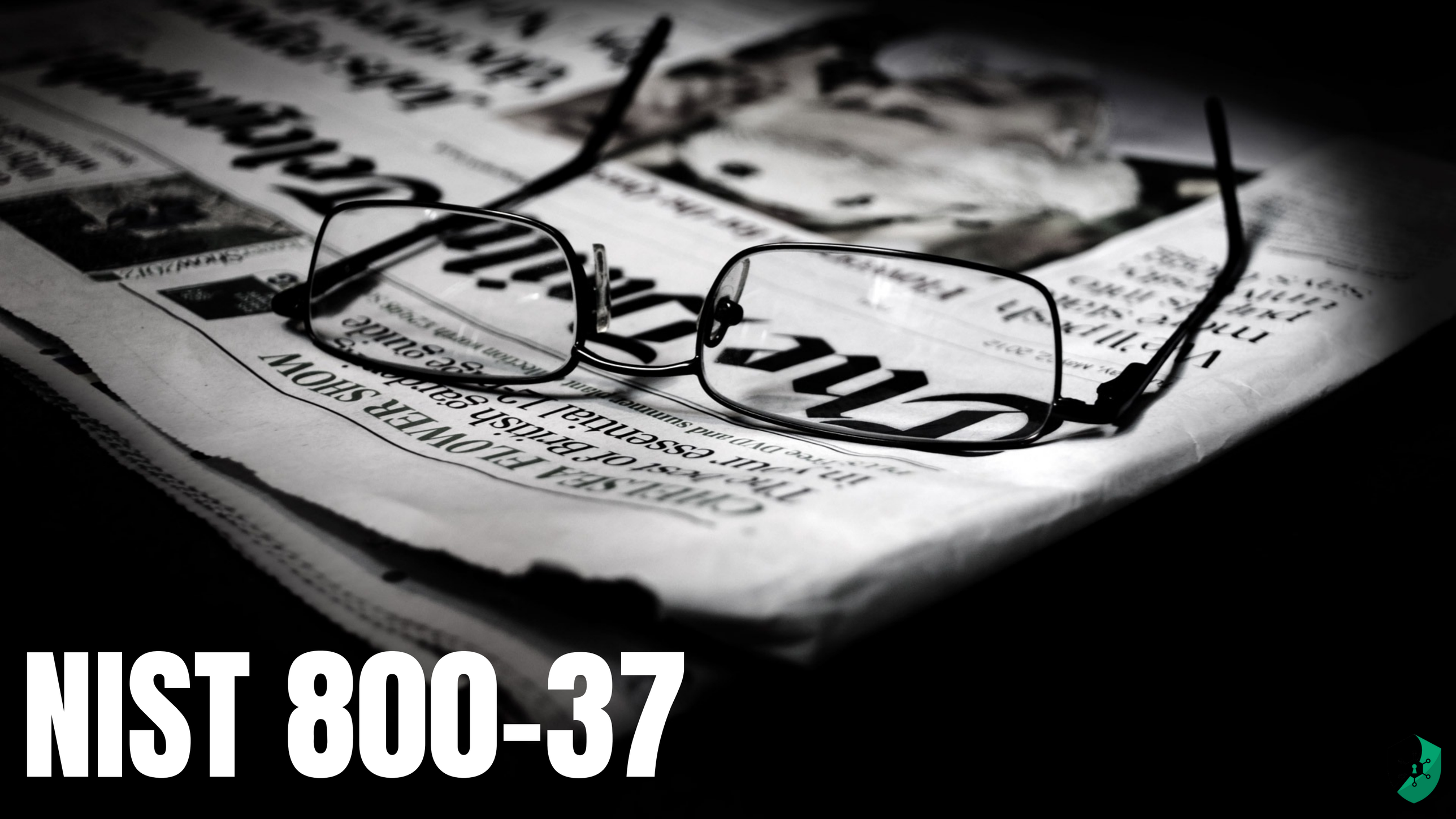

NIST 800-37

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

Each of the 7 steps have:

- Purpose Statement
- Outcomes
- Tasks

3.1 PREPARE

Purpose

The purpose of the ***Prepare*** step is to carry out essential activities at the organization, mission and business process, and information system levels of the organization to help prepare the organization to manage its security and privacy risks using the *Risk Management Framework*.

PREPARE TASKS—ORGANIZATION LEVEL

Table 1 provides a summary of tasks and expected outcomes for the RMF *Prepare* step at the *organization* level. Applicable Cybersecurity Framework constructs are also provided.

TABLE 1: PREPARE TASKS AND OUTCOMES—ORGANIZATION LEVEL

Tasks	Outcomes
TASK P-1 RISK MANAGEMENT ROLES	• Individuals are identified and assigned key roles for executing the Risk Management Framework. [*Cybersecurity Framework*: **ID.AM-6**; **ID.GV-2**]
TASK P-2 RISK MANAGEMENT STRATEGY	• A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established. [*Cybersecurity Framework*: **ID.RM; ID.SC**]
TASK P-3 RISK ASSESSMENT—ORGANIZATION	• An organization-wide risk assessment is completed or an existing risk assessment is updated. [*Cybersecurity Framework*: **ID.RA; ID.SC-2**]
TASK P-4 ORGANIZATIONALLY-TAILORED CONTROL BASELINES AND CYBERSECURITY FRAMEWORK PROFILES (OPTIONAL)	• Organizationally-tailored control baselines and/or Cybersecurity Framework Profiles are established and made available. [*Cybersecurity Framework*: **Profile**]
TASK P-5 COMMON CONTROL IDENTIFICATION	• Common controls that are available for inheritance by organizational systems are identified, documented, and published.
TASK P-6 IMPACT-LEVEL PRIORITIZATION (OPTIONAL)	• A prioritization of organizational systems with the same impact level is conducted. [*Cybersecurity Framework*: **ID.AM-5**]
TASK P-7 CONTINUOUS MONITORING STRATEGY—ORGANIZATION	• An organization-wide strategy for monitoring control effectiveness is developed and implemented. [*Cybersecurity Framework*: **DE.CM; ID.SC-4**]

Quick link to summary table for RMF tasks, responsibilities, and supporting roles.

Some tasks are matched to specific outcomes in the NIST cyber security framework

RISK MANAGEMENT ROLES

TASK P-1 Identify and assign individuals to specific roles associated with security and privacy risk management.

Potential Inputs: Organizational security and privacy policies and procedures; organizational charts.

Expected Outputs: Documented Risk Management Framework role assignments.

Primary Responsibility: Head of Agency; Chief Information Officer; Senior Agency Official for Privacy.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Information Security Officer.

Discussion: The roles and responsibilities of key participants in risk management processes are described in Appendix D. The roles and responsibilities may include personnel that are internal or external to the organization, as appropriate. Since organizations have different missions, functions, and organizational structures, there may be differences in naming conventions for risk management roles and how specific responsibilities are allocated among organizational personnel (e.g., multiple individuals filling a single role or one individual filling multiple roles). In either situation, the basic risk management functions remain the same. Organizations ensure that there are no conflicts of interest when assigning the same individual to multiple risk management roles. For example, authorizing officials cannot occupy the role of system owner or common control provider for systems or common controls they are authorizing. In addition, combining multiple roles for security and privacy requires care because the two disciplines may require different expertise, and in some circumstances, the priorities may be competing. Some roles may be allocated to a group or an office rather than to an individual, for example, control assessor, risk executive (function), or system administrator.

References: [SP 800-160 v1] (Human Resource Management Process); [SP 800-181]; [NIST CSF] (Core [Identify Function]).

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