM-4	AC-20, PM-5, SA-9
ID.AM-5		CP-2, RA-2, RA-9, *SA-20* *SC-6*
ID.AM-6		CP-2, PS-7, PM-2, PM-29
Privacy Framework – CONTROL: Disassociated Processing		
	CT.DP-P1	N/A
CT.DP-P2		N/A
	CT.DP-P4	N/A
CT.DP-P5		N/A

12 can be used to implement the priority Cybersecurity Framework Subcategories for the Maintain Continuity & Integrity of Operations Mission Objective

- *These will be among the most critical to implement*

2 are not part of the current baseline

- *SA-20 and SC-6 may need to be added during tailoring*

0 directly map to the Privacy Framework Subcategories prioritized for Maintain Consistent Consumer Experience

- *The Informative References point to other resources that can support implementation*

MITRE

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Communications to Manage Risk

- Risk can never be entirely eliminated but it can be managed – communication helps manage that risk
- Communicating cybersecurity risks as they relate to mission and business objectives:
  - Provides senior leadership risk managers information about impacts to systems that can inform enterprise risk responses
  - Leadership can use the terminology from the Cybersecurity and Privacy Frameworks to communicate risk without forcing them to use IT terminology and instead use terms they already understand and use
  - Enables technical personnel to have a proactive and mission-oriented view and supports decisions by enterprise leadership
  - Can be used by technical personnel to participate in meetings with leadership using terminology that isn't overly complex or technical

Risk management is not a one-size-fits-all approach

Source (adapted): NIST *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Communicating Effectively

- Use the Cybersecurity and Privacy Frameworks in conversations to:
  - Understand where there is potential for impact to mission success
  - Focus on specific cybersecurity and privacy outcomes/priorities
  - Create meaningful risk management discussions and drive explicit differences in terminology to the surface
  - Frame conversations between board room and server room:
    - Using meaningful data
    - Without having to teach technical concepts or cybersecurity or privacy-specific terms
    - Contribute to integrated teams comprised of experts from various fields
  - Inform decisions on risk acceptance
  - Impact strategic goals and objectives
  - Inform allocations of resources
  - Understand tradeoffs in resource allocations and requesting funding to address system needs

Sources (adapted): NIST webinar "The Missing Link: Integrating Cybersecurity and ERM," *https://www.nist.gov/video/missing-link-integrating-cybersecurity-and-erm* NIST Cybersecurity Framework events and presentations (various), https://www.nist.gov/cyberframework/events-and-presentations/past-events, https://www.nist.gov/cyberframework/events-and-presentations/webcasts

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Contact Information

Julie Snyder

jsnyder@mitre.org

@privacyeng

linkedin.com/in/julienetherysnyder

Christina Sames

csames@mitre.org

linkedin.com/in/christina-s-a1177451/

David Weitzel

dweitzel@mitre.org

@david_weitzel

linkedin.com/in/david-weitzel-55119924/

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

© 2022 THE MITRE CORPORATION. ALL RIGHTS RESERVED.