EnterpriseGRC Solutions, Inc.

Just Tell Me What to Do: Building Cloud Products consumed by Government Agencies, Current State

Further Understanding NIST SP 800-53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations; Using an RMF, Selecting from other catalogs

Presented by Robin Basham, CEO, EnterpriseGRC Solutions

To ISC2 Silicon Valley, on March 8th, 2022

“Simply restating controls does not constitute an organizational policy or procedure.”

This is the most repeated phrase in the NIST SP 800-53.

Building Cloud Products for Federal Agencies – Using NIST to Shift Compliance Left

Vendors & Consultants must be NIST Compliant

Vendors and Consultants working with Federal Agencies are required to establish secure products and services and to do so using a Cybersecurity Framework mapped to address common cybersecurity-related responsibilities.

Common sets of categorized outcomes are:

- NIST SP 800-53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Cybersecurity Framework (CSF) and NIST Privacy Framework (PF) as mapped to NIST Special Publication (SP) 800-53, Revision 5, NERC, ISSA, ISO
- Various cybersecurity frameworks, such as CIS-CSC 8.1, CCM v4.5 which are also mapped to the CSF/PF Core and to the SP 800-53 controls that support the achievement of the Subcategories

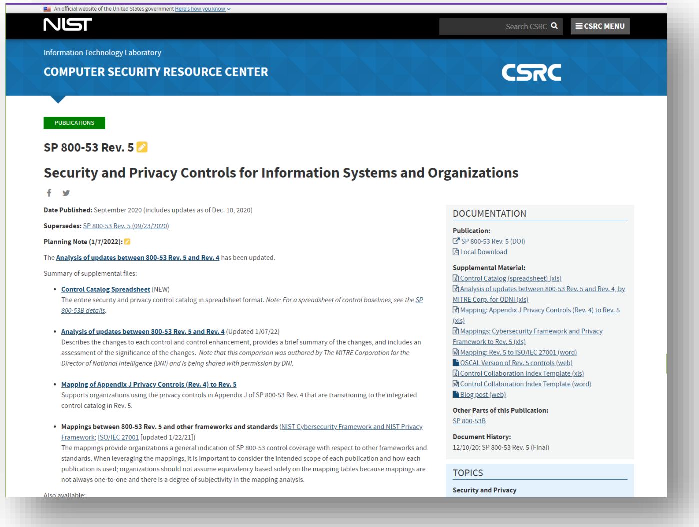
What it really takes to implement NIST

The CCM 4.2 to NIST SP 800-53r5 mapping is now available Cloud Controls Matrix and CAIQ v4 | CSA (cloudsecurityalliance.org)

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

Using NIST Special Publication 800-53 to Shift Left

1. This training teaches that NIST SP 800-53 is a catalog and part of a Risk Management Framework
2. We'll review the history of NIST and ITL's SP 800-53 effort and highlight CSF, CCM, CIS-CSC, ISO, & SOC 2 mappings
3. We'll describe the components of the Security and Privacy controls "Catalog" relative to Legal Requirements
4. We'll cover NIST's Risk Management approach, the RMF and how the CSF also fits into its implementation.
5. We'll Enable you to reference the SP 800-53 for functional and assessment purposes and to extend that to DFARS, SOC 2, STAR, FedRamp, or ISO/IEC 27001 and Cloud Certification scenarios


An official website of the United States government Here's how you know
NIST
Search CSRC
CSRC MENU
CSRC
PUBLICATIONS

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

SP 800-53 Rev. 5

Security and Privacy Controls for Information Systems and Organizations

Date Published: September 2020 (includes updates as of Dec. 10, 2020)

Supersedes: SP 800-53 Rev. 5 (09/23/2020)

Planning Note (1/7/2022):

The **Analysis of updates between 800-53 Rev. 5 and Rev. 4** has been updated.

Summary of supplemental files:

- **Control Catalog Spreadsheet** (NEW)
  The entire security and privacy control catalog in spreadsheet format. *Note: For a spreadsheet of control baselines, see the SP 800-53B details.*
- **Analysis of updates between 800-53 Rev. 5 and Rev. 4** (Updated 1/07/22)
  Describes the changes to each control and control enhancement, provides a brief summary of the changes, and includes an assessment of the significance of the changes. *Note that this comparison was authored by The MITRE Corporation for the Director of National Intelligence (DNI) and is being shared with permission by DNI.*
- **Mapping of Appendix J Privacy Controls (Rev. 4) to Rev. 5**
  Supports organizations using the privacy controls in Appendix J of SP 800-53 Rev. 4 that are transitioning to the integrated control catalog in Rev. 5.
- **Mappings between 800-53 Rev. 5 and other frameworks and standards** (NIST Cybersecurity Framework and NIST Privacy Framework; ISO/IEC 27001 [updated 1/22/21])
  The mappings provide organizations a general indication of SP 800-53 control coverage with respect to other frameworks and standards. When leveraging the mappings, it is important to consider the intended scope of each publication and how each publication is used; organizations should not assume equivalency based solely on the mapping tables because mappings are not always one-to-one and there is a degree of subjectivity in the mapping analysis.

Also available:

DOCUMENTATION

Publication:
SP 800-53 Rev. 5 (DOI)
Local Download

Supplemental Material:
Control Catalog (spreadsheet) (xls)
Analysis of updates between 800-53 Rev. 5 and Rev. 4, by MITRE Corp. for ODNI (xls)
Mapping: Appendix J Privacy Controls (Rev. 4) to Rev. 5 (xls)
Mappings: Cybersecurity Framework and Privacy Framework to Rev. 5 (xls)
Mapping: Rev. 5 to ISO/IEC 27001 (word)
OSCAL Version of Rev. 5 controls (web)
Control Collaboration Index Template (xls)
Control Collaboration Index Template (word)
Blog post (web)

Other Parts of this Publication:
SP 800-53B

Document History:
12/10/20: SP 800-53 Rev. 5 (Final)

TOPICS

Security and Privacy

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

The CCM 4.2 to NIST SP 800-53r5 mapping is now available Cloud Controls Matrix and CAIQ v4 | CSA (cloudsecurityalliance.org)

NIST Compliance is more than just NIST SP 800-53

EnterpriseGRC Solutions, Inc.

While some companies have adopted NIST SP 800-53 rev 5, many Cloud Service Providers are not actively engaged to manage Federal Systems and Data. Those entities need a path to demonstrating NIST Compliance. This likely involves the CSF and or NIST SP 800-171. These CSP often engage in parallel attestations such as SOC 2, ISO/IEC 2700 series, CIS-CSC, and CSA STAR.

- Cybersecurity Framework (CSF) publishes with mapping to NIST SP 800-53 and ISO/IEC 27001, but its missing granular detail mapping down to the enhancements and needs a refresh to cover the cloud attributes associated with ISO/IEC 27001 and 27002, plus ISO/IEC 27017, CCM v4.5, CIS-CSC v8, and SOC 2® - SOC for Service Organizations: Trust Services Criteria.
- In addition to these considerations, most companies have or will soon embark on DFARS CMMC 2.0 compliance.
- To learn more about CMMC and NIST 171 you may want to replay January's ISC2 East Bay training NIST 171 CMMC Training

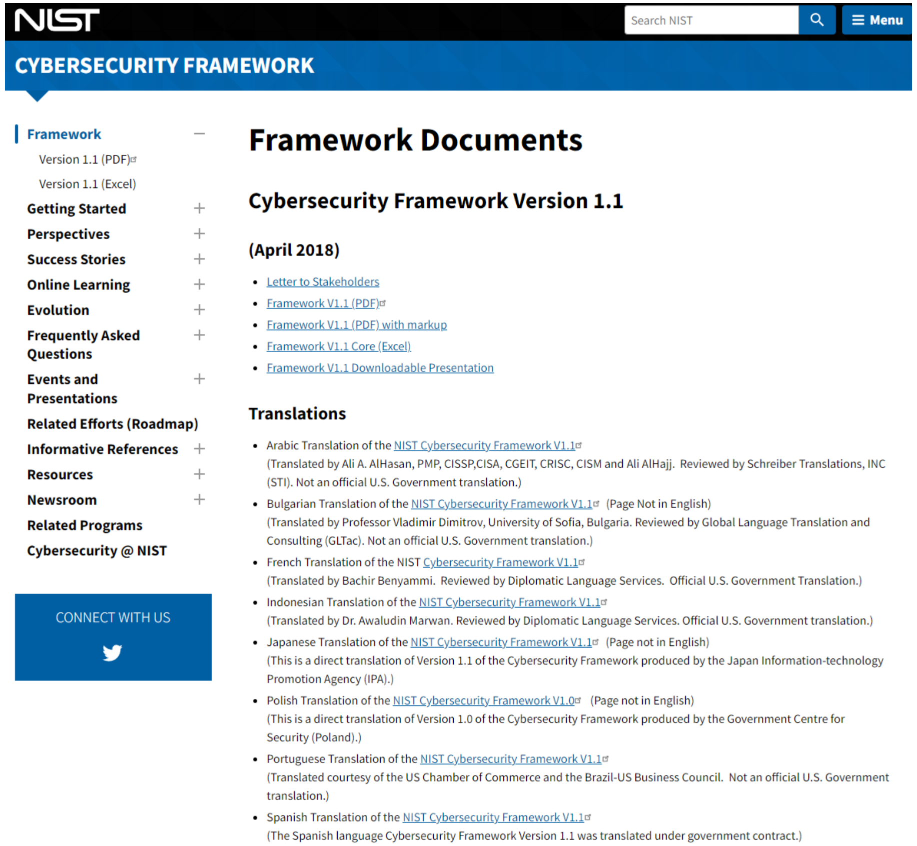
SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

Many Companies will accomplish NIST compliance with the CSF

EnterpriseGRC Solutions, Inc.

Widely Adopted and Highly Accessible

Framework Documents | NIST



Framework Documents

Cybersecurity Framework Version 1.1

(April 2018)

- Letter to Stakeholders
- Framework V1.1 (PDF)
- Framework V1.1 (PDF) with markup
- Framework V1.1 Core (Excel)
- Framework V1.1 Downloadable Presentation

Translations

- Arabic Translation of the NIST Cybersecurity Framework V1.1
(Translated by Ali A. AlHasan, PMP, CISSP,CISA, CGEIT, CRISC, CISM and Ali AlHajj. Reviewed by Schreiber Translations, INC (STI). Not an official U.S. Government translation.)
- Bulgarian Translation of the NIST Cybersecurity Framework V1.1 (Page Not in English)
(Translated by Professor Vladimir Dimitrov, University of Sofia, Bulgaria. Reviewed by Global Language Translation and Consulting (GLTac). Not an official U.S. Government translation.)
- French Translation of the NIST Cybersecurity Framework V1.1
(Translated by Bachir Benyammi. Reviewed by Diplomatic Language Services. Official U.S. Government Translation.)
- Indonesian Translation of the NIST Cybersecurity Framework V1.1
(Translated by Dr. Awaludin Marwan. Reviewed by Diplomatic Language Services. Official U.S. Government translation.)
- Japanese Translation of the NIST Cybersecurity Framework V1.1 (Page not in English)
(This is a direct translation of Version 1.1 of the Cybersecurity Framework produced by the Japan Information-technology Promotion Agency (IPA).)
- Polish Translation of the NIST Cybersecurity Framework V1.0 (Page not in English)
(This is a direct translation of Version 1.0 of the Cybersecurity Framework produced by the Government Centre for Security (Poland).)
- Portuguese Translation of the NIST Cybersecurity Framework V1.1
(Translated courtesy of the US Chamber of Commerce and the Brazil-US Business Council. Not an official U.S. Government translation.)
- Spanish Translation of the NIST Cybersecurity Framework V1.1
(The Spanish language Cybersecurity Framework Version 1.1 was translated under government contract.)

Pluses and Minuses in using CSF 1.1 Current state

- ⊕ Using the CSF 1.1 plus Privacy Framework finally extends to major gaps between AICPA Cybersecurity mandates related to the SOC 2 as necessary for specific industries
- ⊕ The CSF 1.1 better aligns with ISO/IEC 27017 added requirements for Cloud Services
- ⊖ Industry mappings are not keeping pace with the Cybersecurity Framework which is currently served in CSF Tools mapped to CIS-CSC v7.1 and CCM 3.0 which causes problems with cyber event interpretation
- ⊖ Mappings to NIST SP 800-53 miss critical new guidance necessary to EO 14028, SR, PT, PM
- ⊖ Mappings to CCM 3 v. CCM 4.2 misses advancements in all domains, but especially Encryption and Data Security

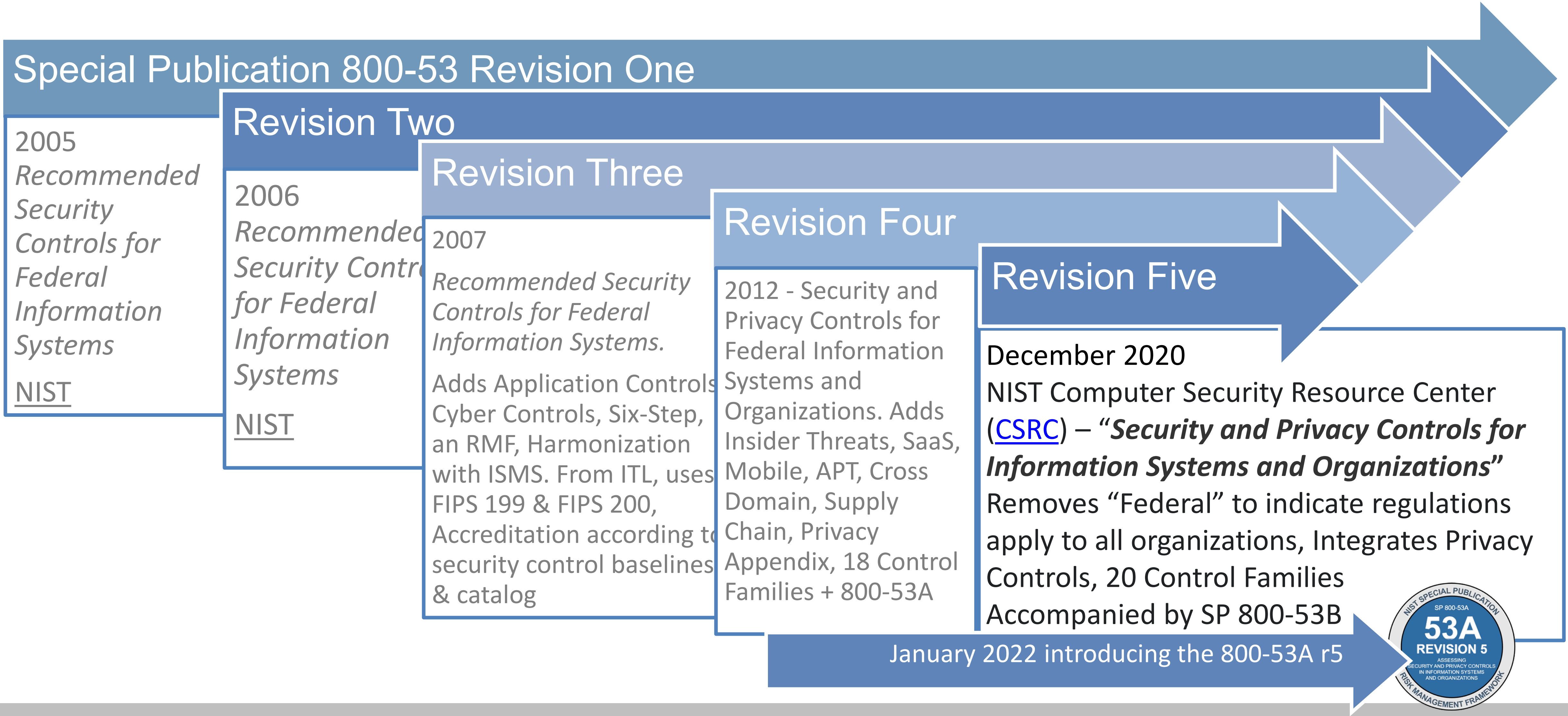
The CCM 4.2 to NIST SP 800-53r5 mapping is now available Cloud Controls Matrix and CAIQ v4 | CSA (cloudsecurityalliance.org)

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

NIST SP 800-53
Background & History

The Evolution of NIST SP 800-53 Revision Five

EnterpriseGRC Solutions, Inc.



Special Publication 800-53 Revision One

2005 *Recommended Security Controls for Federal Information Systems*

NIST

Revision Two

2006 *Recommendec Security Contr for Federal Information Systems*

NIST

Revision Three

2007

Recommended Security Controls for Federal Information Systems.

Adds Application Controls Cyber Controls, Six-Step, an RMF, Harmonization with ISMS. From ITL, uses FIPS 199 & FIPS 200, Accreditation according t security control baselines & catalog

Revision Four

2012 - Security and Privacy Controls for Federal Information Systems and Organizations. Adds Insider Threats, SaaS, Mobile, APT, Cross Domain, Supply Chain, Privacy Appendix, 18 Control Families + 800-53A

Revision Five

December 2020

NIST Computer Security Resource Center (CSRC) – "***Security and Privacy Controls for Information Systems and Organizations***"

Removes "Federal" to indicate regulations apply to all organizations, Integrates Privacy Controls, 20 Control Families

Accompanied by SP 800-53B

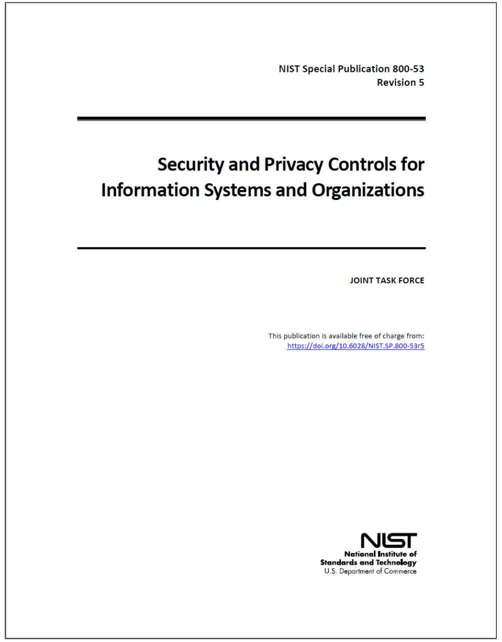
January 2022 introducing the 800-53A r5

NIST SPECIAL PUBLICATION
SP 800-53A
53A
REVISION 5
ASSESSING SECURITY AND PRIVACY CONTROLS IN INFORMATION SYSTEMS AND ORGANIZATIONS
RISK MANAGEMENT FRAMEWORK

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

NIST is Risk Management, Information Security, and Privacy

EnterpriseGRC Solutions, Inc.



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for
Information Systems and Organizations

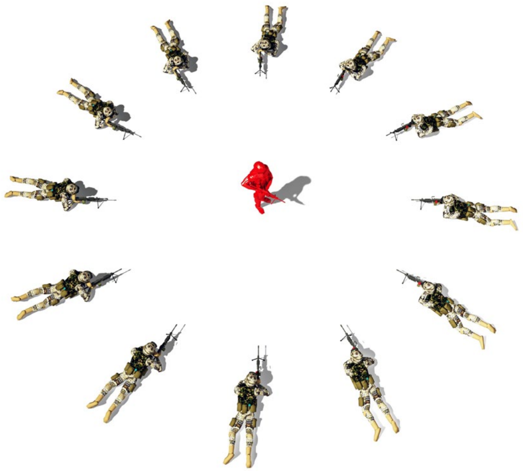
JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Publications involve Risk Management, Information Security, and Privacy.

NIST guidance offers protection measures that address threats to US critical infrastructure and the continuity of our government.



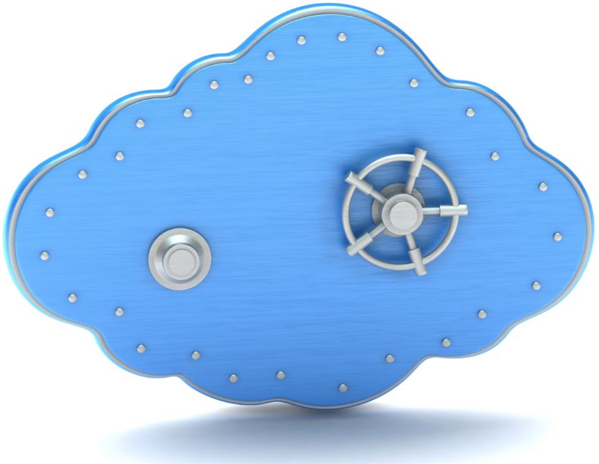
RISK MANAGEMENT

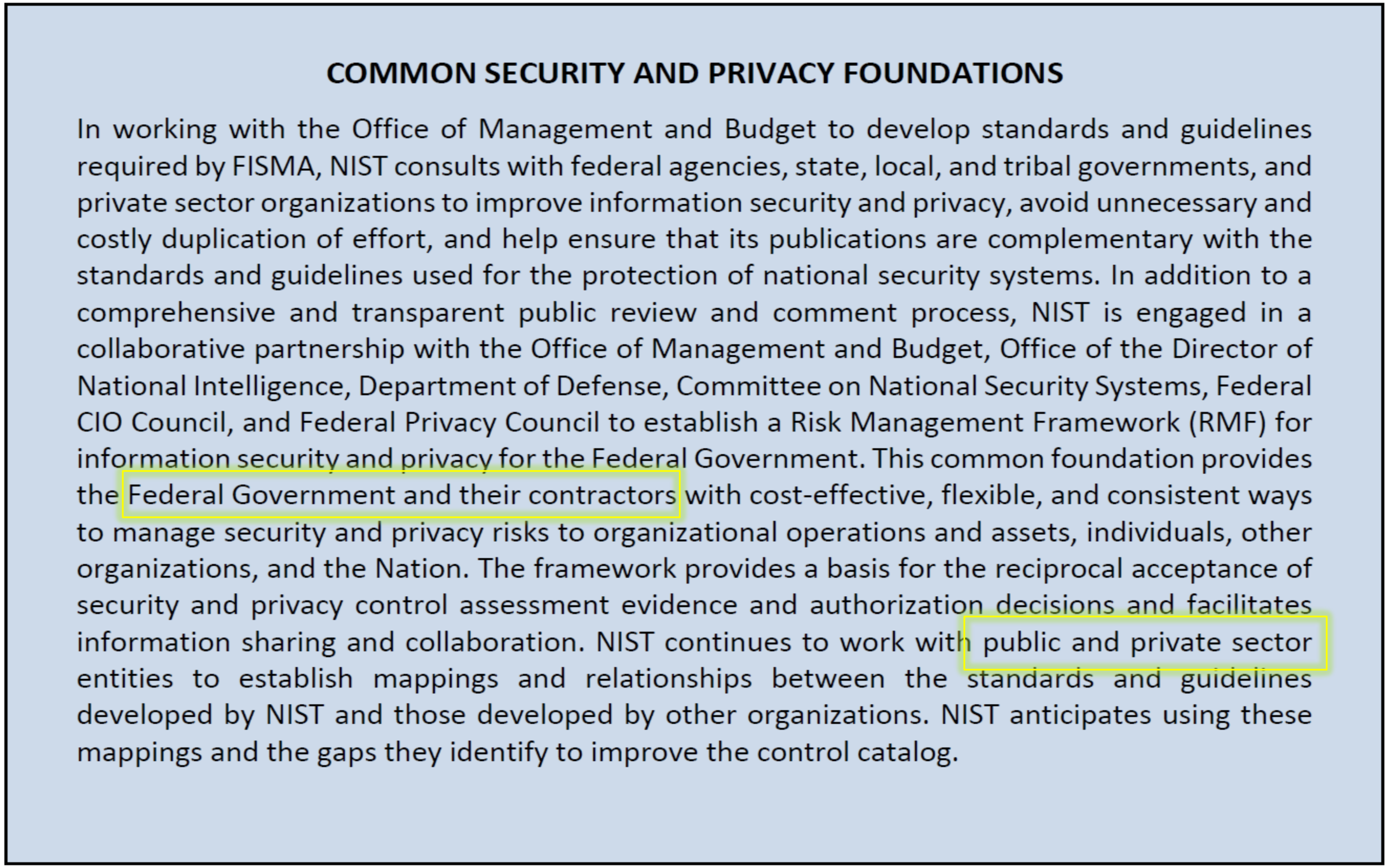
Organizations must exercise *due diligence* in managing information security and privacy risk. This is accomplished, in part, by establishing a comprehensive risk management program that uses the flexibility inherent in NIST publications to categorize systems, select and implement security and privacy controls that meet mission and business needs, assess the effectiveness of the controls, authorize the systems for operation, and continuously monitor the systems. Exercising due diligence and implementing robust and comprehensive information security and privacy risk management programs can facilitate compliance with applicable laws, regulations, executive orders, and governmentwide policies. Risk management frameworks and risk management processes are essential in developing, implementing, and maintaining the protection measures necessary to address stakeholder needs and the current threats to organizational operations and assets, individuals, other organizations, and the Nation. Employing effective risk-based processes, procedures, methods, and technologies ensures that information systems and organizations have the necessary trustworthiness and resiliency to support essential mission and business functions, the U.S. critical infrastructure, and continuity of government.

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

NIST Also Works with Public and Private Sector

With the onset of Cloud Technology, the Federal Government and its contractors could no longer operate in complete isolation, so NIST frameworks evolved to service the Public and Private Sectors.





COMMON SECURITY AND PRIVACY FOUNDATIONS

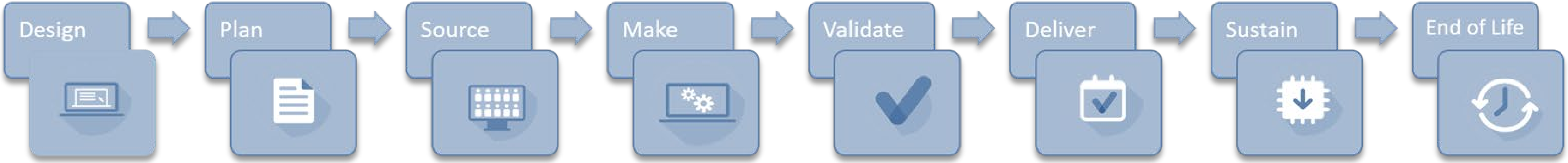
In working with the Office of Management and Budget to develop standards and guidelines required by FISMA, NIST consults with federal agencies, state, local, and tribal governments, and private sector organizations to improve information security and privacy, avoid unnecessary and costly duplication of effort, and help ensure that its publications are complementary with the standards and guidelines used for the protection of national security systems. In addition to a comprehensive and transparent public review and comment process, NIST is engaged in a collaborative partnership with the Office of Management and Budget, Office of the Director of National Intelligence, Department of Defense, Committee on National Security Systems, Federal CIO Council, and Federal Privacy Council to establish a Risk Management Framework (RMF) for information security and privacy for the Federal Government. This common foundation provides the Federal Government and their contractors with cost-effective, flexible, and consistent ways to manage security and privacy risks to organizational operations and assets, individuals, other organizations, and the Nation. The framework provides a basis for the reciprocal acceptance of security and privacy control assessment evidence and authorization decisions and facilitates information sharing and collaboration. NIST continues to work with public and private sector entities to establish mappings and relationships between the standards and guidelines developed by NIST and those developed by other organizations. NIST anticipates using these mappings and the gaps they identify to improve the control catalog.

Information Systems – Broad-Based Perspective

INFORMATION SYSTEMS — A BROAD-BASED PERSPECTIVE

As we push computers to “the edge,” building an increasingly complex world of interconnected systems and devices, security and privacy continue to dominate the national dialogue. There is an urgent need to further strengthen the underlying systems, products, and services that we depend on in every sector of the critical infrastructure to ensure that those systems, products, and services are sufficiently trustworthy and provide the necessary resilience to support the economic and national security interests of the United States. NIST Special Publication 800-53, Revision 5, responds to this need by embarking on a proactive and systemic approach to develop and make available to a broad base of public and private sector organizations a comprehensive set of security and privacy safeguarding measures for all types of computing platforms, including general purpose computing systems, cyber-physical systems, cloud systems, mobile systems, industrial control systems, and Internet of Things (IoT) devices. Safeguarding measures include both security and privacy controls to protect the critical and essential operations and assets of organizations and the privacy of individuals. The objective is to make the systems we depend on more penetration resistant to attacks, limit the damage from those attacks when they occur, and make the systems resilient, survivable, and protective of individuals’ privacy.

Adding System & Service Acquisition (SA) and Supply Chain Risk Management (SR)



As the world increases its cloud and IoT dependencies, NIST raises emphasis on System and Services Acquisitions and on Supply Chain Risk Management.

DEVELOPMENT OF INFORMATION SYSTEMS, COMPONENTS, AND SERVICES

With a renewed emphasis on the use of trustworthy, secure information systems and supply chain security, it is essential that organizations express their security and privacy requirements with clarity and specificity in order to obtain the systems, components, and services necessary for mission and business success. Accordingly, this publication provides controls in the System and Services Acquisition (SA) and Supply Chain Risk Management (SR) families that are directed at developers. The scope of the controls in those families includes information system, system component, and system service development *and* the associated developers whether the development is conducted internally by organizations or externally through the contracting and acquisition processes. The affected controls in the control catalog include SA-8, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20, SA-21, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, and SR-11.

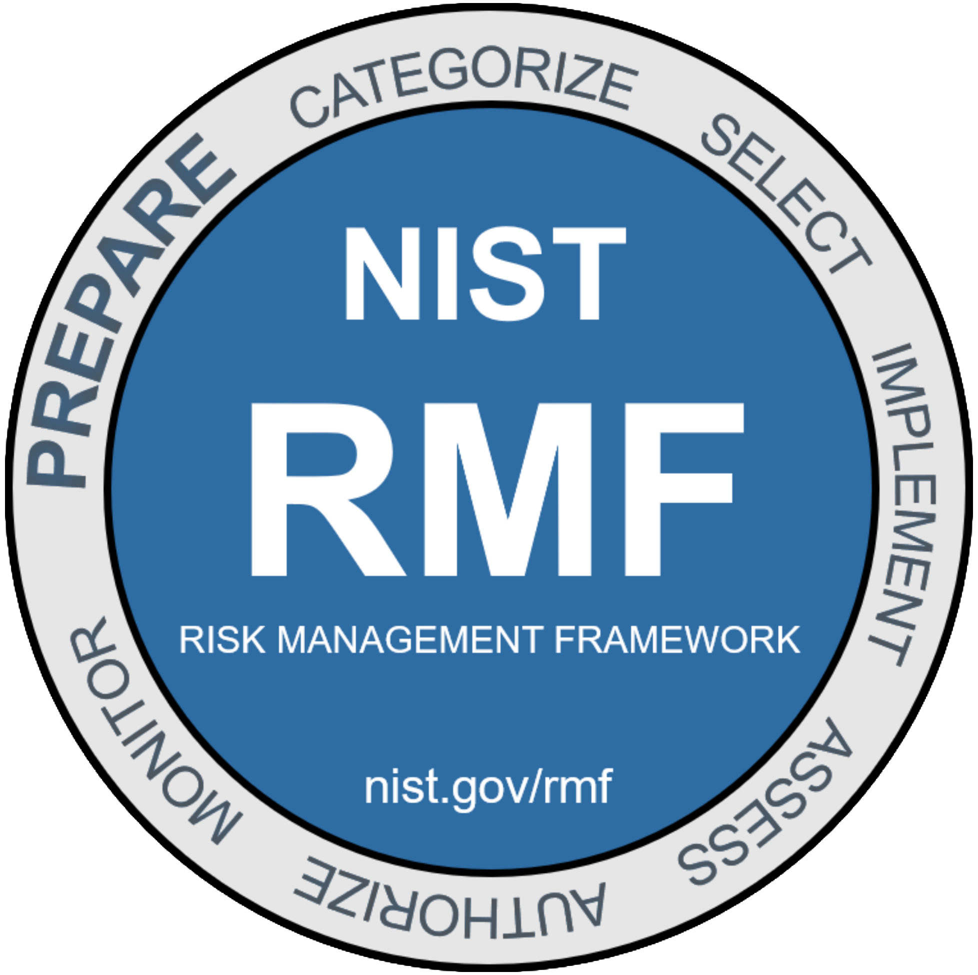
SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

Risk Management Framework

RMF NIST Special Publication 800-37, Guide for Applying the Risk Management Framework is a holistic and comprehensive risk management process

Integrates the Risk Management Framework (RMF) into the system development lifecycle (SDLC)

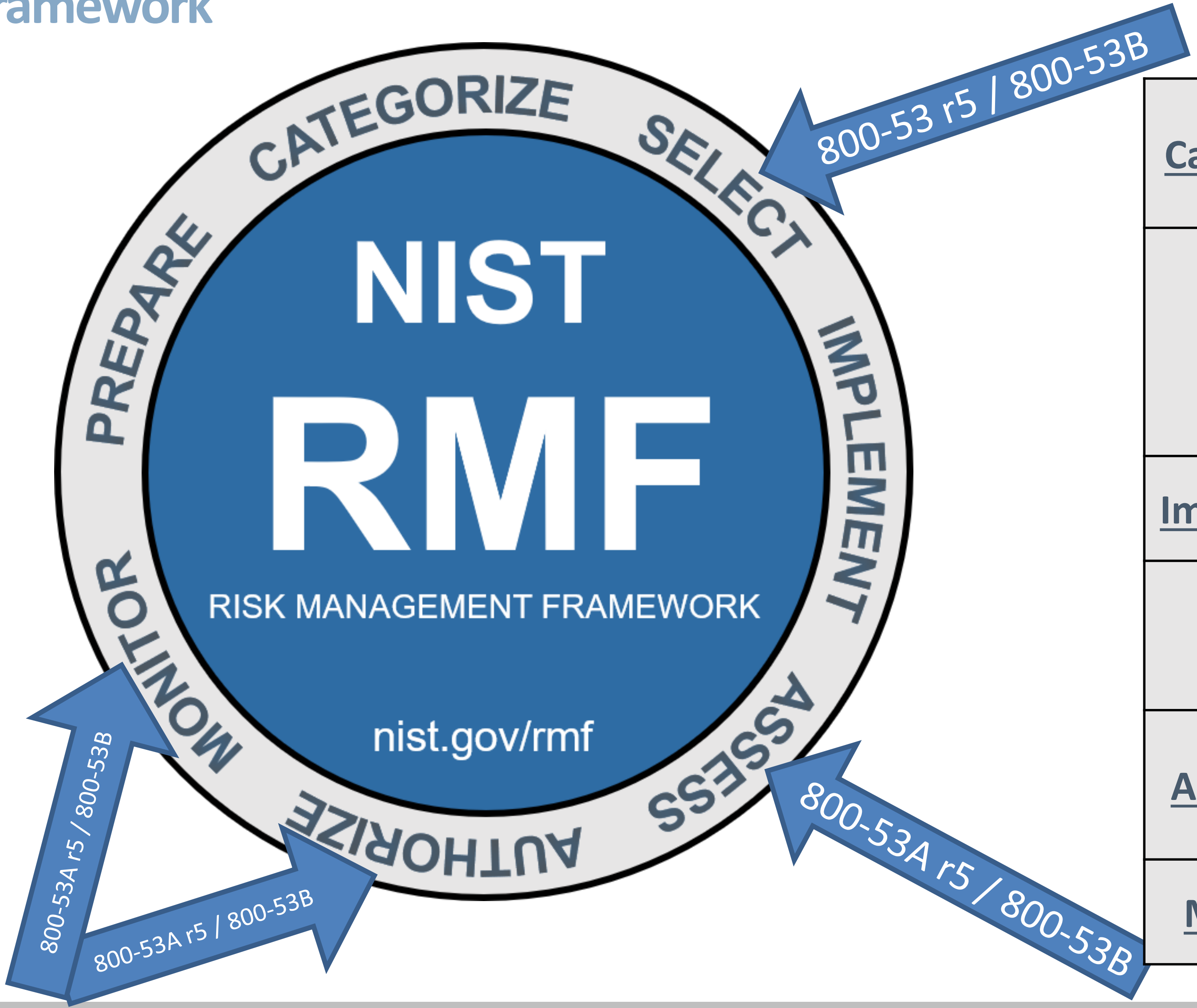
Provides processes (tasks) for each of the six steps in the RMF at the system level



SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

"SELECT", "Assess" and "Monitor" stages in the Risk Management Framework

EnterpriseGRC Solutions, Inc.

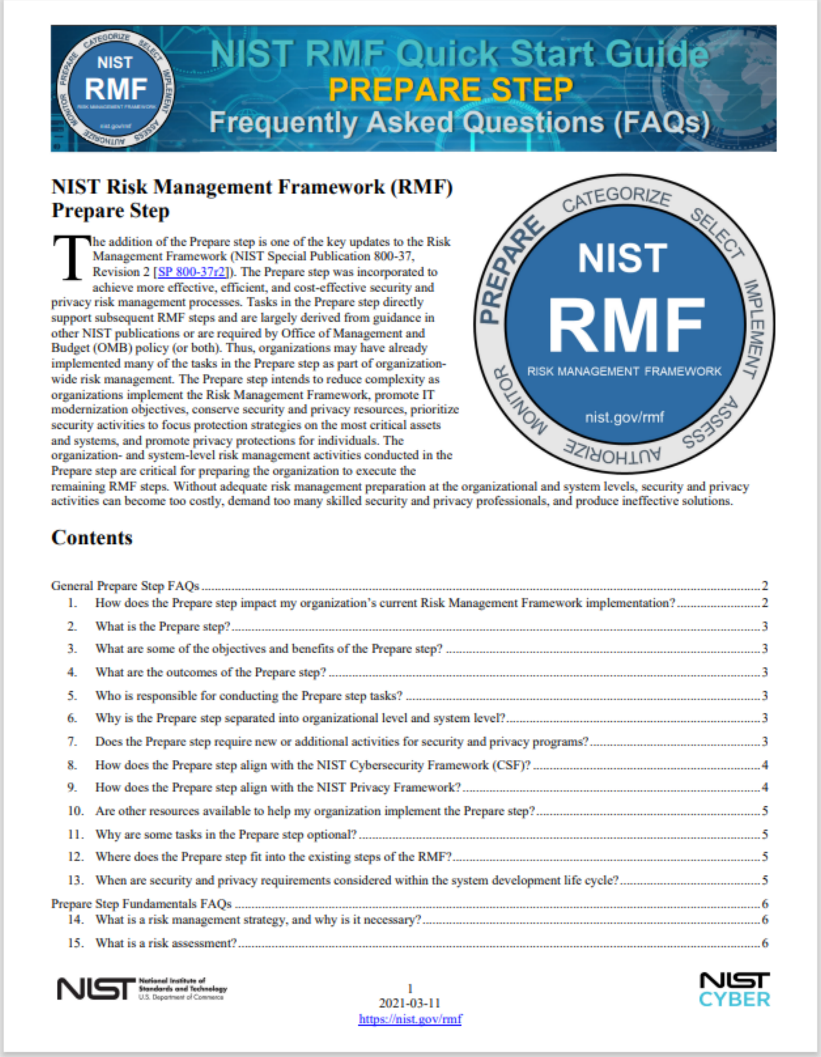


Categorize	**Categorize** the system and information processed, stored, and transmitted based on an impact analysis (FIPS 199)
Select	**Select** the set of NIST SP 800-53 r5 controls to protect the system based on risk assessment(s) (NIST SP 800-53B Baseline) *NIST CSF, CCM, ISO27001+27002+27017, CIS-CSC v8.1, NIST SP 800 171r2+172, SOC 2, etc.
Implement	**Implement** the controls and document how controls are deployed
Assess	**Assess** to determine if the controls are in place, operating as intended, and producing the desired results (NIST SP 800-53A) *SOC 2, NIST 171, STAR
Authorize	The senior official makes a risk-based decision to **authorize** the system (to operate) – the outcome of the NIST SP 800-53B Assess step
Monitor	Continuously **monitor** control implementation and risks to the system (as in 800-53B)

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

Each Step in the RMF has an associated 15-page guide

- **Quick Start Guides (QSG) for the RMF Steps**
- Download RMF QSG: Prepare Step FAQ (.pdf)
- Download RMF QSG: Categorize Step FAQ (.pdf)
- Download RMF QSG: Select Step FAQ (.pdf)
- Download RMF QSG: Implement Step FAQ (.pdf)
- Download RMF QSG: Assess Step FAQ (.pdf)
- Download RMF QSG: Authorize Step FAQ (.pdf)
- Download RMF QSG: Monitor Step FAQ (.pdf)
- Download RMF QSG: ALL FAQs (.zip)
- Download RMF QSG: Roles and Responsibilities (.pdf)



NIST RMF Quick Start Guide
PREPARE STEP
Frequently Asked Questions (FAQs)

NIST Risk Management Framework (RMF)
Prepare Step

The addition of the Prepare step is one of the key updates to the Risk Management Framework (NIST Special Publication 800-37, Revision 2 [SP 800-37r2]). The Prepare step was incorporated to achieve more effective, efficient, and cost-effective security and privacy risk management processes. Tasks in the Prepare step directly support subsequent RMF steps and are largely derived from guidance in other NIST publications or are required by Office of Management and Budget (OMB) policy (or both). Thus, organizations may have already implemented many of the tasks in the Prepare step as part of organization-wide risk management. The Prepare step intends to reduce complexity as organizations implement the Risk Management Framework, promote IT modernization objectives, conserve security and privacy resources, prioritize security activities to focus protection strategies on the most critical assets and systems, and promote privacy protections for individuals. The organization- and system-level risk management activities conducted in the Prepare step are critical for preparing the organization to execute the remaining RMF steps. Without adequate risk management preparation at the organizational and system levels, security and privacy activities can become too costly, demand too many skilled security and privacy professionals, and produce ineffective solutions.

Contents

NIST National Institute of Standards and Technology U.S. Department of Commerce

1
2021-03-11
https://nist.gov/rmf

NIST CYBER

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

Everyone using the NIST RMF should identify with one or more roles

EnterpriseGRC Solutions, Inc.

NIST Risk Management Framework Quick Start Guide

ROLES AND RESPONSIBILITIES CROSSWALK

(October 1, 2021)

NIST National Institute of Standards and Technology U.S. Department of Commerce

ITL INFORMATION TECHNOLOGY LABORATORY

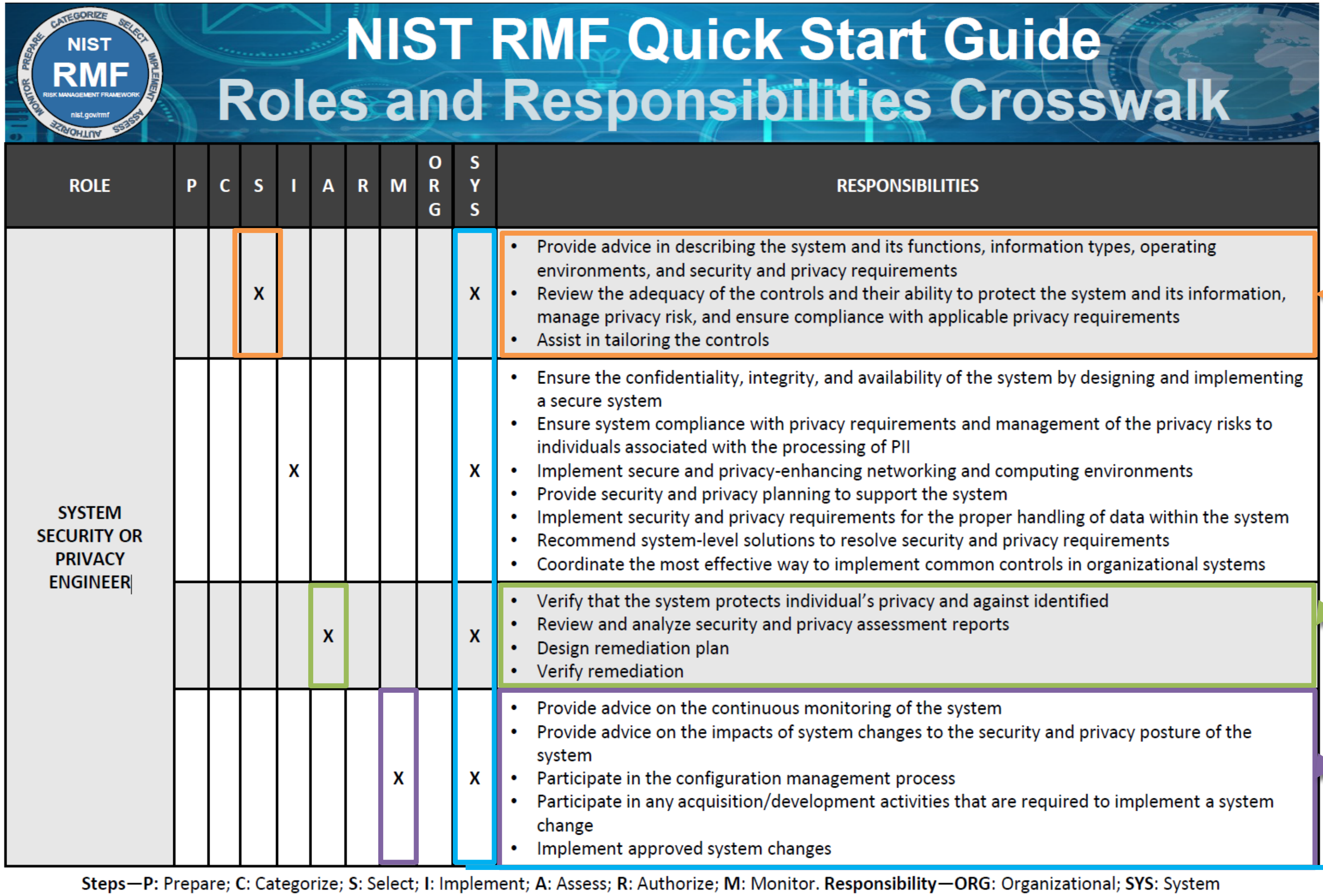
The NIST 800-53 series is written for organizations and systems. Organizations are comprised of roles and systems have roles such as administrator, owner, engineer, user, and architect.

- AUTHORIZING OFFICIAL OR AUTHORIZING
- OFFICIAL DESIGNATED REPRESENTATIVE
- CHIEF ACQUISITION OFFICER
- CHIEF INFORMATION OFFICER
- COMMON CONTROL PROVIDER
- CONTROL ASSESSOR
- ENTERPRISE ARCHITECT
- HEAD OF AGENCY
- INFORMATION OWNER OR STEWARD (OR SYSTEM OWNER)
- MISSION OR BUSINESS OWNER
- RISK EXECUTIVE ACCOUNTABLE OFFICIAL FOR RISK MANAGEMENT
- SECURITY OR PRIVACY ARCHITECT
- SENIOR AGENCY INFORMATION SECURITY OFFICER
- SENIOR AGENCY OFFICIAL FOR PRIVACY
- SYSTEM ADMINISTRATOR
- SYSTEM OWNER
- SYSTEM SECURITY OR PRIVACY ENGINEER
- SYSTEM SECURITY OR PRIVACY OFFICER
- USER

https://csrc.nist.gov/csrc/media/Projects/risk-management/documents/Additional%20Resources/NIST%20RMF%20Roles%20and%20Responsibilities%20Crosswalk.pdf

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

Our Roles & Related Steps – Example "SYSTEM SECURITY OR PRIVACY ENGINEER



NIST RMF Quick Start Guide
Roles and Responsibilities Crosswalk

ROLE	P	C	S	I	A	R	M	ORG	SYS	RESPONSIBILITIES
SYSTEM SECURITY OR PRIVACY ENGINEER			X						X	• Provide advice in describing the system and its functions, information types, operating environments, and security and privacy requirements • Review the adequacy of the controls and their ability to protect the system and its information, manage privacy risk, and ensure compliance with applicable privacy requirements • Assist in tailoring the controls
				X					X	• Ensure the confidentiality, integrity, and availability of the system by designing and implementing a secure system • Ensure system compliance with privacy requirements and management of the privacy risks to individuals associated with the processing of PII • Implement secure and privacy-enhancing networking and computing environments • Provide security and privacy planning to support the system • Implement security and privacy requirements for the proper handling of data within the system • Recommend system-level solutions to resolve security and privacy requirements • Coordinate the most effective way to implement common controls in organizational systems
					X				X	• Verify that the system protects individual's privacy and against identified • Review and analyze security and privacy assessment reports • Design remediation plan • Verify remediation
							X		X	• Provide advice on the continuous monitoring of the system • Provide advice on the impacts of system changes to the security and privacy posture of the system • Participate in the configuration management process • Participate in any acquisition/development activities that are required to implement a system change • Implement approved system changes

Steps—P: Prepare; **C**: Categorize; **S**: Select; **I**: Implement; **A**: Assess; **R**: Authorize; **M**: Monitor. **Responsibility—ORG**: Organizational; **SYS**: System

P: Prepare (step)

C: Categorize (step)

S: Select (step)

I: Implement (step)

A: Assess (step)

R: Authorize (step)

M: Monitor (step)

ORG: Organizational (responsibility)

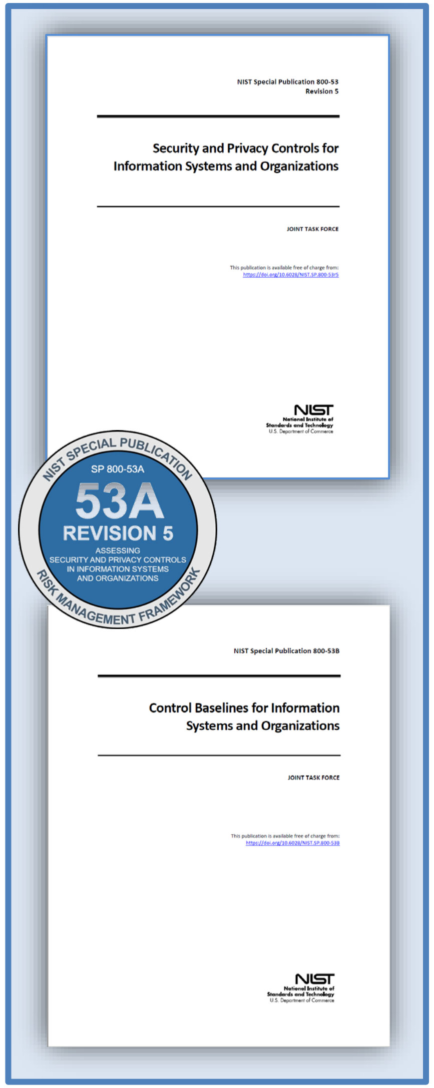
SYS: System (responsibility)

Dig Deeper –> Learn about Role-Based RMF

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

NIST Special Publication 800-53 is a Control Catalog

EnterpriseGRC Solutions, Inc.



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for
Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-53B

Control Baselines for Information
Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53B

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

The National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 5, **Security and Privacy Controls for Information Systems and Organizations**, is the control catalog used for Federal and Non-Federal information technology.

SP 800-53, the standard, is meant for use by any organization and is required by law for anyone who works with US Federal Information Systems.

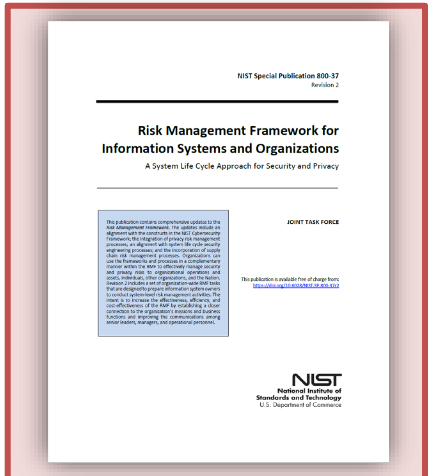
> *Take away: NIST 800-53 is a **catalog** of **security** and **privacy controls** representing **recommended security practices** primarily for federal, but also for nonfederal information systems.*

NIST SP 800-53 represents the Select, Assess, and Authorize steps in the six phases of the NIST Risk Management Framework, (NIST RMF)

> *Take away: NIST RMF includes selecting NIST 800-53 controls and assessing with 800-53A, two steps in the Risk Management Framework (RMF), as authorized by 800-53B (FedRAMP)*

NIST SP 800-53 r5 second part, the 800-53B Control Baselines for Information Systems and Organizations, represents the assurance process used to assess compliance. The implementation of the FIPS PUB 199 establishes baselines.

> *Take away: NIST 800-53B is the set of Baselines used to establish confidence in the effectiveness of controls as required for systems categorized as low, moderate, or high. The process to categorize systems is the FIPS PUB 199.*



NIST Special Publication 800-37
Revision 2

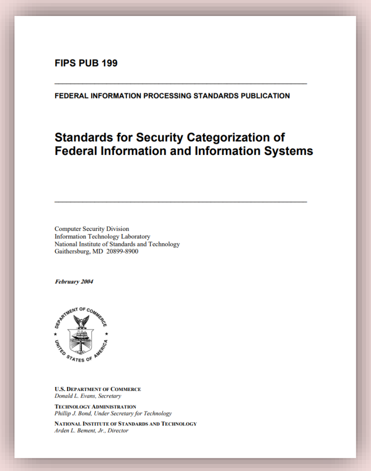
Risk Management Framework for
Information Systems and Organizations
A System Life Cycle Approach for Security and Privacy

This publication contains comprehensive updates to the *Risk Management Framework*. The updates include an alignment with the constructs in the NIST Cybersecurity Framework; the integration of privacy risk management processes; an alignment with system life cycle security engineering processes; and the incorporation of supply chain risk management processes. Organizations can use the frameworks and processes in a complementary manner within the RMF to effectively manage security and privacy risks to organizational operations and assets, individuals, other organizations, and the Nation. Revision 2 includes a set of organization-wide RMF tasks that are designed to prepare information system owners to conduct system-level risk management activities. The intent is to increase the effectiveness, efficiency, and cost-effectiveness of the RMF by establishing a closer connection to the organization's missions and business functions and improving the communications among senior leaders, managers, and operational personnel.

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-37r2

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of
Federal Information and Information Systems

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

February 2004

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

Can you categorize?

EnterpriseGRC Solutions, Inc.

The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on **information access and disclosure**, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]			
Integrity Guarding against improper information **modification or destruction** and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]			
Availability Ensuring timely and reliable **access** to and use of information. [44 U.S.C., SEC. 3542]			

The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

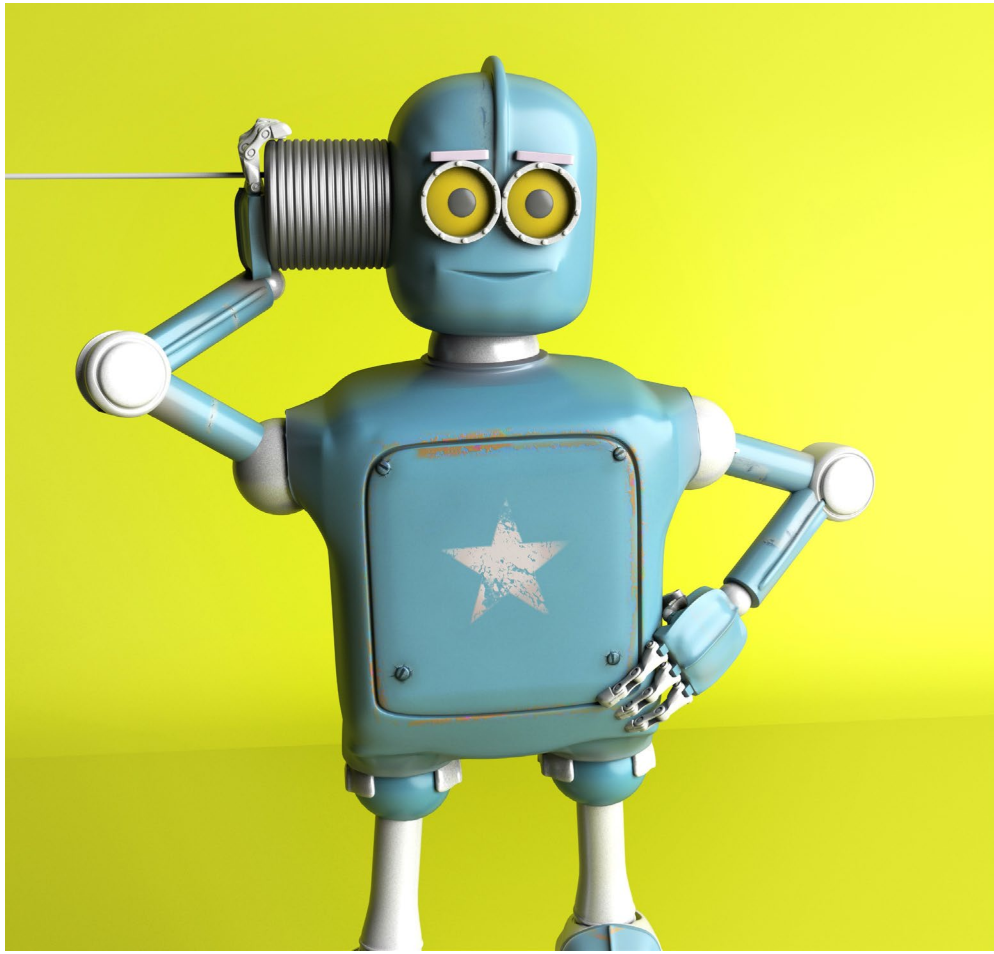
The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

The disruption of access t
information or an inform
could be expected to hav
or catastrophic adverse e
organizational operation
organizational assets, or i

Assess and Monitor with SP 800-53A



- SP 800-53A is a companion guideline to [SP 800-53] Security and Privacy Controls for Systems and Organizations. Each publication provides guidance for implementing specific steps in the Risk Management Framework (RMF).
- SP 800-53 and [SP 800-53B] address the Select step of the RMF and provide guidance on security and privacy control selection (i.e., determining the controls needed to manage risks to organizational operations and assets, individuals, other organizations, and the Nation).
- SP 800-53A addresses the Assess and Monitor steps of the RMF and provides guidance on the security and privacy control assessment processes. SP 800-53A also includes guidance on how to build effective assessment plans and how to analyze and manage assessment results.

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

Assessing Security and Privacy Controls in Information Systems and Organizations. 800-53A

EnterpriseGRC Solutions, Inc.

Abstract

This publication provides a methodology and set of procedures for conducting assessments of security and privacy controls employed within systems and organizations within an effective risk management framework. The assessment procedures, executed at various phases of the system development life cycle, are consistent with the security and privacy controls in NIST Special Publication 800-53, Revision 5. The procedures are customizable and can be easily tailored to provide organizations with the needed flexibility to conduct security and privacy control assessments that support organizational risk management processes and are aligned with the stated risk tolerance of the organization. Information on building effective security and privacy assessment plans is also provided with guidance on analyzing assessment results.

Keywords

assessment; assessment plan; assurance; control assessment; FISMA; Privacy Act; privacy controls; Open Security Controls Assessment Language; OSCAL; privacy requirements; Risk Management Framework; security controls; security requirements

DOCUMENTATION

Publication:

SP 800-53A Rev. 5 (DOI)

Local Download

Supplemental Material:

Download Spreadsheet (xls)

Download Plain Text (txt)

Download CSV (other)

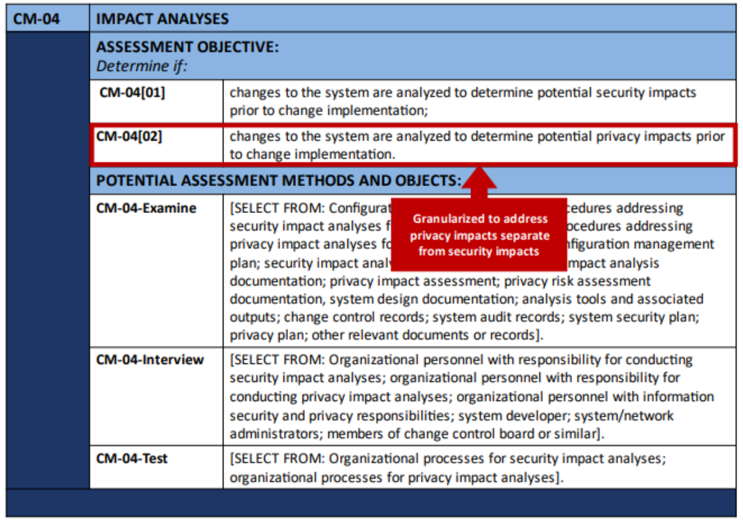
README for CSV (txt)

OSCAL GitHub (web)

Other Parts of this Publication:

SP 800-53 Rev. 5

SP 800-53B

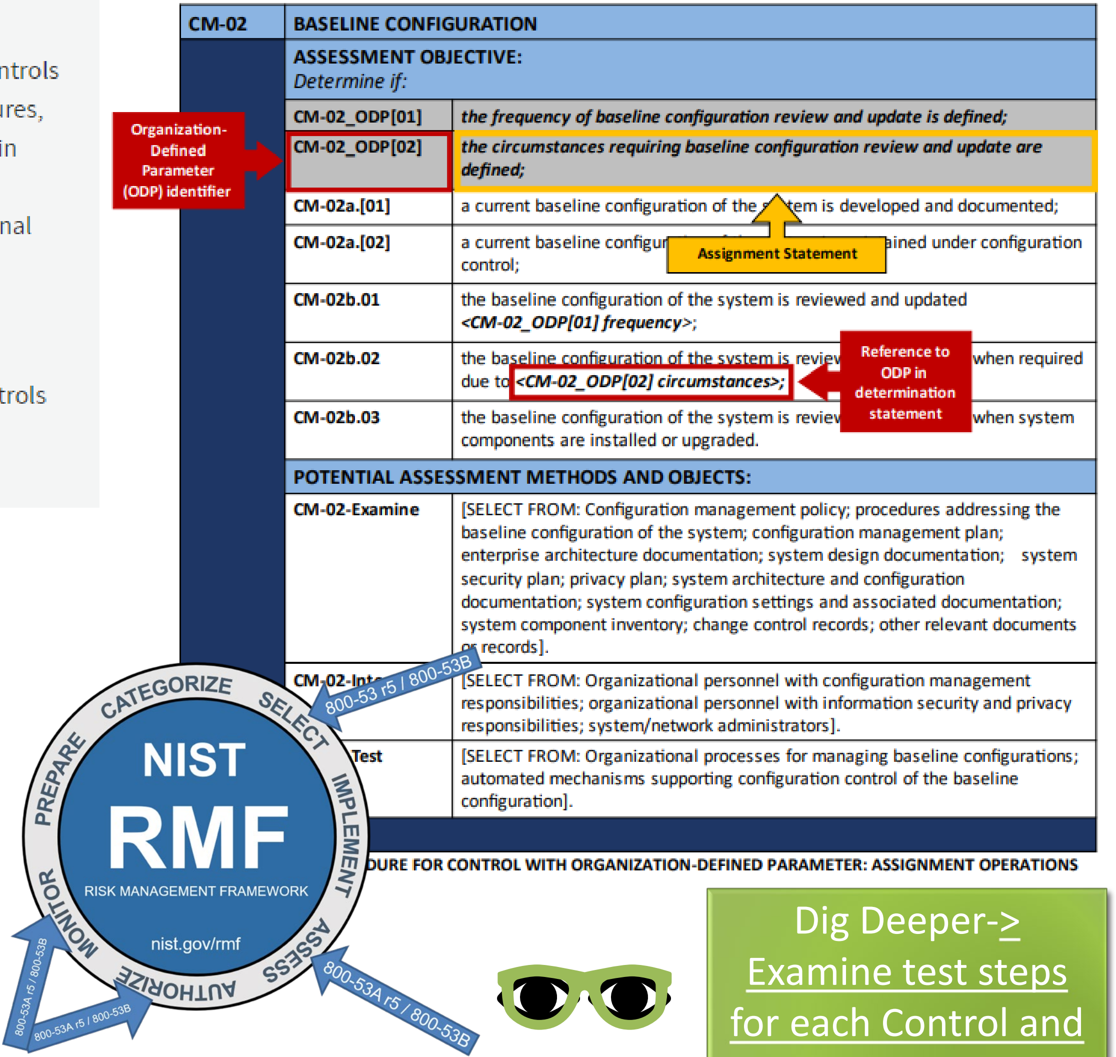


CM-04	IMPACT ANALYSES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-04[01]	changes to the system are analyzed to determine potential security impacts prior to change implementation;
	CM-04[02]	changes to the system are analyzed to determine potential privacy impacts prior to change implementation.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-04-Examine	[SELECT FROM: Configurat cedures addressing security impact analyses f ocedures addressing privacy impact analyses fo nfiguration management plan; security impact analy mpact analysis documentation; privacy impact assessment; privacy risk assessment documentation, system design documentation; analysis tools and associated outputs; change control records; system audit records; system security plan; privacy plan; other relevant documents or records].
	CM-04-Interview	[SELECT FROM: Organizational personnel with responsibility for conducting security impact analyses; organizational personnel with responsibility for conducting privacy impact analyses; organizational personnel with information security and privacy responsibilities; system developer; system/network administrators; members of change control board or similar].
	CM-04-Test	[SELECT FROM: Organizational processes for security impact analyses; organizational processes for privacy impact analyses].

Granularized to address privacy impacts separate from security impacts

FIGURE 2. ASSESSMENT PROCEDURE FOR A CONTROL FURTHER GRANULARIZED TO FACILITATE ASSESSMENT

https://csrc.nist.gov/csrc/media/Publications/sp/800-53a/rev-5/final/documents/sp800-53ar5-assessment-procedures.txt



CM-02	BASELINE CONFIGURATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-02_ODP[01]	***the frequency of baseline configuration review and update is defined;***
	CM-02_ODP[02]	***the circumstances requiring baseline configuration review and update are defined;***
	CM-02a.[01]	a current baseline configuration of the tem is developed and documented;
	CM-02a.[02]	a current baseline configur ained under configuration control;
	CM-02b.01	the baseline configuration of the system is reviewed and updated ***<CM-02_ODP[01] frequency>***;
	CM-02b.02	the baseline configuration of the system is review when required due to ***<CM-02_ODP[02] circumstances>;***
	CM-02b.03	the baseline configuration of the system is review when system components are installed or upgraded.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-02-Examine	[SELECT FROM: Configuration management policy; procedures addressing the baseline configuration of the system; configuration management plan; enterprise architecture documentation; system design documentation; system security plan; privacy plan; system architecture and configuration documentation; system configuration settings and associated documentation; system component inventory; change control records; other relevant documents or records].
	CM-02-Int	[SELECT FROM: Organizational personnel with configuration management responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	Test	[SELECT FROM: Organizational processes for managing baseline configurations; automated mechanisms supporting configuration control of the baseline configuration].

Organization-Defined Parameter (ODP) identifier

Assignment Statement

Reference to ODP in determination statement

DURE FOR CONTROL WITH ORGANIZATION-DEFINED PARAMETER: ASSIGNMENT OPERATIONS

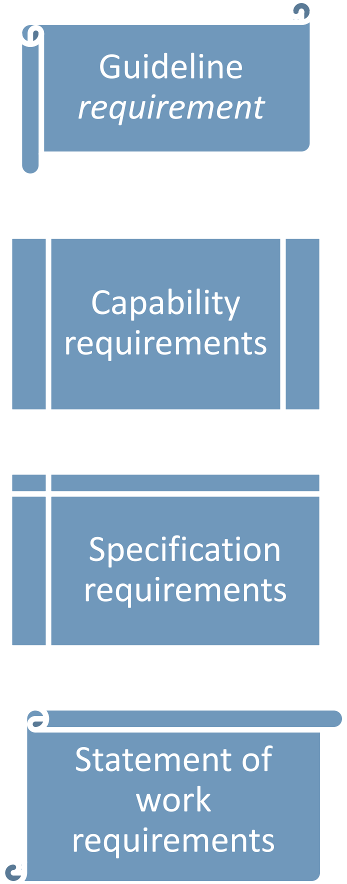
Dig Deeper-> Examine test steps for each Control and Enhancement

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

Requirements

Requirements refer to information security and privacy obligations, ranging from actual law to granular system-based expressions of stakeholder protection.

- A **guideline** requirement can reference an **expression of legal policy** as a broader set of stakeholder protections derived from those sources. When applied to a system, they determine the necessary security, privacy, and assurance **characteristics of the system**.
- **Capability** requirements describe a **capability that the system or organization must provide to satisfy a stakeholder protection** need. (Think about CSP and shared responsibility here.)
- **Specification** requirements are system requirements **particular to hardware, software, and firmware components**—capabilities that implement all or part of a control and that may be assessed (i.e., as part of the verification, validation, testing, and evaluation processes).
- **Statement of work requirements** to refer to actions that must be performed operationally or during system development.



Guideline *requirement*

Capability requirements

Specification requirements

Statement of work requirements

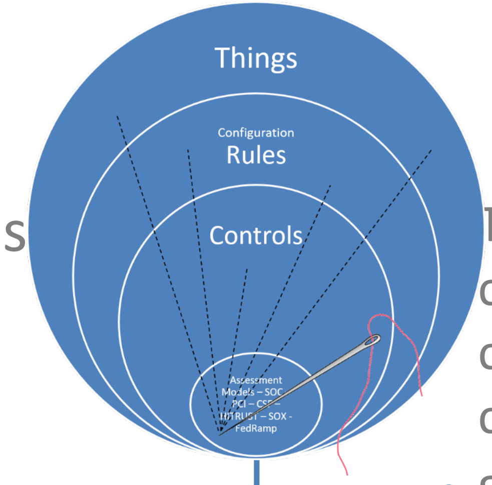
SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

Implementing: Common Controls v. System Specific

EnterpriseGRC Solutions, Inc.

Common Controls

- Common controls are capabilities such as functions or corporate policy, that extend to the entire company. For example, the company might have one common privacy policy extending to all business units, programs, and even third parties.



Hybrid or System Specific

The determination as to the appropriate control implementation approach (i.e., common, hybrid, or system-specific) is context-dependent.

- System-specific controls may include OWASP Web Security Testing Guide | OWASP Foundation, MITRE ATT&CK®, and CIS Benchmarks (cisecurity.org) to become part of a System Security Plan (SSP) and where they require a Plan of Actions and Milestones (POA&M) to keep track of findings and their remediation.

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

The implementation of control involves complex planning

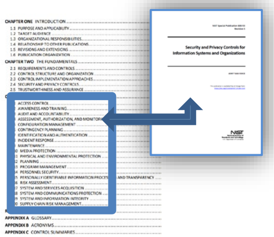
Common Control	Hybrid	System Controls
Common controls are those whose implementation results in a capability that is inheritable by multiple systems or programs. A control is deemed inheritable when the system or program receives protection from the implemented control, but the control is developed, implemented, assessed, authorized, and monitored by an internal or external entity other than the entity responsible for the system or program. The security and privacy capabilities provided by common controls can be inherited from many sources, including mission or business lines, organizations, enclaves, environments of operation, sites, or other systems or programs.	When a control is implemented as a hybrid control, the common control provider is responsible for ensuring the implementation, assessment, and monitoring of the common part of the hybrid control, and the system owner is responsible for ensuring the implementation, assessment, and monitoring of the system-specific part of the hybrid control. The determination as to the appropriate control implementation approach (i.e., common, hybrid, or system-specific) is context-dependent. The control implementation approach cannot be determined to be common, hybrid, or system-specific simply based on the language of the control. Identifying the control implementation approach can result in significant savings to organizations in implementation and assessment costs and a more consistent application of the controls organization-wide. Typically, the identification of the control implementation approach is straightforward. However, the implementation takes significant planning and coordination.	A security or privacy control for an information system that is implemented at the system level and is not inherited by any other information system. NIST SP 800-37 Rev. 2 NIST SP 800-53 Rev. 5 from OMB Circular A-130 (2016) NIST SP 800-53B from OMB Circular A-130 (2016) A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system. CNSSI 4009-2015 from NIST SP 800-53 Rev. 4 (This exists in rev 5 too) NIST SP 800-137 under System-Specific Security Control from CNSSI 4009 System-specific controls may include OWASP Web Security Testing Guide | OWASP Foundation, MITRE ATT&CK®, and CIS Benchmarks (cisecurity.org) to become part of a System Security Plan (SSP) and where they require a Plan of Actions and Milestones (POA&M) to keep track of findings and their remediation.

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

Control Families in SP 800-53 R5

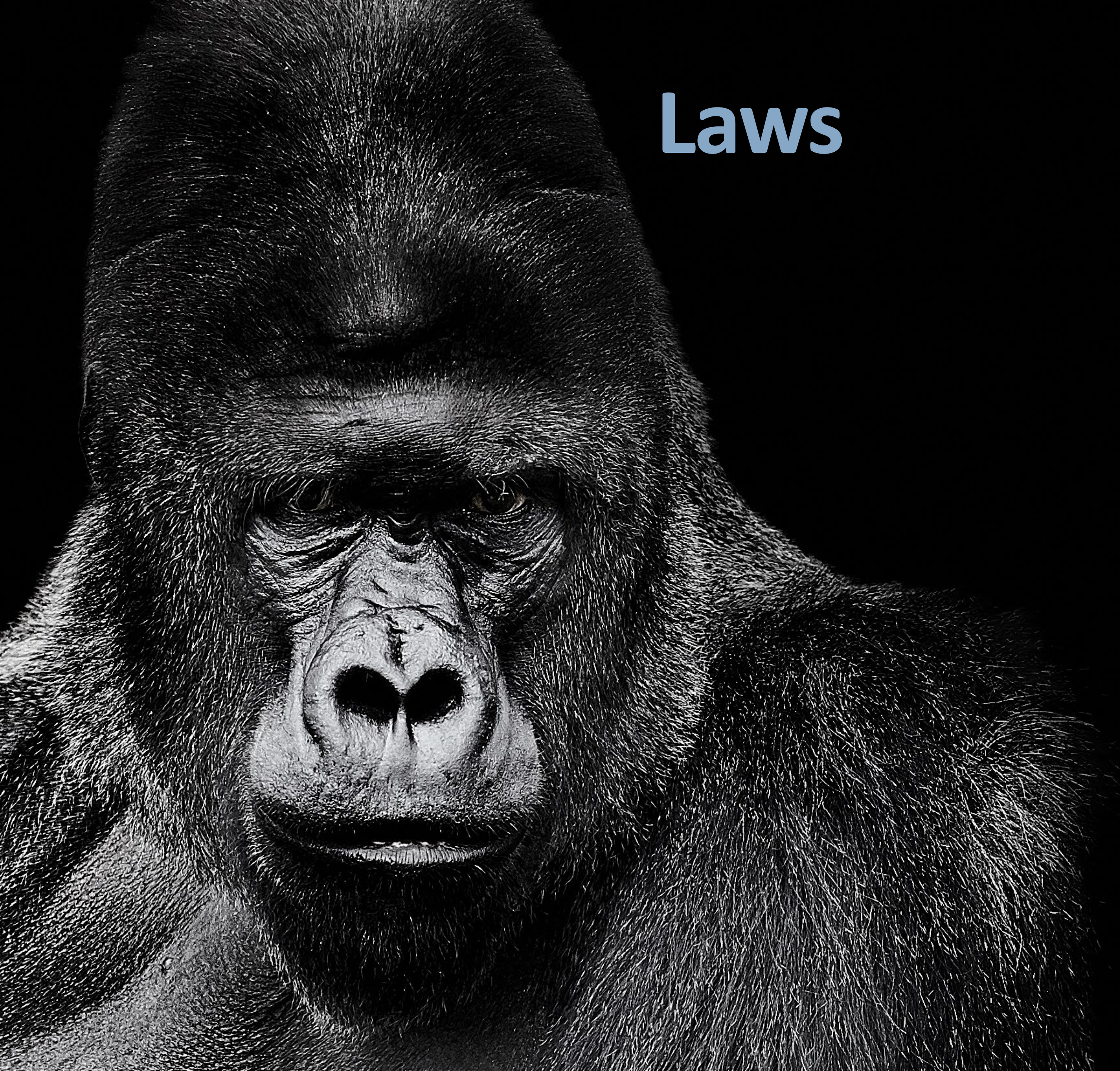
AC - ACCESS CONTROL	AT - AWARENESS AND TRAINING	AU - AUDIT AND ACCOUNTABILITY	CA - ASSESSMENT, AUTHORIZATION, AND MONITORING	CM - CONFIGURATION MANAGEMENT
CP - CONTINGENCY PLANNING	IA - IDENTIFICATION AND AUTHENTICATION	IR - INCIDENT RESPONSE	MA - MAINTENANCE	MP - MEDIA PROTECTION
PE - PHYSICAL AND ENVIRONMENTAL PROTECTION	PL - PLANNING	PM - PROGRAM MANAGEMENT	PS - PERSONNEL SECURITY	PT - PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY
RA - RISK ASSESSMENT	SA - SYSTEM AND SERVICES ACQUISITION	SC - SYSTEM AND COMMUNICATIONS PROTECTION	SI - SYSTEM AND INFORMATION INTEGRITY	SR - SUPPLY CHAIN RISK MANAGEMENT

NIST SP 800-53 r5 has 20 Control Families (Domains), 298 Controls, 709 Control Enhancements, and ~400 Supporting NISTIR, FIPS, and SP Referenced documents.
18 out of 20 “Families” derive from FIPS PUB 200. PT and SR Controls were added in NIST SP 800-53 r5 and are currently called into scope as part of the summer 2022 FedRamp v5.



SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

Laws



The US Inspector General Metrics is an example of the Government's use of NIST SP 800-53 Rev 5 as well as other NIST Products to assure compliance with US Laws & Regulations

EnterpriseGRC Solutions, Inc.

E-Government Act

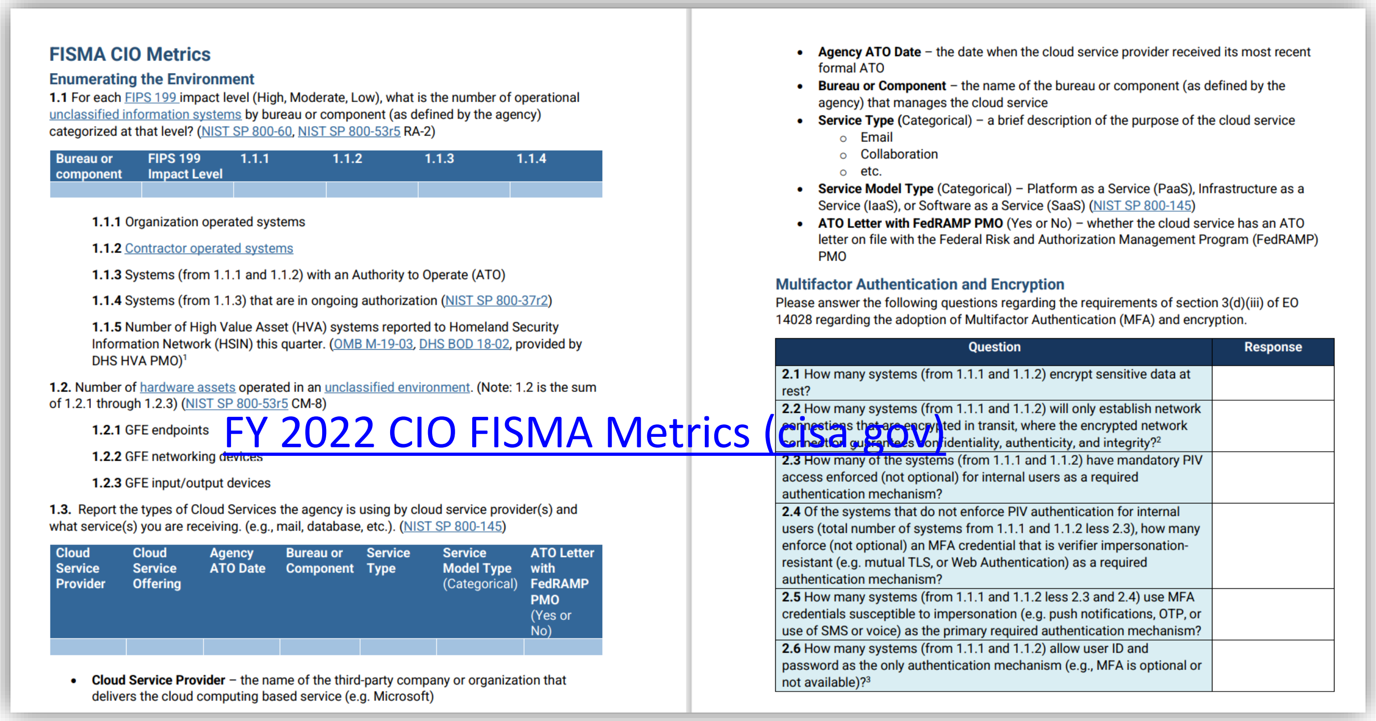
Federal Information Security Modernization Act

Homeland Security Presidential Directive 12

Homeland Security Presidential Directive 7

OMB Circular A-11

OMB Circular A-130



FISMA CIO Metrics

Enumerating the Environment

1.1 For each FIPS 199 impact level (High, Moderate, Low), what is the number of operational unclassified information systems by bureau or component (as defined by the agency) categorized at that level? (NIST SP 800-60, NIST SP 800-53r5 RA-2)

Bureau or component	FIPS 199 Impact Level	1.1.1	1.1.2	1.1.3	1.1.4

1.1.1 Organization operated systems

1.1.2 Contractor operated systems

1.1.3 Systems (from 1.1.1 and 1.1.2) with an Authority to Operate (ATO)

1.1.4 Systems (from 1.1.3) that are in ongoing authorization (NIST SP 800-37r2)

1.1.5 Number of High Value Asset (HVA) systems reported to Homeland Security Information Network (HSIN) this quarter. (OMB M-19-03, DHS BOD 18-02, provided by DHS HVA PMO)[1]

1.2. Number of hardware assets operated in an unclassified environment. (Note: 1.2 is the sum of 1.2.1 through 1.2.3) (NIST SP 800-53r5 CM-8)

1.2.1 GFE endpoints

1.2.2 GFE networking devices

1.2.3 GFE input/output devices

1.3. Report the types of Cloud Services the agency is using by cloud service provider(s) and what service(s) you are receiving. (e.g., mail, database, etc.). (NIST SP 800-145)

Cloud Service Provider	Cloud Service Offering	Agency ATO Date	Bureau or Component	Service Type	Service Model Type (Categorical)	ATO Letter with FedRAMP PMO (Yes or No)

- **Cloud Service Provider** – the name of the third-party company or organization that delivers the cloud computing based service (e.g. Microsoft)
- **Agency ATO Date** – the date when the cloud service provider received its most recent formal ATO
- **Bureau or Component** – the name of the bureau or component (as defined by the agency) that manages the cloud service
- **Service Type** (Categorical) – a brief description of the purpose of the cloud service
  - Email
  - Collaboration
  - etc.
- **Service Model Type** (Categorical) – Platform as a Service (PaaS), Infrastructure as a Service (IaaS), or Software as a Service (SaaS) (NIST SP 800-145)
- **ATO Letter with FedRAMP PMO** (Yes or No) – whether the cloud service has an ATO letter on file with the Federal Risk and Authorization Management Program (FedRAMP) PMO

Multifactor Authentication and Encryption

Please answer the following questions regarding the requirements of section 3(d)(iii) of EO 14028 regarding the adoption of Multifactor Authentication (MFA) and encryption.

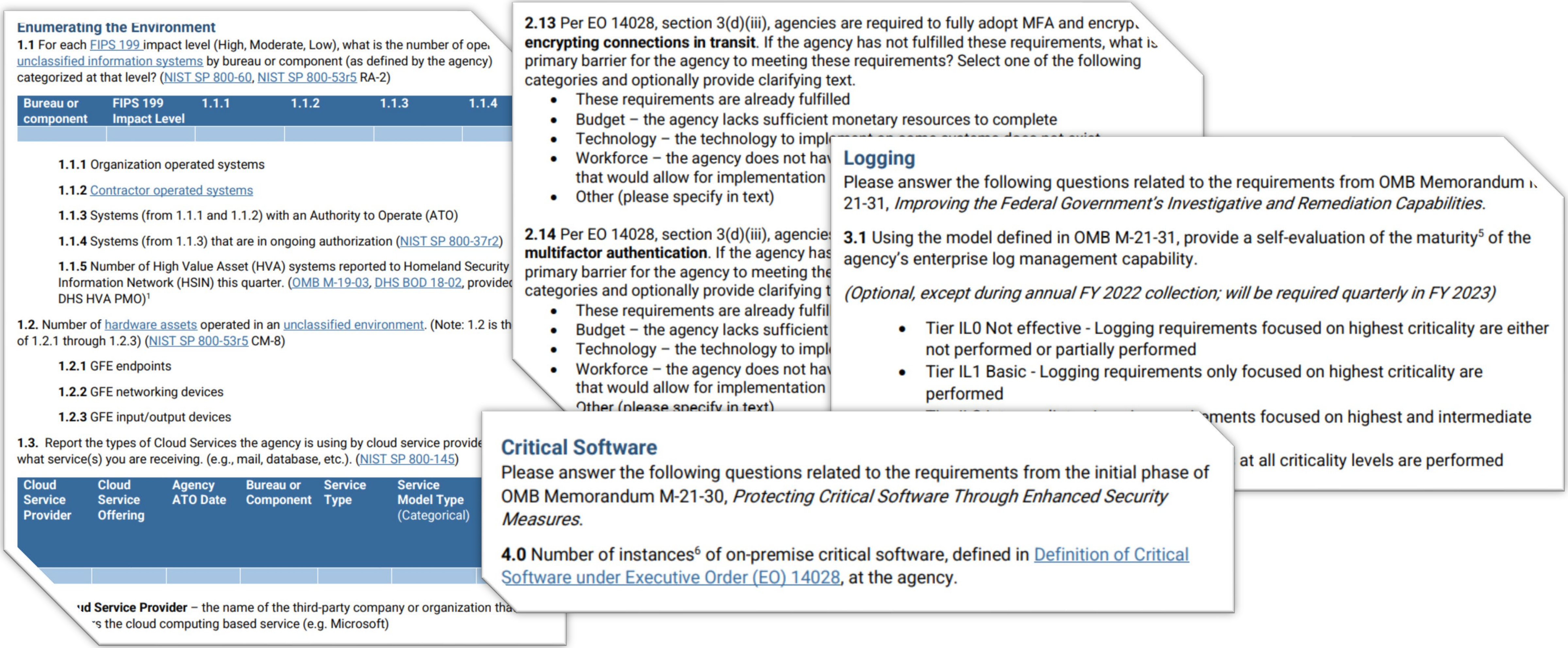
Question	Response
2.1 How many systems (from 1.1.1 and 1.1.2) encrypt sensitive data at rest?	
2.2 How many systems (from 1.1.1 and 1.1.2) will only establish network connections that are encrypted in transit, where the encrypted network connection guarantees confidentiality, authenticity, and integrity?[2]	
2.3 How many of the systems (from 1.1.1 and 1.1.2) have mandatory PIV access enforced (not optional) for internal users as a required authentication mechanism?	
2.4 Of the systems that do not enforce PIV authentication for internal users (total number of systems from 1.1.1 and 1.1.2 less 2.3), how many enforce (not optional) an MFA credential that is verifier impersonation-resistant (e.g. mutual TLS, or Web Authentication) as a required authentication mechanism?	
2.5 How many systems (from 1.1.1 and 1.1.2 less 2.3 and 2.4) use MFA credentials susceptible to impersonation (e.g. push notifications, OTP, or use of SMS or voice) as the primary required authentication mechanism?	
2.6 How many systems (from 1.1.1 and 1.1.2) allow user ID and password as the only authentication mechanism (e.g., MFA is optional or not available)?[3]	

FY 2022 CIO FISMA Metrics (cisa.gov)

Dig Deeper –> FY 2022 CIO FISMA Metrics (cisa.gov)

Some examples where measurement demonstrates a legal requirement

EnterpriseGRC Solutions, Inc.



Enumerating the Environment

1.1 For each FIPS 199 impact level (High, Moderate, Low), what is the number of ope unclassified information systems by bureau or component (as defined by the agency) categorized at that level? (NIST SP 800-60, NIST SP 800-53r5 RA-2)

Bureau or component	FIPS 199 Impact Level	1.1.1	1.1.2	1.1.3	1.1.4

1.1.1 Organization operated systems

1.1.2 Contractor operated systems

1.1.3 Systems (from 1.1.1 and 1.1.2) with an Authority to Operate (ATO)

1.1.4 Systems (from 1.1.3) that are in ongoing authorization (NIST SP 800-37r2)

1.1.5 Number of High Value Asset (HVA) systems reported to Homeland Security Information Network (HSIN) this quarter. (OMB M-19-03, DHS BOD 18-02, providec DHS HVA PMO)[1]

1.2. Number of hardware assets operated in an unclassified environment. (Note: 1.2 is th of 1.2.1 through 1.2.3) (NIST SP 800-53r5 CM-8)

1.2.1 GFE endpoints

1.2.2 GFE networking devices

1.2.3 GFE input/output devices

1.3. Report the types of Cloud Services the agency is using by cloud service provide what service(s) you are receiving. (e.g., mail, database, etc.). (NIST SP 800-145)

Cloud Service Provider	Cloud Service Offering	Agency ATO Date	Bureau or Component	Service Type	Service Model Type (Categorical)

ud Service Provider – the name of the third-party company or organization tha s the cloud computing based service (e.g. Microsoft)

2.13 Per EO 14028, section 3(d)(iii), agencies are required to fully adopt MFA and encryp **encrypting connections in transit**. If the agency has not fulfilled these requirements, what is primary barrier for the agency to meeting these requirements? Select one of the following categories and optionally provide clarifying text.

- These requirements are already fulfilled
- Budget – the agency lacks sufficient monetary resources to complete
- Technology – the technology to impl
- Workforce – the agency does not hav that would allow for implementation
- Other (please specify in text)

2.14 Per EO 14028, section 3(d)(iii), agencie **multifactor authentication**. If the agency has primary barrier for the agency to meeting the categories and optionally provide clarifying t

- These requirements are already fulfil
- Budget – the agency lacks sufficient
- Technology – the technology to impl
- Workforce – the agency does not hav that would allow for implementation
- Other (please specify in text)

Logging

Please answer the following questions related to the requirements from OMB Memorandum M 21-31, *Improving the Federal Government's Investigative and Remediation Capabilities*.

3.1 Using the model defined in OMB M-21-31, provide a self-evaluation of the maturity[5] of the agency's enterprise log management capability.

(Optional, except during annual FY 2022 collection; will be required quarterly in FY 2023)

- Tier IL0 Not effective - Logging requirements focused on highest criticality are either not performed or partially performed
- Tier IL1 Basic - Logging requirements only focused on highest criticality are performed
- ements focused on highest and intermediate
- at all criticality levels are performed

Critical Software

Please answer the following questions related to the requirements from the initial phase of OMB Memorandum M-21-30, *Protecting Critical Software Through Enhanced Security Measures*.

4.0 Number of instances[6] of on-premise critical software, defined in Definition of Critical Software under Executive Order (EO) 14028, at the agency.

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

Noteworthy Standards and Regulations in Assessment, Authorization, and Monitoring

- NIST SP 800-100, Information Security Handbook: A Guide for Managers
- An Introduction to Privacy Engineering and Risk Management in Federal Systems (nist.gov)
- Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment (nist.gov)
- NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (nist.gov)`
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- An Introduction to Information Security (nist.gov)
- OMB Circular A130 (whitehouse.gov)

Different roles require different types of guidance. The Assess, Authorization, and Monitor steps of the RMF address these responsibilities as they apply to the capabilities expected for each of these roles. Question: Which of these documents seems most suited to you?

Confidentiality – Integrity – Availability - Privacy

PM PROGRAM MANAGEMENT

PM - PROGRAM MANAGEMENT

FISMA, The Privacy Act, and OMB A-130 require federal agencies to develop, implement, and provide oversight for organization-wide information security and privacy programs to help ensure the confidentiality, integrity, and availability of federal information processed, stored, and transmitted by federal information systems and to protect individual privacy.

Program management (PM) controls are implemented at the organization level and not directed at individual information systems. The PM controls and facilitates organizational compliance with applicable federal laws, executive orders, directives, policies, regulations, and standards.

The PM controls are independent of [FIPS 200] impact levels and, therefore, are not associated with the control baselines described in the SP 800-53B.

Organizations document program management controls in the information security and privacy program plans.

The organization-wide information security program plan (see PM-1) and privacy program plan (see PM-18) supplement system security and privacy plans (see PL-2) developed for organizational information systems. Together, the system security and privacy plans for the individual information systems and the information security and privacy program plans cover the totality of security and privacy controls employed by the organization.

- FISMA PUBL283.PS (congress.gov)
- The Privacy Act of 1974 - PRIVACT STATUTE (govinfo.gov)
- NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems
- Assessing Information Security Continuous Monitoring (ISCM) Programs
- NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- OMB Circular A130 (whitehouse.gov)

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

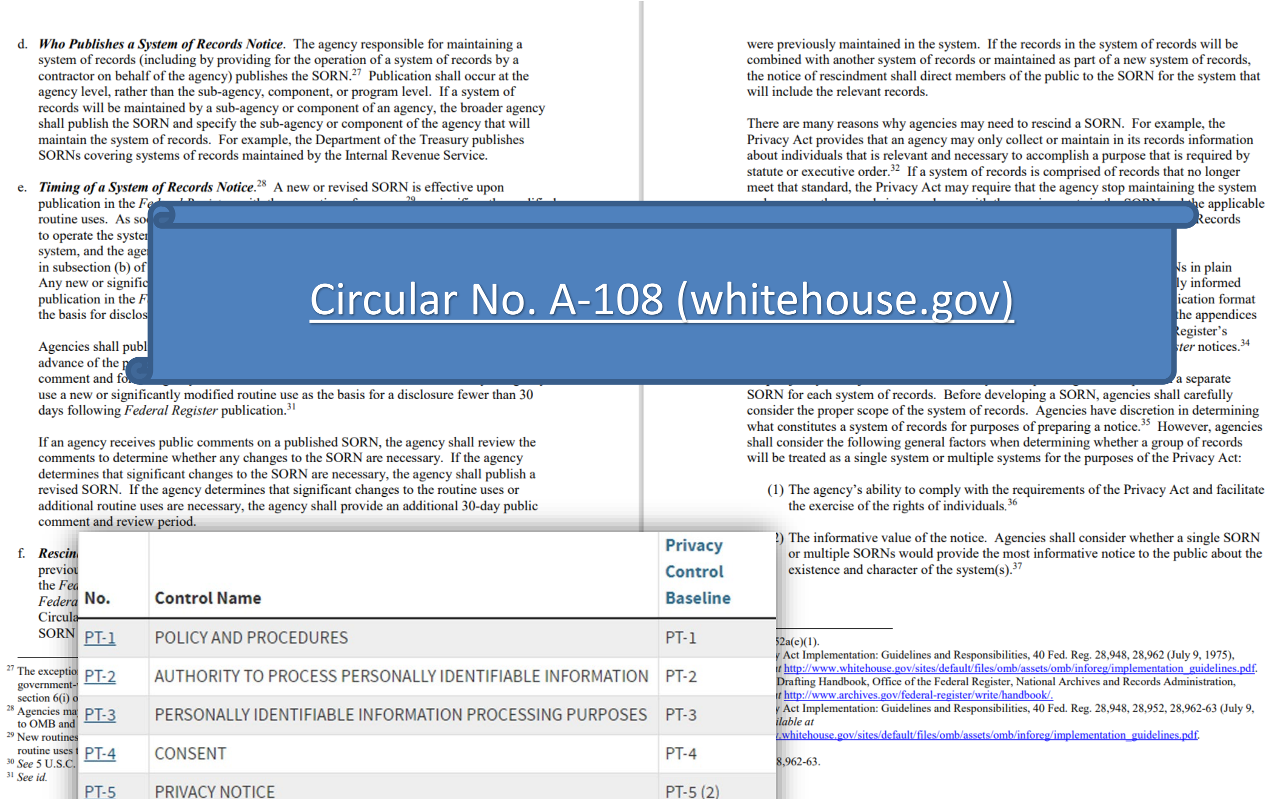
PT Personally Identifiable Information Processing and Transparency

PT - PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY

Personally Identifiable Information Processing and Transparency (PT): is a new Revision five control family, replacing the entire of Appendix J controls from 800-53 r4. The 800-53 r5 assigns an adds a fourth Baseline for Privacy and assigning 97 controls and enhancements as necessary to meeting current Privacy obligations.

PT controls enforce Privacy Regulations while mitigating risk related to Privacy breach. PT simplifies previous controls AP, AR, DI, DM, IP, SE, TR, and UL from Appendix J, replacing them with Policy and Procedure, Authority to collect PII, PII Processing, Consent, Privacy Notice, System of Records, Specific Categories of PII, and Computer matching (monitoring) requirements.

Students need to open OMB Circular No. A-108.



d. ***Who Publishes a System of Records Notice***. The agency responsible for maintaining a system of records (including by providing for the operation of a system of records by a contractor on behalf of the agency) publishes the SORN.[27] Publication shall occur at the agency level, rather than the sub-agency, component, or program level. If a system of records will be maintained by a sub-agency or component of an agency, the broader agency shall publish the SORN and specify the sub-agency or component of the agency that will maintain the system of records. For example, the Department of the Treasury publishes SORNs covering systems of records maintained by the Internal Revenue Service.

e. ***Timing of a System of Records Notice***.[28] A new or revised SORN is effective upon
publication in the *Fe*
routine uses. As so
to operate the syster
system, and the ager
in subsection (b) of
Any new or signific
publication in the *F*
the basis for disclos

Agencies shall publ
advance of the p
comment and fo
use a new or significantly modified routine use as the basis for a disclosure fewer than 30 days following *Federal Register* publication.[31]

If an agency receives public comments on a published SORN, the agency shall review the comments to determine whether any changes to the SORN are necessary. If the agency determines that significant changes to the SORN are necessary, the agency shall publish a revised SORN. If the agency determines that significant changes to the routine uses or additional routine uses are necessary, the agency shall provide an additional 30-day public comment and review period.

f. ***Rescin***
previou
the *Fed*
Federa
Circula
SORN

[27] The exceptio
government-
section 6(i) o
[28] Agencies ma
to OMB and
[29] New routines
routine uses t
[30] *See* 5 U.S.C.
[31] *See id.*

were previously maintained in the system. If the records in the system of records will be combined with another system of records or maintained as part of a new system of records, the notice of rescindment shall direct members of the public to the SORN for the system that will include the relevant records.

There are many reasons why agencies may need to rescind a SORN. For example, the Privacy Act provides that an agency may only collect or maintain in its records information about individuals that is relevant and necessary to accomplish a purpose that is required by statute or executive order.[32] If a system of records is comprised of records that no longer meet that standard, the Privacy Act may require that the agency stop maintaining the system
he applicable
Records

Ns in plain
ly informed
ication format
the appendices
Register's
ter notices.[34]

a separate SORN for each system of records. Before developing a SORN, agencies shall carefully consider the proper scope of the system of records. Agencies have discretion in determining what constitutes a system of records for purposes of preparing a notice.[35] However, agencies shall consider the following general factors when determining whether a group of records will be treated as a single system or multiple systems for the purposes of the Privacy Act:

(1) The agency's ability to comply with the requirements of the Privacy Act and facilitate the exercise of the rights of individuals.[36]

2) The informative value of the notice. Agencies shall consider whether a single SORN or multiple SORNs would provide the most informative notice to the public about the existence and character of the system(s).[37]

52a(e)(1).
y Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,948, 28,962 (July 9, 1975),
t http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf.
Drafting Handbook, Office of the Federal Register, National Archives and Records Administration,
t http://www.archives.gov/federal-register/write/handbook/.
y Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,948, 28,952, 28,962-63 (July 9,
ilable at
.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf.

8,962-63.

Circular No. A-108 (whitehouse.gov)

No.	Control Name	Privacy Control Baseline
PT-1	POLICY AND PROCEDURES	PT-1
PT-2	AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION	PT-2
PT-3	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES	PT-3
PT-4	CONSENT	PT-4
PT-5	PRIVACY NOTICE	PT-5 (2)
PT-6	SYSTEM OF RECORDS NOTICE	PT-6 (1) (2)
PT-7	SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION	PT-7 (1) (2)
PT-8	COMPUTER MATCHING REQUIREMENTS	PT-8

Dig deeper?

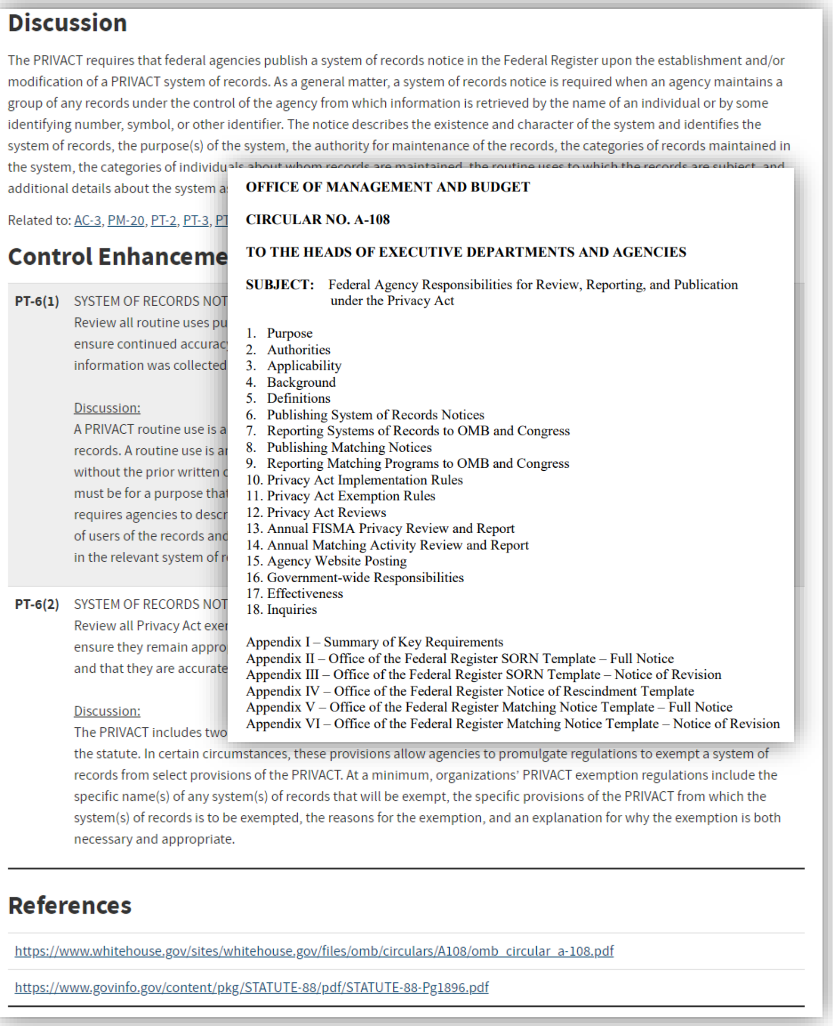
SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

PII Processing and Transparency

- Authority to process and Processing Purposes consider Data Tagging and Automation. Suggested reading for this subject includes Attribute Metadata: A Proposed Schema for Evaluating Federated Attributes
- Organizations take steps to ensure that PII is processed for authorized purposes, including training personnel, monitoring, and auditing organizational PII processing.
- Organizations monitor for changes in personally identifiable information processing, consulting with the senior agency official for privacy and legal counsel to ensure that any new purposes that arise from changes in processing are compatible with the purpose for which the information was collected. If the new purpose is not compatible, personnel implement mechanisms in accordance with defined requirements to *allow* or to *prevent* the new processing.
- Mechanisms like obtaining consent from individuals, opt-in v. opt-out, revising privacy policies, or other measures to manage privacy risks that arise from changes in personally identifiable information processing purposes require specific functions in code and services, as explained in Digital Identity Guidelines (nist.gov)

Attribute Metadata: A Proposed Schema for Evaluating Federated Attributes

Digital Identity Guidelines (nist.gov)



Discussion

The PRIVACT requires that federal agencies publish a system of records notice in the Federal Register upon the establishment and/or modification of a PRIVACT system of records. As a general matter, a system of records notice is required when an agency maintains a group of any records under the control of the agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier. The notice describes the existence and character of the system and identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individu
additional details about the system a

Related to: AC-3, PM-20, PT-2, PT-3, PT

Control Enhanceme

PT-6(1) SYSTEM OF RECORDS NOT
Review all routine uses pu
ensure continued accurac
information was collected

Discussion:
A PRIVACT routine use is a
records. A routine use is a
without the prior written c
must be for a purpose tha
requires agencies to descr
of users of the records and
in the relevant system of r

PT-6(2) SYSTEM OF RECORDS NOT
Review all Privacy Act exe
ensure they remain appro
and that they are accurate

Discussion:
The PRIVACT includes two
the statute. In certain circumstances, these provisions allow agencies to promulgate regulations to exempt a system of records from select provisions of the PRIVACT. At a minimum, organizations' PRIVACT exemption regulations include the specific name(s) of any system(s) of records that will be exempt, the specific provisions of the PRIVACT from which the system(s) of records is to be exempted, the reasons for the exemption, and an explanation for why the exemption is both necessary and appropriate.

References

https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A108/omb_circular_a-108.pdf

https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf

OFFICE OF MANAGEMENT AND BUDGET

CIRCULAR NO. A-108

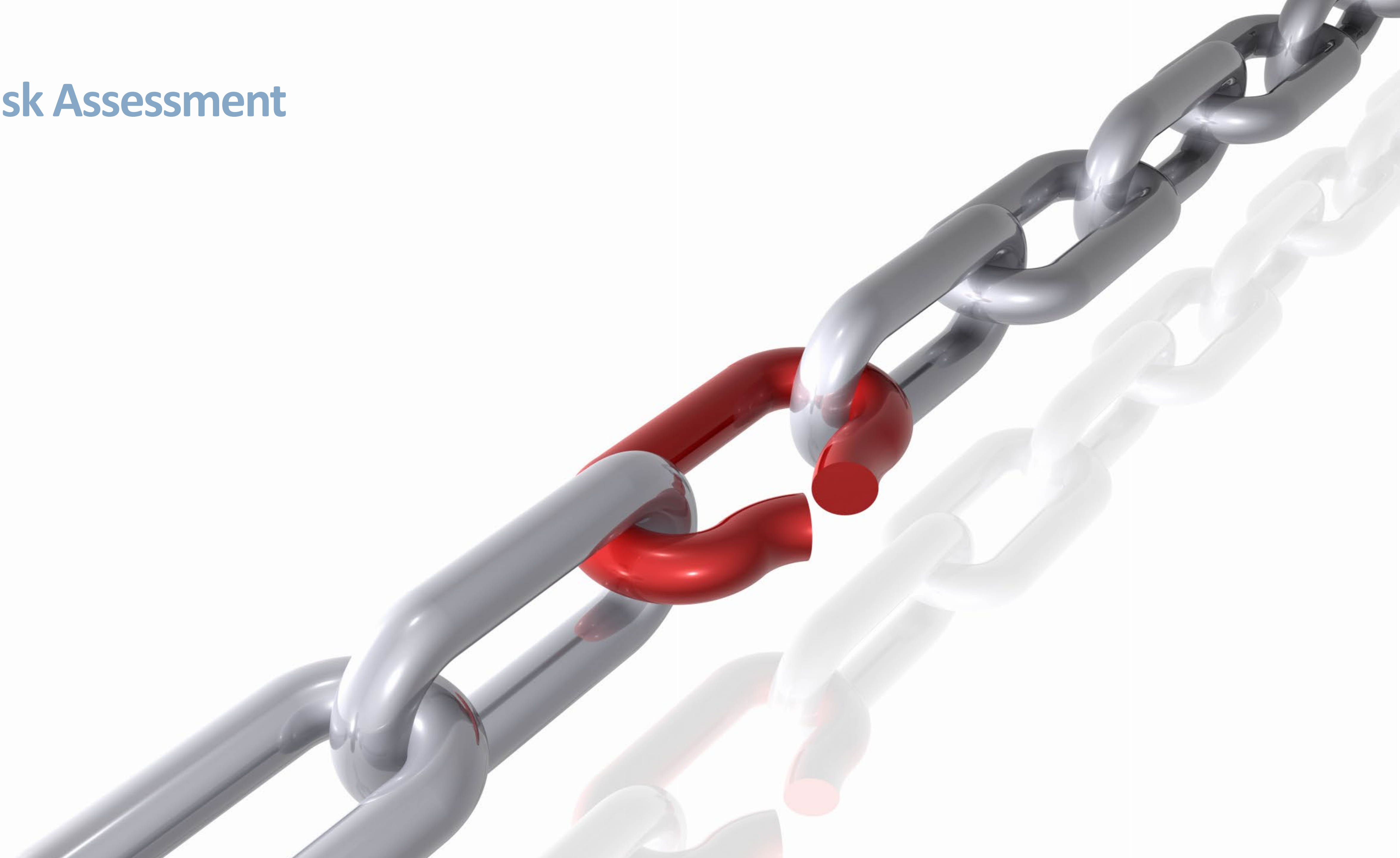
TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act

1. Purpose
2. Authorities
3. Applicability
4. Background
5. Definitions
6. Publishing System of Records Notices
7. Reporting Systems of Records to OMB and Congress
8. Publishing Matching Notices
9. Reporting Matching Programs to OMB and Congress
10. Privacy Act Implementation Rules
11. Privacy Act Exemption Rules
12. Privacy Act Reviews
13. Annual FISMA Privacy Review and Report
14. Annual Matching Activity Review and Report
15. Agency Website Posting
16. Government-wide Responsibilities
17. Effectiveness
18. Inquiries

Appendix I – Summary of Key Requirements
Appendix II – Office of the Federal Register SORN Template – Full Notice
Appendix III – Office of the Federal Register SORN Template – Notice of Revision
Appendix IV – Office of the Federal Register Notice of Rescindment Template
Appendix V – Office of the Federal Register Matching Notice Template – Full Notice
Appendix VI – Office of the Federal Register Matching Notice Template – Notice of Revision

Risk Assessment



RA-5: Vulnerability Monitoring and Scanning, and CSF Tools

EnterpriseGRC Solutions, Inc.

Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;

Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

- Enumerating platforms, software flaws, and improper configurations;
- Formatting checklists and test procedures; and
- Measuring vulnerability impact;

Analyze vulnerability scan reports and results from vulnerability monitoring;

Remediate legitimate vulnerabilities in accordance with an organizational assessment of risk;

Share information obtained from the vulnerability monitoring process and control assessments with organization-defined personnel or roles to help eliminate similar vulnerabilities in other systems; and

Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned. (paraphrased) NIST Risk Management Framework | CSRC – note the removal of parameterized comments since this is purely illustrative examples.

RA-5(2): Update Vulnerabilities to Be Scanned

BASELINE(S): Low / Moderate / High

Update the system vulnerabilities to be scanned organization-defined frequency , prior to a new scan, when new vulnerabilities are identified and reported].

RA-5(3): Breadth and Depth of Coverage

Define the breadth and depth of vulnerability scanning coverage.

RA-5(4): Discoverable Information

BASELINE(S): High

Determine information about the system that is discoverable and take organization-defined corrective actions.

RA-5(5): Privileged Access

BASELINE(S): Moderate / High

Implement privileged access authorization to organization-defined system components for organization-defined vulnerability scanning activities.

RA-5(6): Automated Trend Analyses

Compare the results of multiple vulnerability scans using organization-defined automated mechanisms.

RA-5(8): Review Historic Audit Logs

Review historic audit logs to determine if a vulnerability identified in a organization-defined system has been previously exploited within an organization-defined time period.

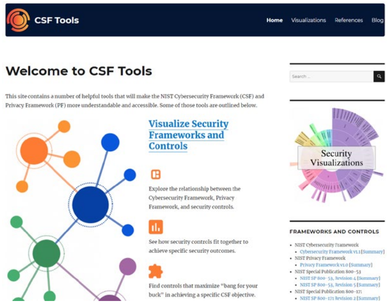
RA-5(10): Correlate Scanning Information

Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.

RA-5(11): Public Disclosure Program

BASELINE(S): Low / Moderate / High

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.



Welcome to CSF Tools

This site contains a number of helpful tools that will make the NIST Cybersecurity Framework (CSF) and Privacy Framework (PF) more understandable and accessible. Some of those tools are outlined below.

Visualize Security Frameworks and Controls

Explore the relationship between the Cybersecurity Framework, Privacy Framework, and security controls.

See how security controls fit together to achieve specific security outcomes.

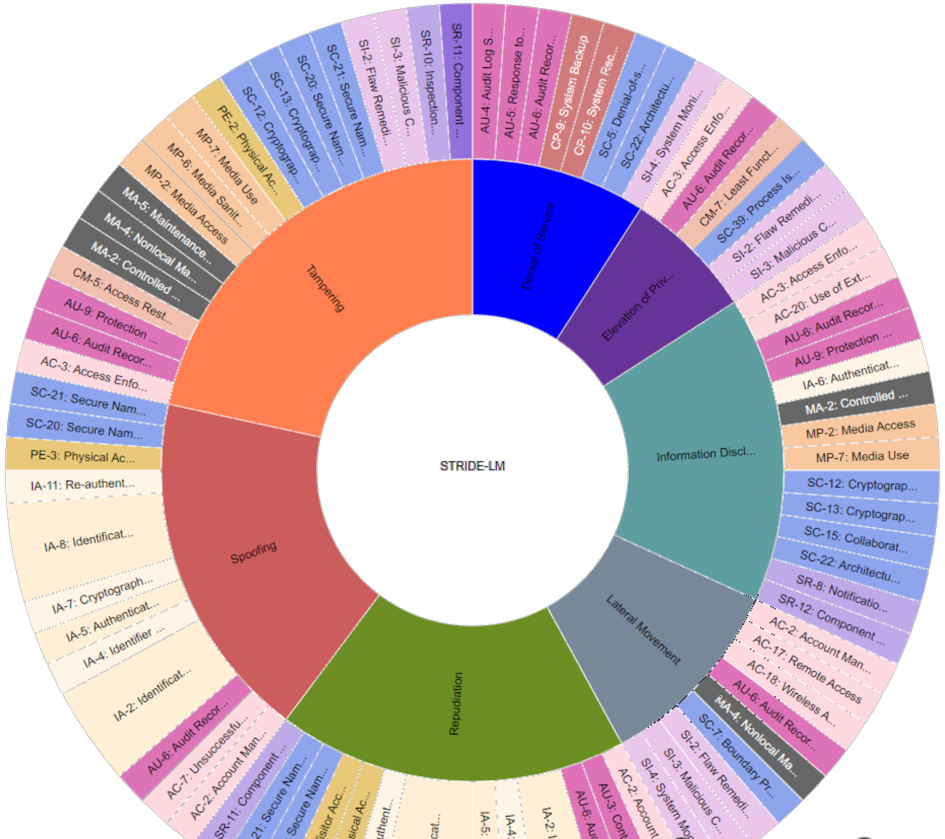
Find controls that maximize "bang for your buck" in achieving a specific CSF objective.

FRAMEWORKS AND CONTROLS

- NIST Cybersecurity Framework
  - Cybersecurity Framework v1.1 [Summary]
- NIST Privacy Framework
  - Privacy Framework v1.0 [Summary]
- NIST Special Publication 800-53
  - NIST SP 800-53, Revision 4 [Summary]
  - NIST SP 800-53, Revision 5 [Summary]
- NIST Special Publication 800-171
  - NIST SP 800-171 Revision 2 [Summary]

Let's explore NIST's CSF tools for Vulnerability Monitoring and Scanning

Introducing Lateral Movement, the Seventh Threat Classification



STRIDE-LM Threat Model

Introduction to STRIDE-LM

The process of threat modeling can be very beneficial in determining how to best protect a computer application or network. The purpose of the threat modeling is to evaluate the system from the perspective of a potential attacker, then select appropriate controls for reducing the risk of those attacks.

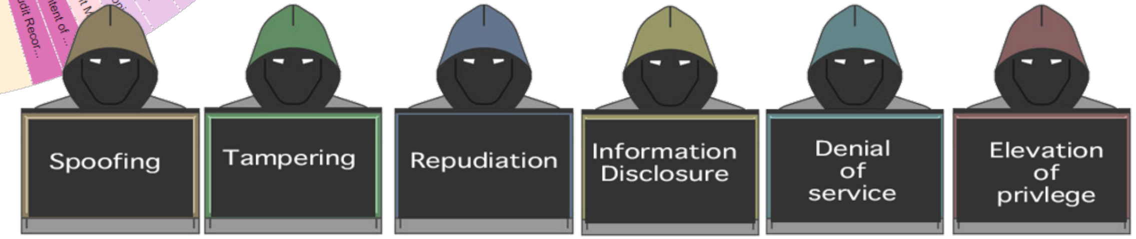
STRIDE is a popular threat model originally developed at Microsoft. It is an acronym for six classifications of threats to systems:

1. **Spoofing** – Impersonating another user or system component to obtain its access to the system
2. **Tampering** – Altering the system or data in some way that makes it less useful to the intended users
3. **Repudiation** – Plausible deniability of actions taken under a given user or process
4. **Information Disclosure** – Release of information to unauthorized parties (e.g., a data breach)
5. **Denial of Service** – Making the system unavailable to the intended users
6. **Elevation of Privilege** – Granting a user or process additional access to the system without authorization

Practitioners at Lockheed Martin noted that STRIDE was developed primarily to address engineering and development projects, rather than network defense. To make the model more applicable to the latter, they added a seventh classification:

7. **Lateral Movement** – Expanding control over the target network beyond the initial point of compromise.

STRIDE-LM Threat Model - CSF Tools



CSF 1.1 Controls mapped to RA-5

ID.RA-1: Asset vulnerabilities are identified and documented

PR.IP-12: A vulnerability management plan is developed and implemented

DE.AE-2: Detected events are analyzed to understand attack targets...

DE.CM-8: Vulnerability scans are performed

DE.DP-4: Event detection information is communicated

DE.DP-5: Detection processes are continuously improved

RS.AN-1: Notifications from detection systems are investigated

RS.MI-3: Newly identified vulnerabilities are mitigated or documented...

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

SA SYSTEM AND SERVICES ACQUISITION

SA - SYSTEM AND SERVICES ACQUISITION

Control Family Objective

System and Services Acquisition (SA): Organizations must:

(i) allocate sufficient resources to adequately protect organizational information systems;

(ii) employ system development life cycle processes that incorporate information security considerations;

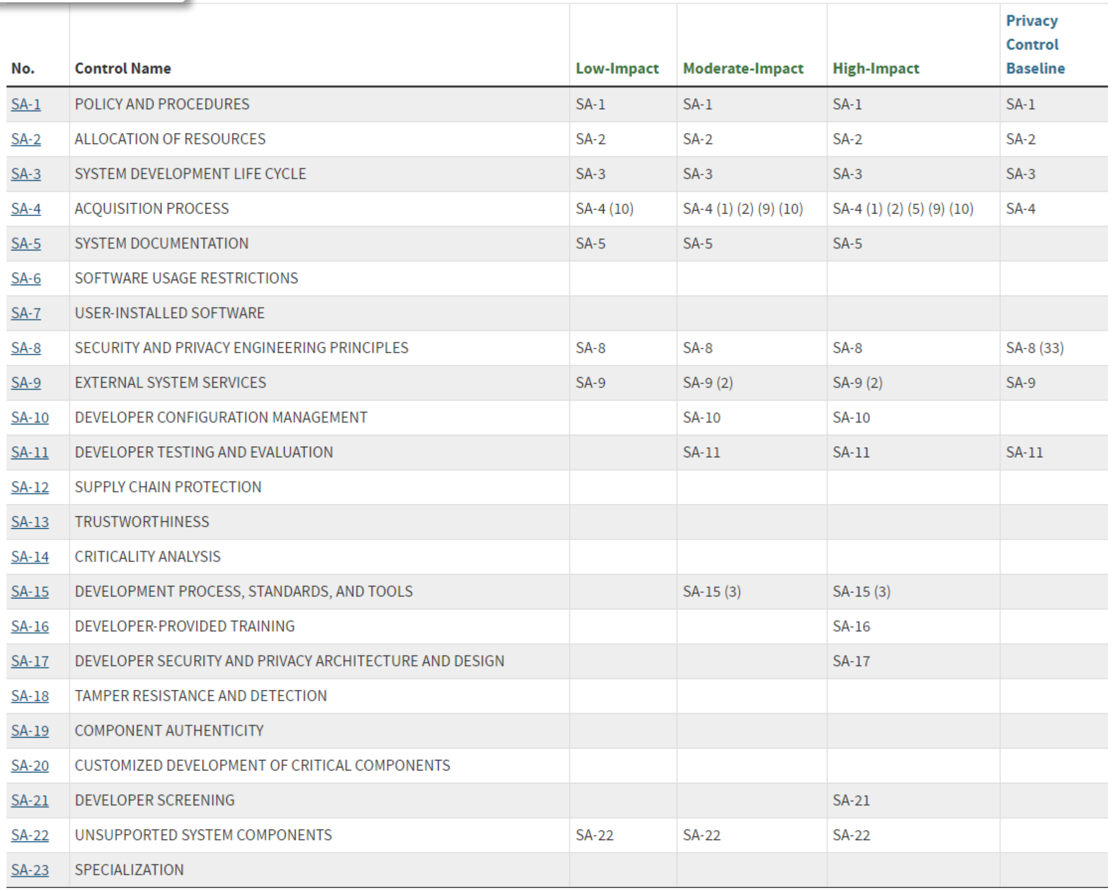
(iii) employ software usage and installation restrictions; and

(iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

SA controls have increased and been rated as having greater importance since the SP 800-53 r4. With 800-53B revision 5 soon to release, 17 controls join the moderate baseline, and factoring heavily we find SA-8 Security and Privacy Engineering Principles. Also note that 7 System and Service Acquisition controls are in the Privacy Baseline.

We will dig deeper into SA-8.

Base Control



No.	Control Name	Low-Impact	Moderate-Impact	High-Impact	Privacy Control Baseline
SA-1	POLICY AND PROCEDURES	SA-1	SA-1	SA-1	SA-1
SA-2	ALLOCATION OF RESOURCES	SA-2	SA-2	SA-2	SA-2
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	SA-3	SA-3	SA-3	SA-3
SA-4	ACQUISITION PROCESS	SA-4 (10)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (5) (9) (10)	SA-4
SA-5	SYSTEM DOCUMENTATION	SA-5	SA-5	SA-5	
SA-6	SOFTWARE USAGE RESTRICTIONS				
SA-7	USER-INSTALLED SOFTWARE				
SA-8	SECURITY AND PRIVACY ENGINEERING PRINCIPLES	SA-8	SA-8	SA-8	SA-8 (33)
SA-9	EXTERNAL SYSTEM SERVICES	SA-9	SA-9 (2)	SA-9 (2)	SA-9
SA-10	DEVELOPER CONFIGURATION MANAGEMENT		SA-10	SA-10	
SA-11	DEVELOPER TESTING AND EVALUATION		SA-11	SA-11	SA-11
SA-12	SUPPLY CHAIN PROTECTION				
SA-13	TRUSTWORTHINESS				
SA-14	CRITICALITY ANALYSIS				
SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS		SA-15 (3)	SA-15 (3)	
SA-16	DEVELOPER-PROVIDED TRAINING			SA-16	
SA-17	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN			SA-17	
SA-18	TAMPER RESISTANCE AND DETECTION				
SA-19	COMPONENT AUTHENTICITY				
SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS				
SA-21	DEVELOPER SCREENING			SA-21	
SA-22	UNSUPPORTED SYSTEM COMPONENTS	SA-22	SA-22	SA-22	
SA-23	SPECIALIZATION				

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

Deep Dive into SA-8 in CSRC Control Family System and Services Acquisition Family

Let's observe the control chart to the right, the column headers referencing scoped Control ID and Control Enhancement ID as assigned to the SP 800-53B FedRamp Assessment using the FIPS 199 to determine their Baselines for Low Impact, Medium Impact, or High Impact, and for inclusion in the Privacy Baseline.
The CSRC online record SA-8 Security and Privacy Engineering Principles exists in all Baselines but only one of the thirty-three enhancements is associated with evidence collected for the Privacy Baseline, SA-8(33).

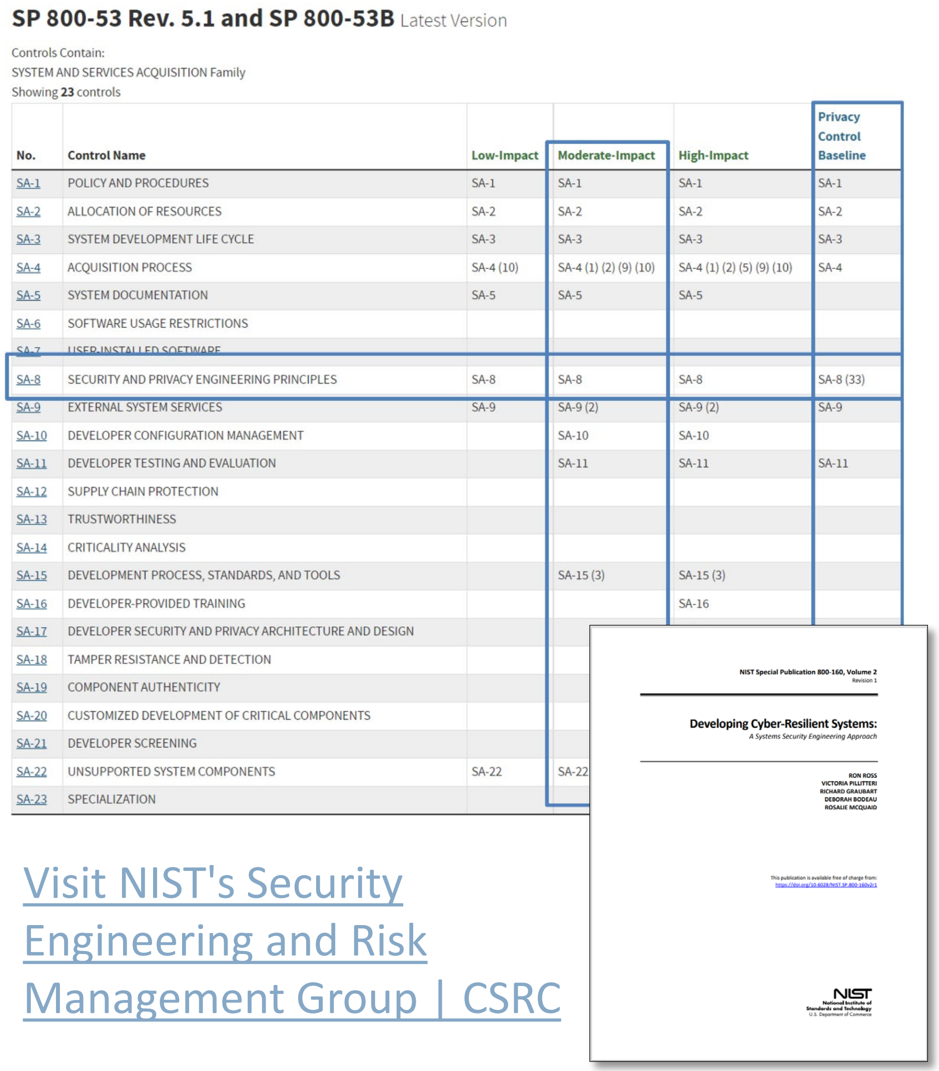
Neglecting enhancements SA-8(1) through (32) is a mistake for anyone hoping to reach sufficient maturity to release a cloud product, however that effort would not be part of a FedRAMP assessment.

Building these tasks into a "Shift Left" approach would avoid future problems since we know software vendors will need them to meet the new Executive Order 14028. (Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028)

SA-8 is part of the SaaS development lifecycle and includes the stages *specification, design, development, implementation,* and *modification*. One can imagine the difficulty in deciding when and how to tag Cloud Product lifecycle tasks. Many of these enhancements are met through the enforcement of other non-NIST frameworks such as OWASP, CIS Benchmarks, or MITRE ATT&CK® framework.

Each major System undergoes its own control review. Each system has its own Software Bill of Materials (SBOM), and each component of the system is part of an inventory. When your DCMA (Government Contract Administrator) requests further evidence of your SBOMB and all associated POA&M and SSP for your cloud offering, the type of reporting provided in SD Elements from Security Compass is essential.

BTW, We're not done with this deep dive.



SP 800-53 Rev. 5.1 and SP 800-53B Latest Version

Controls Contain:
SYSTEM AND SERVICES ACQUISITION Family
Showing **23** controls

No.	Control Name	Low-Impact	Moderate-Impact	High-Impact	Privacy Control Baseline
SA-1	POLICY AND PROCEDURES	SA-1	SA-1	SA-1	SA-1
SA-2	ALLOCATION OF RESOURCES	SA-2	SA-2	SA-2	SA-2
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	SA-3	SA-3	SA-3	SA-3
SA-4	ACQUISITION PROCESS	SA-4 (10)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (5) (9) (10)	SA-4
SA-5	SYSTEM DOCUMENTATION	SA-5	SA-5	SA-5	
SA-6	SOFTWARE USAGE RESTRICTIONS				
SA-7	USER-INSTALLED SOFTWARE				
SA-8	SECURITY AND PRIVACY ENGINEERING PRINCIPLES	SA-8	SA-8	SA-8	SA-8 (33)
SA-9	EXTERNAL SYSTEM SERVICES	SA-9	SA-9 (2)	SA-9 (2)	SA-9
SA-10	DEVELOPER CONFIGURATION MANAGEMENT		SA-10	SA-10	
SA-11	DEVELOPER TESTING AND EVALUATION		SA-11	SA-11	SA-11
SA-12	SUPPLY CHAIN PROTECTION				
SA-13	TRUSTWORTHINESS				
SA-14	CRITICALITY ANALYSIS				
SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS		SA-15 (3)	SA-15 (3)	
SA-16	DEVELOPER-PROVIDED TRAINING			SA-16	
SA-17	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN				
SA-18	TAMPER RESISTANCE AND DETECTION				
SA-19	COMPONENT AUTHENTICITY				
SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS				
SA-21	DEVELOPER SCREENING				
SA-22	UNSUPPORTED SYSTEM COMPONENTS	SA-22	SA-22		
SA-23	SPECIALIZATION				

NIST Special Publication 800-160, Volume 2
Revision 1

Developing Cyber-Resilient Systems:
A Systems Security Engineering Approach

RON ROSS
VICTORIA PILLITTERI
RICHARD GRAUBART
DEBORAH BODEAU
ROSALIE MCQUAID

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-160v2r1

Visit NIST's Security Engineering and Risk Management Group | CSRC

Security and Privacy Engineering Principles – SA-8

Discussion: Systems security and privacy engineering principles are closely related to and implemented throughout the system development life cycle (see SA-3). Organizations can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades. For existing systems, organizations apply systems security and privacy engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems.

The application of systems security and privacy engineering principles helps organizations develop trustworthy, secure, and resilient systems and reduces the susceptibility to disruptions, hazards, threats, and the creation of privacy problems for individuals. Examples of system security engineering principles include: developing layered protections; establishing security and privacy policies, architecture, and controls as the foundation for design and development; incorporating security and privacy requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; tailoring controls to meet organizational needs; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk…

Related to: PL-8, PM-7, RA-2, RA-3, RA-9, SA-3, SA-4, SA-15, SA-17, SA-20, SC-, SC-3, SC-32, SC-39, SR-2, SR-3, SR-4, SR-5 (*)

SA-8(1) Clear Abstractions
SA-8(2) Least Common Mechanism
SA-8(3) Modularity and Layering
SA-8(4) Partially Ordered Dependencies
SA-8(5) Efficiently Mediated Access
SA-8(6) Minimized Sharing
SA-8(7) Reduced Complexity
SA-8(8) Secure Evolvability
SA-8(9) Trusted Components
SA-8(10) Hierarchical Trust
SA-8(11) Inverse Modification Threshold

SA-8(12) Hierarchical Protection
SA-8(13) Minimized Security Elements
SA-8(14) Least Privilege
SA-8(15) Predicate Permission
SA-8(16) Self-reliant Trustworthiness
SA-8(17) Secure Distributed Composition
SA-8(18) Trusted Communications Channels
SA-8(19) Continuous Protection
SA-8(20) Secure Metadata Management
SA-8(21) Self-analysis
SA-8(22) Accountability and Traceability

SA-8(23) Secure Defaults
SA-8(24) Secure Failure and Recovery
SA-8(25) Economic Security
SA-8(26) Performance Security
SA-8(27) Human Factored Security
SA-8(28) Acceptable Security
SA-8(29) Repeatable and Documented Procedures
SA-8(30) Procedural Rigor
SA-8(31) Secure System Modification
SA-8(32) Sufficient Documentation
SA-8(33) Minimization*

As of 2021, only SA-8(33) is part of a Privacy Baseline.

NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems

NIST.SP.800-37r2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

NIST SP 800-53Ar5 Assessing Security and Privacy Controls in Information Systems and Organizations

NIST SP 800-160v1 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

NIST SP 800-60 Volume I Revision 1, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories

NIST SP 800-60 Volume II Revision 1, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

SR SUPPLY CHAIN RISK MANAGEMENT

SR - SUPPLY CHAIN RISK MANAGEMENT

Control Family Objective

Supply chain risk management (SR): addresses the controls in the SR family as well as supply chain-related controls in other families that are implemented within systems and organizations.

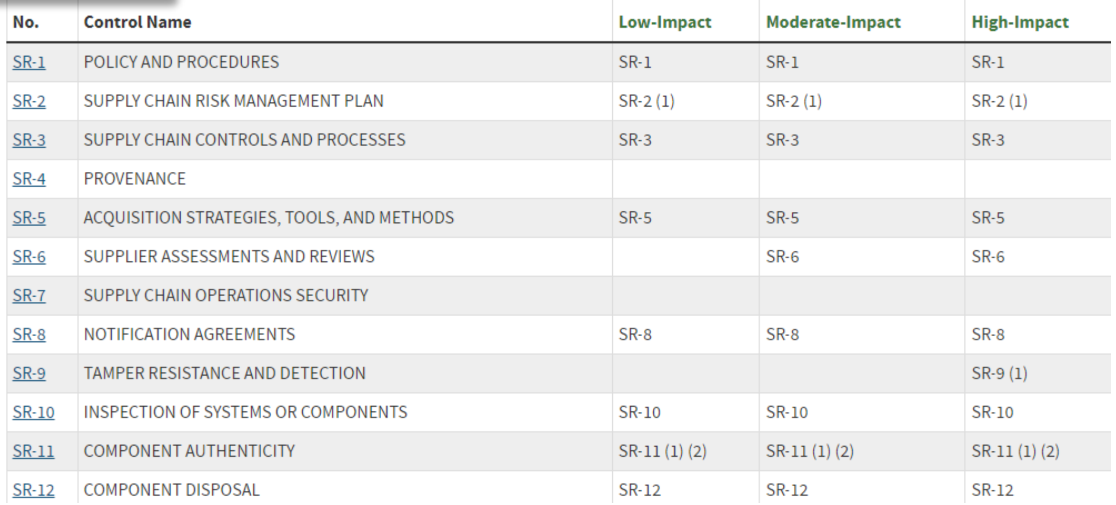
The supply chain risk management strategy, along with its security and privacy program policies and procedures are implemented at every organization level, represents multiple policies that take into consideration the complex nature of supply chain agreements, lifecycles, levels of inspection, and the current state of US regulatory requirement.

Executive Order 14028 of May 12, 2021 (Improving the Nation's Cybersecurity) puts emphasis on ICT SCRM controls. An existing framework for this control area is the Supply Chain Risk Management Practices for Federal Information Systems and Organizations (nist.gov) NIST SP 800-161. Another critical resource NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View covers the entire SCRM lifecycle and assigns all role-based responsibilities and tasks as a part of the SCRM framework.

As a new Control Family, SR was not listed in SP 800-53B however it is expected to appear in revision five, which is expected out in the spring of 2022. SR controls were listed in the 2021 IG Metrics summary.

SR Procedures describe how the policies or controls are implemented. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Base Controls



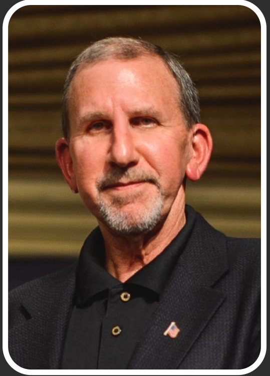
No.	Control Name	Low-Impact	Moderate-Impact	High-Impact
SR-1	POLICY AND PROCEDURES	SR-1	SR-1	SR-1
SR-2	SUPPLY CHAIN RISK MANAGEMENT PLAN	SR-2 (1)	SR-2 (1)	SR-2 (1)
SR-3	SUPPLY CHAIN CONTROLS AND PROCESSES	SR-3	SR-3	SR-3
SR-4	PROVENANCE			
SR-5	ACQUISITION STRATEGIES, TOOLS, AND METHODS	SR-5	SR-5	SR-5
SR-6	SUPPLIER ASSESSMENTS AND REVIEWS		SR-6	SR-6
SR-7	SUPPLY CHAIN OPERATIONS SECURITY			
SR-8	NOTIFICATION AGREEMENTS	SR-8	SR-8	SR-8
SR-9	TAMPER RESISTANCE AND DETECTION			SR-9 (1)
SR-10	INSPECTION OF SYSTEMS OR COMPONENTS	SR-10	SR-10	SR-10
SR-11	COMPONENT AUTHENTICITY	SR-11 (1) (2)	SR-11 (1) (2)	SR-11 (1) (2)
SR-12	COMPONENT DISPOSAL	SR-12	SR-12	SR-12

Events that precipitate an update to supply chain risk management policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. SR includes Policy and Procedures; Supply Chain Risk Management Plan; Supply Chain Controls and Processes; Provenance; Acquisition Strategies, Tools, and Methods; Supplier Assessments and Reviews; Supply Chain Operations Security; Notification Agreements; Tamper Resistance and Detection; Inspection of Systems or Components; Component Authenticity; Component Disposal

Visit Cybersecurity Supply Chain Risk Management | CSRC

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

Thanks to the NIST Risk Management Framework | CSRC Team



Ron Ross a Fellow at the National Institute of Standards and Technology. His focus areas include computer security, systems security engineering, trustworthy systems, and security risk management. Dr. Ross currently leads the NIST Systems Security Engineering Project which includes the development of standards and guidelines for the federal government, contractors, and United States critical infrastructure.

Kelley Dempsey is a Senior Information Security Specialist in the Computer Security Division at NIST. Her research and publication focus areas include information security continuous monitoring, control assessment automation, and risk management; she has co-authored a variety of publications related to information security risk management.

Eduardo Takamura is a security researcher and a member of the RMF Team at NIST. Prior to joining NIST, Eduardo supported NASA and NOAA as (FISMA) Compliance Project Manager, ISSO, ISSE, Control Assessor, System Administrator, and served in other supervisory and non-supervisory IT-related capacities. While the highlight of his 22+ year professional career in support of the federal government was his service as ISSO for a NASA mission to Mars, the opportunity to serve federal cybersecurity and privacy professionals and their supporting contractors to help them manage risks is what brings him the most professional joy and fulfillment.

Ned Goren is a security researcher and a member of the RMF (FISMA) Team at NIST. He is also the Computer Security Division security officer. Prior to joining NIST, he served as a control assessor and as an ISSO at the U.S. Census Bureau.

Rahul Mittal is an IT Specialist and a member of the RMF (FISMA) Team at NIST. During his 10+ years as a federal employee, he has served as a Security Reviewer, ISSO, CISO, and most recently Branch Chief for Compliance and Customer Engagement Support for the Office of Chief Information Officer for HHS. In this role, he interacted with Operational Divisions across the agency and helped health professionals and their supporting contractors apply security and managing risks for systems being rapidly deployed in response to the COVID-19 pandemic.

Derek Sappington is an IT Specialist (Security) and a member of the Computer Security Division in the Information Technology Laboratory at the National Institute of Standards and Technology (NIST). Prior to joining NIST, he served as a contractor at Huntington Ingalls Industries.

Jeff Brewer is a Management and Program Analyst providing key logistical support as the Secretariat for the Federal Cybersecurity and Privacy Professionals Forum and the Federal Cyber Supply Chain Risk Management Forum. Jeff serves as the Designated Federal Officer (DFO) for the Information Security and Privacy Advisory Board (ISPAB) and performs COR Level II responsibilities for numerous contracts. Jeff is inspired daily by the team's accomplishments and is happiest making things happen from behind the scenes.

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

Quiz

Question 1: Which control represents a management function designed to protect and enforce Confidentiality – Integrity – Availability – Privacy

A) PM Program Management

B) SR Supply Chain Risk Management

C) PL Planning

Answer:

Question 2: Given that there are no PT controls in any of the three baselines. Why do we still need to implement it?

A) PT controls are part of the Privacy baselines which is included at all levels of assessment.

B) PT controls are only needed when operating oversees

C) PT controls are optional

Answer:

Question 3: True or False

SC-7 System Boundary involves gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture but not subnets or DMZs.

Answer:

Question 4: True or False

SR Supply Chain Risk Management is not part of FedRAMP

Answer:

Question 5: What is the Seventh Threat Classification?

A) Logical

B) Physical

C) Lateral Movement

Answer: