Committee on National Security Systems

CNSSI 1254
August 2016

(U) RISK MANAGEMENT FRAMEWORK DOCUMENTATION, DATA ELEMENT STANDARDS, AND RECIPROCITY PROCESS FOR NATIONAL SECURITY SYSTEMS

THIS INSTRUCTION PRESCRIBES MINIMUM STANDARDS. YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER IMPLEMENTATION.

NATIONAL MANAGER

FOREWORD

1. The Committee on National Security Systems (CNSS), pursuant to its authority under National Security Directive 42 (Reference 1), is issuing this Instruction 1254, *Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems (NSS),* to prescribe the key Risk Management Framework (RMF) documentation, the associated data elements, and the RMF reciprocity process for NSS. This Instruction enables and facilitates reciprocity through standardization of required RMF core documentation and the data elements contained within each document. Adherence to this Instruction will enable leaders within organizations to make informed, risk-based decisions and foster trust among organizations, leading to the confidence needed to share information.

2. As part of the Joint Task Force (JTF) Transformation Initiative Working Group, the CNSS is working with representatives from the Civilian, Defense, and Intelligence Communities to maintain a unified information security framework. The intent of this unified framework is to improve information security, strengthen risk management processes, and encourage reciprocity among federal agencies. As a result of this collaboration, the CNSS adopts National Institute of Standards and Technology (NIST) issuances where applicable, including the following:

- NIST Special Publication (SP) 800-30, *Guide for Conducting Risk Assessments;*
- NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach;*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*;
- NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*; and
- NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans.*

3. This document will be updated as required by the CNSS.

4. Additional copies of this Instruction may be obtained from the CNSS Secretariat or the CNSS website: https://www.cnss.gov/cnss/

FOR THE NATIONAL MANAGER

/s/
Curtis W. Dukes

CNSS Secretariat (IE412). National Security Agency. 9800 Savage Road, STE 6740. Ft Meade, MD 20755-6716
Office: (410) 854-6805 Unclassified FAX: (443) 479-4700
CNSS@nsa.gov

TABLE OF CONTENTS

SECTION **PAGE**

SECTION I - PURPOSE

1. This Instruction creates a standard for data elements within RMF core documents to establish consistency and to facilitate reciprocity across the NSS community.

2. This Instruction derives the required RMF documents and standard data elements from NIST Special Publications 800-30, 800-37, 800-39, 800-53, and 800-53A.

SECTION II – AUTHORITY

3. The authority to issue this Instruction derives from National Security Directive 42, which outlines the roles and responsibilities for securing NSS consistent with applicable law, Executive Order (E.O.) 12333, *United States Intelligence Activities*, as amended, and other presidential directives. For NSS, where differences between the NIST publications and this Instruction occur, this Instruction takes precedence.

4. Nothing in this Instruction shall alter or supersede the authorities of the Director of National Intelligence.

SECTION III - SCOPE

5. This Instruction provides guidance for security authorization documentation and data elements within RMF core documents to facilitate reciprocity across the national security community. The requirements of this Instruction apply to all United States Government departments, agencies, and their contractors, consultants, and licensees who own, procure, use, operate, or maintain NSS as defined by the *Federal Information Security Modernization Act (FISMA) of 2014*. Specific requirements within this Instruction also apply to all RMF security assessment plan materials as described in NIST SP 800-53A. These requirements apply irrespective of form or generation process. While the scope of this Instruction applies primarily to systems, the RMF documentation, data elements, and reciprocity processes may be applied to other system components (e.g., hardware, software), as indicated in Annex D of this Instruction. Organizations must, however, agree on which RMF core documents and which data elements are required.

SECTION IV - POLICY

6. A standard set of documents and associated data elements are required for RMF core documents, as specified in this Instruction. The requirements established in this Instruction are necessary to facilitate reciprocity in accordance with Committee on National Security Systems Policy (CNSSP) 22, *Policy on Cybersecurity Risk Management for National Security Systems*.

7. There may be artifacts or information gathered during systems engineering processes that could inform the content of the RMF core documents. While the RMF artifacts are beneficial for providing a comprehensive security authorization package, the focus of the information should be on mission and providing that information necessary to enable decision makers to make risk-informed decisions based upon that information. This information should include operational context, architecture, data flow, interfaces, hardware, software, services, and any known risks associated with the system.

8. This Instruction does not dictate the format/templates of the documentation listed below. Organizations are encouraged to apply Security Content Automation Protocol (SCAP) standards to foster automated data sharing as stated in NIST SP 800-117, *Guide to Adopting and Using Security Content Automation Protocol (SCAP) Version 1.0*.

a. RMF CORE DOCUMENTS - The following list of RMF core documents were collected from NIST SPs (see Foreword section) and consists of:

1) System Security Plan (SSP) is a formal document that provides an overview of the security requirements for a system and describes the security controls in place or plans for meeting those requirements;

2) Security Assessment Report (SAR) provides a disciplined and structured approach for documenting the findings of the assessor and recommendations for correcting any identified vulnerabilities in the security controls;

3) Risk Assessment Report (RAR) documents the results of the risk assessment or the formal output from the process of assessing risk. The risk assessment process is outlined in NIST 800-30;

4) Plan of Action and Milestones (POA&M) identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones[1]; and

5) Authorization Decision Document conveys the final security authorization decision from the Authorizing Official (AO) to the Information System Owner (ISO) or common control provider, and other organizational officials, as appropriate.

b. RMF DATA ELEMENTS - An RMF data element is a basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Standardization of data elements documented within the RMF core documents facilitates reciprocity. These data elements may be mapped to other security documentation to avoid duplication of efforts (e.g., test and evaluation, program protection profiles, engineering documents). Annex C contains the list of data elements extracted from the NIST joint

[1] Information and data elements defined herein are consistent with and supplemental to the guidance established in Office of Management and Budget (OMB) Memo 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*.

transformation documents identified in the Foreword section that must be captured within the RMF documentation.

c. RECIPROCITY - Reciprocity is the mutual agreement among participating organizations to share and/or reuse existing data and information included within the RMF core documents in support of authorization and risk management decisions. Reciprocity is achieved through transparency by making sufficient evidence regarding the security posture of a system available to all concerned parties. The process for organizations deploying and receiving systems is listed in Annex D of this document. The RMF facilitates acceptance of existing test and assessment results and security authorization packages.

SECTION V - RESPONSIBILITIES

9. In accordance with CNSSP 22, the national security community will make documentation regarding the security posture of systems available to promote reciprocity and to assist AOs from other organizations in making credible, risk-based decisions regarding the acceptance and use of systems and the information they process, store, or transmit.

SECTION VI - REFERENCES

10. References are listed in Annex A. Future updates to referenced documents shall be applicable to this policy.

SECTION VII - DEFINITIONS

11. All terms used in this Instruction are defined in CNSSI 4009.

ANNEX A

REFERENCES

1. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, 05 July 1990.

2. Federal Information Security Modernization Act of 2014, Pub. L. 113-283 (Dec. 18, 2014).

3. Office of Management and Budget Memo 04-04, *E-Authentication Guidance for Federal Agencies*, 16 December 2003.

4. Office of Management and Budget Memo 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, 17 October 2001.

5. Committee on National Security Systems Instruction 4009, *Committee on National Security Systems (CNSS) Glossary*, 6 April 2015.

6. Committee on National Security Systems Policy 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*, 10 June 2013

7. Committee on National Security Systems Policy 22, *Policy on Cybersecurity Risk Management for National Security Systems*, August 2016.

8. Committee on National Security Systems Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, 27 March 2014.

9. NIST SP 800-30, *Guide for Conducting Risk Assessments*, September 2012.

10. NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010 (includes updates as of 05 June 2014).

11. NIST SP 800-47, *Security Guide for Interconnecting Information Technology System*, August 2002.

12. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.

13. NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (includes updates as of 22 January 2015).

14. NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, December 2014 (includes updates as of 18 December 2014).

15. NIST SP 800-60, Volume I: *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.

16. NIST SP 800-117, *Guide to Adopting and Using Security Content Automation Protocol*, July 2010.

17. NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, April 2015

18. 32 Code of Federal Regulations (CFR) Parts 2001 and 2003, *Classified National Security Information Final Rule, Information Security Oversight Office*, June 28, 2010.

ANNEX B

ACRONYMS

AO	Authorizing Official
ATO	Authorization to Operate
CFR	Code of Federal Regulations
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COTS	Commercial Off-the-Shelf
D/A	Department or Agency
DATO	Denial of Authorization to Operate
DoD	Department of Defense
DoDIN	Department of Defense Information Network
E.O.	Executive Order
FISMA	Federal Information Security Modernization Act
GOTS	Government Off-the-Shelf
IATT	Interim Authorization to Test
ISCM	Information Security Continuous Monitoring
ISO	Information System Owner
ISSM	Information System Security Manager
IT	Information Technology
JTF	Joint Task Force
NIAP	National Information Assurance Partnership
MOA	Memorandum of Agreement

MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NSS	National Security System
OMB	Office of Management and Budget
OSS	Open Source Software
PKI	Public Key Infrastructure
PM	Program Manager
POA&M	Plan of Action and Milestones
POC	Point of Contact
RAR	Risk Assessment Report
RMF	Risk Management Framework
SAR	Security Assessment Report
SCA	Security Control Assessor
SCAP	Security Content Automation Protocol
S/SCI	Secret/Sensitive Compartmented Information
SISO	Senior Information Security Officer
SLA	Service Level Agreement
SP	Special Publication
SSP	System Security Plan
SRG	Security Requirement Guide
STIG	Security Technical Implementation Guide
TS/SCI	Top Secret/Sensitive Compartmented Information

ANNEX C

ESSENTIAL DATA ELEMENTS

1. Table C-1 provides the data elements contained in an RMF core document. These data elements may be mapped to other security documentation to avoid duplication of effort (e.g., test and evaluation, program protection profiles, engineering documents). In addition, there may be artifacts or information gathered during systems engineering processes that could inform the content of the RMF core documents.

2. While the data elements below provide guidance on documenting RMF artifacts, the focus of the information should be on mission and providing that information necessary to enable decision makers to make risk-informed decisions based upon that information. This information should include operational context, architecture, data flow, interfaces, hardware, software, services, and any known risks associated with the system.

3. The following data elements are listed in alphabetical order. Columns from left to right are as follows:

a. Data Element Number – Used for tracking purposes. Departments/Agencies (D/A) are not required to use these numbers within organization-specific templates.

b. RMF Core Document(s):

1) SSP

2) SAR

3) RAR

4) POA&M[2]

5) Authorization Decision Document

c. RMF Data Element – Name of data element to be used within document(s)

d. RMF Data Element Description – Provides description of data element

e. Source – Indicates the source requiring the RMF core document and/or the RMF data element

[2] Information and data elements defined herein are consistent with and supplemental to the guidance established in OMB M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*.

Table C-1: RMF Essential Data Elements

#	RMF Core Document(s)	RMF Data Element	RMF Data Element Description	Source
Data Elements in All RMF Core Documents				
1.	SSP SAR POA&M RAR Authorization Decision Document	Data Classification Level and Handling Markings	Unclassified, Confidential, Secret, Top Secret, Secret/Sensitive Compartmented Information (S/SCI), Top Secret/Sensitive Compartmented Information (TS/SCI), SAP (Special Access Programs), Atomic Energy Act (AEA) markings, dissemination controls and other handling markings	NIST SP 800-37, 32 CFR Parts 2001 and 2003
2.	SSP SAR POA&M RAR Authorization Decision Document	Department/Agency /Organization Name	Parent or governing department/agency/organization that manages, owns, and/or controls the system	NIST SP 800-37
3.	SSP SAR POA&M RAR Authorization Decision Document	Information Technology (IT) Type	IT Type (e.g., information system: enclave, major application, platform IT system, general support systems). Indicate whether the system stand-alone or networked	NIST SP 800-37
4.	SSP SAR POA&M RAR Authorization Decision Document	Security Categorization	Categorization impact values (low, moderate, high) for security objectives (confidentiality, integrity, availability)	NIST SP 800-37, CNSSI 1253
5.	SSP SAR POA&M RAR Authorization Decision Document	Short Title for the System (e.g., System Acronym)	Provide a shortened or commonly used name or abbreviation (e.g., acronym) for the system name	NIST SP 800-37
6.	SSP SAR POA&M RAR Authorization Decision Document	System Name	Full name of the system	NIST SP 800-37

#	RMF Core Document(s)	RMF Data Element	RMF Data Element Description	Source
7.	SSP SAR POA&M RAR Authorization Decision Document	System Unique Identifier	Unique system identifier (typically a number or code, such as an IT Portfolio Management registration number). The numbering schema for the system unique identifier is organizationally defined	NIST SP 800-37
8.	SSP SAR POA&M RAR Authorization Decision Document	System Version or Release Number	Version number and release date of system	NIST SP 800-37
SSP and SAR Data Elements				
1.	SSP SAR	Operational Environment	Production, test, research and development, tactical, deployed, or other (list type of operational environment)	NIST SP 800-37
SAR, RAR, and POA&M Data Elements				
1.	SAR RAR POA&M	Assessment Date	Dates of all current security control assessments for the system	NIST SP 800-37
2.	SAR RAR POA&M	Vulnerability Identifier	A number used to track and correlate vulnerabilities that are ongoing within the organization. The numbering schema for the vulnerability identifier is organizationally defined and is organizationally derived	NIST SP 800-37
SSP Data Elements				
1.	SSP	Authorization Boundary Diagram	Diagram depicting all components of a system to be authorized for operation by an AO and excludes separately authorized systems, to which the system is connected	NIST SP 800-53
2.	SSP	Authorization Status	Authorization to Operate (ATO), ATO - with conditions, Interim Authorization to Test (IATT), Denial of Authorization to Operate (DATO), No Authorization Determination at this time	NIST SP 800-53
3.	SSP	Authorization Termination Date	If applicable, identifies the date the current authorization (ATO, IATT, and ATO with conditions) will expire	NIST SP 800-37

#	RMF Core Document(s)	RMF Data Element	RMF Data Element Description	Source
4.	SSP	Cryptographic Key Management Information	Data required to track, disseminate, and use a security key needed to secure information. All systems containing classified information must use NSA-approved encryption techniques. FIPS validated for protection of information that requires compartment access. Yes/No? FIPS validated for unclassified access. Yes/No NSA Approved Cryptographic Solution? Yes/No If not, provide cryptographic key management technology and processes	NIST SP 800-37
5.	SSP	E-Authentication Assessment/Privacy Impact Assessment	Indicate whether an E-Authentication risk assessment has been performed for the system. Yes/No	NIST SP 800-63 or OMB M-04-04
6.	SSP	External Security Services	Are external security services provided? If yes, list the provider, list the services provided, identify if services are in accordance with security requirements of the organization. Document that the necessary assurances have been obtained and the risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the use of the external services is acceptable	NIST SP 800-37
7.	SSP	Hardware/Software Inventory	Provides hardware and software inventory - individually list each component - system component inventory, assignment value: hardware inventory specifications (manufacturer, type, model, serial number), software version number, system/component owner, and for a networked component/device, the device/machine name (hostname), and (where applicable) compliance with CNSSP 11 for IA or IA-enabled products listed. Must name each component (e.g., if a system has 20 Dell servers, each must be individually identified).	NIST SP 800-37, CNSSP 11

#	RMF Core Document(s)	RMF Data Element	RMF Data Element Description	Source
8.	SSP	Internal and External System Interfaces	Include communications interfaces external to this system (to other systems). Identifies the: Name of system (or providers of the communication services); Organization; Type of communications or type of interconnection used (ports, protocols, and services); Provider(s) of the communications services; Boundaries crossed; Approval/registration status; Authorizations for interconnection; Date of agreement; and Authorization status and date. This includes any commercially provided solutions (e.g., Cloud, Application Program Interfaces)	NIST SP 800-47
9.	SSP	Network Connection Rules	Network connection rules for communicating with internal and external systems *Information from the Interconnection Agreements can be used for the description.*	NIST SP 800-37
10.	SSP	Information Type	Lists types of information processed, stored, and transmitted by the system.	NIST SP 800-60
11.	SSP	Information Flows/Paths	Identifies the information flows and paths to/from the system (including inputs and outputs)	NIST SP 800-37
12.	SSP	Mission Criticality and Mission Critical Functions	Identify if there are mission critical functions present within the system? Yes/No If yes, identify any mission critical functions supported by the system	FIPS Pub 199 or NIST SP 800-53
13.	SSP	Ownership/Operation	Indicates if the system is government-owned, government-operated; government-owned, contractor-operated; contractor-owned, contractor-operated; non-federal (state and local governments, grantees)	NIST SP 800-37
14.	SSP	Physical Environment	Describe the building composition to include the exterior wall, interior wall and ceiling compositions, the physical security provided for the building (e.g., guards, cameras, access pads), TEMPEST Accreditation or SCIF assessments may be used as validation of Physical Environment protections"	NIST SP 800-37
15.	SSP	RMF Key Roles and Corresponding Responsibilities	Member names, official titles, parent organization and contact information (e.g., phone number, email)	NIST SP 800-37

#	RMF Core Document(s)	RMF Data Element	RMF Data Element Description	Source
16.	SSP	Security Controls	List of controls after categorization, application of overlays, and any system-specific tailoring. List common/inherited controls and source of inheritance, list any Common Control Providers (CCPs), and describe the management of common and hybrid controls (controls that have both system-specific and common characteristics). Provide a short description of how each control is implemented (description can include multiple controls). Document how and at what frequency, CCPs will make compliance status of inherited controls available. Reference to the information security Continuous monitoring (ISCM) strategy should be included. Identify status of each control as implemented, planned, or not applicable. For controls identified as not applicable, provide justification. Provide a risk-based rationale for adding or removing a control (tailoring). For those controls tailored by an overlay, referencing the name of the overlay is sufficient rationale. If two overlays provide conflicting guidance, then select which overlay takes precedence and document the rationale for the decision. Also include within the list the security control number, family, and name	NIST SP 800-37 or NIST SP 800-53, CNSSI 1253
17.	SSP	Security Review Date	Indicates the date of the last annual security review for systems with an ATO.	NIST SP 800-53
18.	SSP	Software Category	Commercial off-the-shelf (COTS) Government off-the-shelf (GOTS) Open Source Software (OSS)	NIST SP 800-53
19.	SSP	System Function Description	Provide a narrative description of the system, its function, and uses. Indicate if the system is stand-alone and if it is directly or indirectly connected to the organization's enterprise network (e.g., for the DoD, the Department of Defense Information Network (DoDIN)).	NIST SP 800-37
20.	SSP	System Lifecycle Phase (numbered) or Acquisition Milestone (lettered)	1 = Material Solution Analysis 2 = Milestone-A Technology Maturation and Risk Reduction 3 = Milestone-B Engineering and Manufacturing Development 4 = Milestone-C Production and Deployment 5 = Operations and Support	NIST SP 800-37

#	RMF Core Document(s)	RMF Data Element	RMF Data Element Description	Source
			6 = Disposal	
21.	SSP	System User Categories	Description of users and their access rights and privileges for the system. Description of users (Include all that apply and the access rights and privileges for each): Organization Personnel. Contractors. Federal/State/Local. Organization. Foreign Nationals. Coalition Partners. General Public.	NIST SP 800-37
22.	SSP	User Access Requirements, Restrictions, Constraints	Description of user access requirements, restrictions, or constraints (e.g., clearance, compartment, and citizenship requirements) for access to the system. Include privileged user ID information (user's role/function)	NIST SP 800-53
SAR Data Elements				
1.	SAR	Assessment Environment	Description of the environment where the most recent testing took place, including information on the site location and security system. Identify any supporting equipment (i.e. emulators, sniffers, analyzers, traffic generators, satellite simulators) that were used to support the assessment event, and list any external interfaces active during the test event. Explain any constraints imposed by the environment on the assessment event which impacted on the quality or quantity of testing able to be performed. Identify all personnel present for the assessment, their organizations, and their role in the assessment event. Resource: test results report	NIST SP 800-53A

#	RMF Core Document(s)	RMF Data Element	RMF Data Element Description	Source
2.	SAR	Assumptions, Limitations/ Constraints, Issues	Identifies: Assumptions Limitations/Constraints (e.g., inherited controls, test environment, system configuration). Issues Any assumptions or limitations/constraints the SCA applied to the assessment of the system and any issues associated with those assumptions and limitations/constraints	NIST SP 800-53A
3.	SAR	SCA Executive Summary	Executive summary from the detailed findings that are generated during a security control assessment. An executive summary provides an AO with an abbreviated version of the assessment report focusing on the highlights of the assessment, synopsis of key findings, and/or recommendations for addressing weaknesses and deficiencies in the security controls	NIST SP 800-37
4.	SAR	SCA and Organization	Name of the SCA's organization and the SCA's contact information (name, role/title, email, phone number)	NIST SP 800-53A
5.	SAR	Type of Assessment/ Objective	Identifies developmental testing and evaluation, independent verification and validation, assessments supporting security authorizations or reauthorizations, audits, ongoing monitoring, assessments subsequent to remediation actions, etc.	NIST SP 800-53A
6.	SAR	Security Control Assessment Methodology/ Procedure	Identifies methodology and procedures used to assess controls (e.g., NIST SP 800-53A, DoD Joint Security Implementation Guide). If other methodology or procedures were used, provide rationale for deviation from standard assessment resources	NIST SP 800-53A
7.	SAR	Security Control Compliance Status	Once assessed, identify controls as satisfied, other than satisfied, not evaluated. If using agency-specific terminology, provide mapping to the above NIST compliance status terms	NIST SP 800-53A
8.	SAR	Security Control Traceability	Provides the traceability from security controls listed in the SSP to the system security requirements derived from those controls	NIST SP 800-53A
9.	SAR	Systems and/or Components Assessed	List systems (if enclave) and/or components assessed within authorization boundary	NIST SP 800-53A

#	RMF Core Document(s)	RMF Data Element	RMF Data Element Description	Source
10.	SAR	Test Results	Test results from external evaluation sources or recent test results used to verify implementation of a control for that current instance/version of the system (e.g., date of the recent test, testing resource, testing criteria and requirements used, changing conditions associated with security controls over time, degree of independence of previous assessments)	NIST SP 800-53A
RAR Data Elements				
1.	RAR	Purpose for Risk Assessment	Describe the purpose of the risk assessment. The purpose may be to determine risk at various system life cycle phases, to include the security categorization, to tailor security controls, to assess the risk of non-compliant security controls, to assess the impact of actual or proposed changes to the system in operations, etc.	NIST SP 800-30
2.	RAR	Risk Assessment POC	Risk Assessment POC contact information (e.g., name, phone number, email)	NIST SP 800-30
3.	RAR	Scope	The scope of the risk assessment can be at any of the three tiers in the risk management hierarchy (i.e., organization, mission/business process, or system), or the scope can be limited to certain portions of the system. Identify scope of assessment including boundaries and intended mission(s) the system is designed to support	NIST SP 800-30
4.	RAR	Risk Assessment Approach	Identifies the type of risk assessment methodology used (qualitative, semi-quantitative, or quantitative)	NIST SP 800-30
5.	RAR	Risk Analysis Approach	Threat-based, Vulnerability Based, or Asset Impact Based	NIST SP 800-30
6.	RAR	Organizational Risk Tolerance	Risk Tolerance (including a list of the range of consequences to be considered) –The level of risk an entity is willing to assume in order to achieve a potential desired result; Identify any organization risk tolerance levels set at Tier 1, Tier 2, and Tier 3	NIST SP 800-30
7.	RAR	Threat Sources	Identifies threat sources that could initiate the threat event	NIST SP 800-30
8.	RAR	Threat Source Capability	Indicates the adversarial threat source's capability to initiate a threat event	NIST SP 800-30

#	RMF Core Document(s)	RMF Data Element	RMF Data Element Description	Source
9.	RAR	Threat Source Intent	Indicates the adversarial threat source's intent to initiate a threat event	NIST SP 800-30
10.	RAR	Threat Source Targeting	Indicates if the adversarial threat source has historically targeted or is actively targeting the system	NIST SP 800-30
11.	RAR	Threat Event	Identifies the potential threat event	NIST SP 800-30
12.	RAR	Vulnerability or Predisposing Condition	Identifies vulnerabilities which could be exploited by threat sources and the predisposing conditions which could increase the likelihood of undesirable consequences and/or adverse impacts	NIST SP 800-30
13.	RAR	Vulnerability Severity or Pervasiveness of Predisposing Condition	Identifies the severity of vulnerabilities or the pervasiveness of the predisposing conditions as very low, low, moderate, high, very high	NIST SP 800-30
14.	RAR	Likelihood of Threat Event Initiation/Occurrence	Indicates the likelihood the threat event will be initiated or occur, taking into consideration the adversarial threat source's capability, intent, and targeting; non-adversarial threat source's historical evidence and empirical data; timeframe and frequency of event; state of the organization (e.g., environment, architecture, system, and presence/effectiveness of security controls); vulnerabilities; and predisposing conditions	NIST SP 800-30
15.	RAR	Likelihood of Threat Event Success	Determine the likelihood the threat event, once it is initiated or occurs, will result in an adverse impact, regardless of the magnitude of harm (i.e., impact)	NIST SP 800-30
16.	RAR	Overall Likelihood	Indicates the likelihood the threat event will be initiated or occur and result in adverse impact (i.e., combination of likelihood of threat event initiation/occurrence and likelihood the initiated event succeeds)	NIST SP 800-30
17.	RAR	Level of Impact	Determine the level of impact associated with the undesirable consequences of the threat event. Determine the undesirable consequences (i.e., potential harm to organizational operations, organizational assets, individuals, other organizations, or the Nation) of the threat event	NIST SP 800-30
18.	RAR	Residual Risk Level	For individual entries in the RAR, indicates the residual risk level expected after mitigations are implemented (as described in the POA&M). Identifies the risk level as one of the following: very low, low, moderate, high, and very high)	NIST SP 800-30

#	RMF Core Document(s)	RMF Data Element	RMF Data Element Description	Source
19.	RAR	Number of Controls with Risks Identified	Indicates the number of controls identified for each level of risk (i.e., very low, low, moderate, high, or very high)	NIST SP 800-30
20.	RAR	Overall Risk Posture	Describe the overall level of risk (e.g., very low, low, moderate, high, or very high) to the system, considering all individual risks, mitigating factors, environment, architecture, system's security categorization, historical evidence, etc.	NIST SP 800-30
21.	RAR	RAR Executive Summary	Executive summary from the detailed findings generated during risk assessment. An executive summary provides an AO with an abbreviated version of the risk assessment report focusing on the highlights of the assessment, purpose, synopsis of key findings, and/or recommendations for addressing risk	NIST SP 800-30
POA&M Data Elements				
1.	POA&M	Vulnerability (Weaknesses or Deficiency)	A short description of the program or system-level information security vulnerability that poses a risk of compromising confidentiality, integrity, or availability of information or the system, if applicable Contains both initial vulnerability (does not include false positives) from the SAR and the risk assessment level from the RAR	NIST SP 800-37
2.	POA&M	Short Description of Weakness or Deficiency	Sufficient detail must be provided to permit oversight and tracking	NIST SP 800-37
3.	POA&M	Event that Identified Weakness or Deficiency	Includes the event that identified the deficiency (e.g., security controls assessment, penetration test), reviewing organization, and date the weakness was identified	NIST SP 800-37
4.	POA&M	Security Control Identifier	NIST SP 800-53 security control identifier that was found to be deficient. For a security vulnerability (weakness) found by means other than a security controls assessment (e.g., vulnerability test), map the deficient function to the applicable security control	NIST SP 800-53
5.	POA&M	Comments	Used for additional detail or clarifications; must be used if there is a delay. The "Comments" column should identify obstacles and challenges to resolving the weakness not related to funding (e.g., lack of personnel or expertise or developing new system to replace legacy system)	NIST SP 800-37

#	RMF Core Document(s)	RMF Data Element	RMF Data Element Description	Source
6.	POA&M	Scheduled Completion Date	A realistic estimate of the date when the corrective action will be implemented/tested. This date should not be changed. Actual completion date should be placed in the Status field	NIST SP 800-37
7.	POA&M	Milestones with Completion Dates	Outlines the specific high-level steps to be executed in mitigating the weakness and the estimated completion date for each step. Initial milestones and completion dates should not be changed. Changes to milestones should be placed in the Changes to Milestones field	NIST SP 800-37
8.	POA&M	Changes to Milestones	New estimated date of a milestone's completion, if the original date is not met. The new date and reason for the change in milestone completion should be recorded. No changes should be made to the original estimate	NIST SP 800-37
9.	POA&M	Vulnerability (Weakness) Status	Indicates the stage or state of the vulnerability (weakness) in the corrective process cycle (Completed, Ongoing, Delayed, or Planned). The Completed status should be used only when a vulnerability (weakness) has been fully resolved and the corrective action has been tested. When listing items as "Completed," also include the date of completion in this column	NIST SP 800-37
10.	POA&M	POC	Organization or title of the position within the organization who is responsible for the mitigation of the weakness. Assigned responsible individuals may be included in the POA&M as well	NIST SP 800-37
Authorization Decision Document Data Elements				
1.	Authorization Decision Document	Authorization Decision	Indicates the type of authorization decision for the system (i.e., ATO or DATO)	NIST SP 800-37
2.	Authorization Decision Document	Authorizing Official	Includes AO signature (manual or Public Key Infrastructure (PKI)-certified digital signature). Include an explicit statement that the AO understands and accepts residual risk	NIST SP 800-37
3.	Authorization Decision Document	Authorization Date	Identify the date the authorization decision was determined	NIST SP 800-37
4.	Authorization Decision Document	Authorization Termination Date	Identify the date the authorization expires	NIST SP 800-37
5.	Authorization Decision Document	Overall Residual Risk	Includes the overall risk posture and listing the number of risks by level (i.e., very low to very high). See the RAR for detailed descriptions on each risk	NIST SP 800-37

#	RMF Core Document(s)	RMF Data Element	RMF Data Element Description	Source
6.	Authorization Decision Document	Risk Executive (Function) Input (If Provided)	The security related-considerations from the Risk Executive which the AO deems relevant and affects the final authorization decision. These considerations are viewed from organization-wide perspective with regard to the overall strategic goals and objectives in carrying out the mission and business functions. (e.g., organizational risk tolerance, organization's overall risk mitigation strategy, core mission and business requirements, dependencies among systems, ongoing risk monitoring requirements, and other types of risks not directly associated with the system or its environment of operation)	NIST SP 800-37
7.	Authorization Decision Document	System Name/Acronym	Full descriptive name of the system and acronym	NIST SP 800-37
8.	Authorization Decision Document	Terms/ Conditions for Authorization Note: *This information can only be provided, if a system is given Authorization to Operate.*	Provides a description of any specific limitations or restrictions placed on the operation of the system Example terms/conditions for authorization: *(i) the required security status reports for the system are submitted to this office every year; (ii) the vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk which is deemed unacceptable; and (iii) the system has not exceeded the maximum allowable time period between security authorizations in accordance with federal and agency policy*	NIST SP 800-37

ANNEX D

RECIPROCITY

1. Reciprocity helps ensure IT capabilities are developed and fielded rapidly and efficiently across an information enterprise. Applied appropriately, reciprocity reduces redundant testing, assessments, documentation, and the associated costs in time and resources. Organizations entering into reciprocal agreements will discuss all deviations from the data elements and resolve to both organizations' satisfaction.

2. To facilitate reciprocity, the concepts in the following paragraphs are fundamental to a common understanding:

a. Systems have only a single authorization. Multiple authorizations indicate multiple systems under separate ownership and configuration control.

b. Deploying[3] systems with authorizations are intended to be accepted into receiving organizations without adversely affecting the authorizations of either the deployed system or the receiving system or site. Configuration differences introduced by using the system in a new or different environment may require additional testing. ISOs and Program Managers (PM) of deploying systems must coordinate system security requirements with receiving organizations or their representatives early and throughout system development.

c. An authorization decision for a system cannot be made without completing the required assessments and analysis, as recorded in the security authorization package (e.g., in the SAR or RAR). Deploying organizations must provide the complete security authorization package (to include supporting artifacts) to receiving organizations.

d. The AO for a receiving system does not issue a new/additional ATO for the deployed system. However, the receiving organization updates their hosting system ATO to include any additional or modified security controls associated with hosting the deploying system. Depending on risk assessment factors of the receiving organization, the changes caused by the deployed system may change the authorization decision of the hosting system.

e. Organizations have the right to refuse participating in reciprocity with another organization, if the system's RMF core documentation is not considered complete enough to provide an informed understanding of potential or existing risks, or there would be excessive risk to the system or site, as determined by the system or site AO. Such decisions to refuse participation in reciprocity should be documented by the refusing AO, and provided, upon request, to the deploying organization's ISO or PM, AO, and organization Senior Information Security Officer (SISO), and to the refusing organization's Component SISO. Disputes should be resolved at the lowest possible level. Disputes that cannot be resolved will be raised to the next appropriate level.

[3] A deploying system is one system that is being developed for deployment within multiple receiving organizations with different AOs.

RECIPROCITY SCENARIOS

3. The following section does not represent all possible reciprocity circumstances. The cases in paragraph a through f describe the proper application of policy on reciprocity in the most frequently occurring scenarios:

a. **A new system is being developed by Organization A for deployment into Organizations B, C, D, and E.** In this scenario, Organization A, will maintain ownership and configuration control of the system. Organization A completes RMF steps 1-5[4], documents the results in the RMF core documents, and provides the documentation (and supporting artifacts) to the AOs of hosting environments for Organizations B, C, D, and E, who must determine if the documentation provides sufficient information to confirm adequate security measures are in place and establish an acceptable level of risk for deployment within their organizations.

b. **A system is authorized and subsequently deployed into receiving sites authorized by a separate organization.** In this scenario, the deploying organization's security assessment documentation and supporting artifacts are made available to the receiving site organization. If the receiving organization determines there is insufficient information in the documentation or inadequate security measures in place for establishing an acceptable level of risk, the receiving organization may negotiate with the deploying organization for additional security-related information and/or additional security-related measures. The additional security-related information or security measures may be provided by the deploying organization, the system developer, the receiving organization, some other external third party, or a combination of the above. Once the receiving organization's AO believes adequate security measures are in place and the level of risk is acceptable, the AO may issue a separate authorization for this instance of the system.

c. **A system is authorized by an organization, and another organization takes ownership of the system for deployment.** Systems with an existing authorization issued by other federal organizations require authorization by the receiving AO prior to operating, if the providing organization relinquishes configuration and maintenance of the system to the receiving organization. The receiving organization will maximize reuse of the external organization's RMF core documentation (and supporting artifacts) to support the authorization by the receiving AO.

d. **An organization plans to use an IT service under contract from a commercial entity authorized (or provisionally authorized) by another internal or external organization (e.g., a commercial cloud service provider authorized by the Federal Risk and Authorization Management Program Joint Authorization Board).** In this scenario, the organization leverages an existing authorization and maximizes reuse of the existing documentation to support a new authorization. If the organization determines there are inadequate security measures in place for establishing an acceptable level of risk, the organization may negotiate with the IT service provider for additional security measures and the associated security-related information. Upon assessment and approval of all newly included

[4] RMF steps 1- 5 can be found on the RMF Knowledge Service: https://rmfks.osd.mil/rmf/RMFImplementation/Pages/RMFProcess.aspx

security-related information and the documentation of any potentially applicable security measures in the contract agreement with the IT service provider, the organization AO may issue an authorization.

e. **A system is authorized by an organization AO for that organization's use, and the system is subsequently provided to another organization for it to use as a separately owned, managed, and maintained system.** In this scenario, the receiving organization becomes the PM or ISO and that organization's AO must authorize the system as a separate instance. The receiving system or site will maximize reuse of the existing RMF core documentation and it's supporting artifacts to support the authorization by the receiving AO. Following the issuance of the authorization, subsequent deployment of the system to other receiving sites will follow the review and acceptance process described in paragraph 3.b above.

f. **A system component has been assessed by an organization for that organization's use, and the component is subsequently provided to another organization for it to use as a separately owned, managed, and maintained component.** In this scenario, a security assessment is conducted against applicable security controls and the component is hardened in accordance with applicable security configuration standards (e.g., Security Technical Implementation Guides (STIG), Security Requirements Guides (SRG), National Information Assurance Partnership (NIAP)-approved protection profiles). The receiving system or site will maximize reuse of the existing RMF core documentation to support the acceptance and incorporation by the receiving Information System Security Manager (ISSM) under the direction of the AO. The receiving ISSM may request new tests be conducted (by the receiving organization) after the component is included in the receiving organization's system or network baseline prior to accepting the risk and updating its current ATO or approving its initial ATO.

RECIPROCITY PROCESS

4. The reciprocity process is provided below. This process applies most directly to scenario 3.a above, but it may be adapted as required to apply to the other scenarios (e.g., an authorization decision document may not be relevant in all scenarios, or precisely which AO makes the final authorization decision may vary by scenario). The deploying organization:

a. Initiates the security authorization package and submits an electronic copy of the SSP, SAR, RAR, POA&M, Authorization Decision Document, and list of deployment sites as well as projected dates of deployment through the deploying and receiving organization's POCs.

b. Provides continuing visibility of the system's security authorization package to the receiving systems(s) or site(s).

1) Provides status updates of the RMF activities.

2) Resolves any security issues raised.

c. In coordination with the receiving organization, ensures security control assessments address any and all additional receiving organization security controls or requested adjustments to the assigned security controls identified during security reviews.

d. No later than 60 working days prior to planned deployment, provides a status update to the receiving organization.

e. Issues an authorization decision for the system and version being deployed.

f. Provides installation and configuration requirements documentation to receiving site(s) prior to system deployment.

5. The receiving organization:

a. Maintains situational awareness of the deploying system development and assessment activities.

b. Makes the receiving system(s) security authorization package available to the organization deploying the system.

c. Determines the security impact of connecting the deploying system within the receiving system(s) (e.g., requests for adjustments to the assigned security controls). Implements any receiving system or site augmenting security controls required to support deploying the system.

d. Tests security controls, as appropriate.

1) Security controls that are built into the system will not be re-tested as they do not change when the system is deployed.

2) Controls that require configuration upon deployment must be tested by the receiving system owner.

3) Inherited controls (i.e., controls that will be implemented by the receiving systems) must be (or must have been) validated by the receiving system ISO and supporting documentation or artifacts must be developed.

e. Executes a documented agreement (e.g., Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), or Service Level Agreement (SLA)) with the deploying organization for the maintenance and monitoring of the security posture of the system by a cybersecurity service provider. The document should address such topics as: operating constraints, operating environment, monitoring requirements, security maintenance, and roles and responsibilities.

f. Issues a formal authorization to connect the system (e.g., approval to connect memorandum.). This includes a statement by the receiving organization AO granting approval

for a deployed system to connect to the hosting/receiving system. The receiving system AO's decision is based on the determination that the risk to the hosting/receiving system is acceptable.

1) Provides a copy of implementing documentation (e.g., "authorization to connect") to deploying organization AO.

2) Notifies and provides guidance to subordinate site(s) that the system is authorized to operate and/or connect only in the authorized configuration.

g. Updates hosting/receiving system authorization and/or connection documentation to reflect the incorporation/connection of the system.

h. Ensures the deploying system's installation guide and applicable security configuration requirements are implemented.

i. Ensures mitigations are implemented and maintained in accordance with the deploying system's POA&M.