SmartSuite

Framework / Risk Management / NIST Special Publications

NIST SP 800-30 Rev. 1 – Guide for Conducting Risk Assessments

NIST SP 800-30 Rev. 1 is the NIST guide for conducting information security risk assessments: how to prepare, conduct, communicate, and maintain them at every tier of the organization.



What it is

NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, is the NIST guidance for carrying out information security risk assessments of federal information systems and organizations, amplifying the guidance in SP 800-39 (Section 1.1). It defines a risk model built on threat sources, threat events, vulnerabilities, predisposing conditions, likelihood and impact (Section 2.3.1), and sets out a four-step process of 15 tasks for preparing, conducting, communicating and maintaining an assessment (Chapter Three).

NIST published Revision 1 on September 17, 2012 through the Joint Task Force Transformation Initiative, superseding the July 2002 edition. Section 1.1 states that the guidance satisfies FISMA and the requirements of OMB Circular A-130, Appendix III, and applies to all federal information systems other than national security systems; state, local and tribal governments and private sector organizations are encouraged to use it. In the federal process it supplies the risk assessment that the Risk Management Framework in SP 800-37 draws on.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	VERSION Revision 1 (September 17, 2012)
EFFECTIVE September 17, 2012	DOMAIN Risk Management	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: csrc.nist.gov/pubs/sp/800/30/r1/final

Why it matters

- **A common risk vocabulary** Threat sources, threat events, vulnerabilities, predisposing conditions, likelihood and impact are defined in Section 2.3.1 and the Appendix B glossary and used the same way in every assessment.
- **Assessments at every tier** Section 2.4 applies the same process at Tier 1 (organization), Tier 2 (mission/business process) and Tier 3 (information system), so results roll up and inform each other.
- **Defensible risk ratings** Assessment scales in Tables G-2 to G-5 (likelihood), H-3 (impact) and I-2 and I-3 (risk) let teams show how each rating was reached.
- **Direct input to the RMF** Appendix K describes how an initial assessment informs the tailoring of control baselines and how later assessments inform authorization decisions under SP 800-37.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST SP 800-30 Rev. 1

Risk Assessment Record (Tasks 1-1 to 1-5)

Hold the purpose, scope, assumptions, constraints, information sources and chosen risk model for every assessment as one record, so the prepare step is documented before the analysis starts.

Threat Source and Event Register (Tasks 2-1 and 2-2)

Record adversarial, accidental, structural and environmental threat sources from Table D-2 and the threat events of Tables E-2 and E-3, with a relevance rating per Table E-4.

Vulnerability and Predisposing Condition Log (Task 2-3)

Track vulnerabilities with their severity (Table F-2) and predisposing conditions with their pervasiveness (Table F-5), linked to the systems and processes they affect.

Likelihood, Impact and Risk Scoring (Tasks 2-4 to 2-6)

Score on the Very Low to Very High scales of Tables G-5, H-3 and I-3 and keep the rationale for each value with the record, as Section 2.3 asks.

Risk Response Link (Appendix J)

Link each determined risk to the response decision and to the SP 800-53 controls selected, so assessment results flow into the Risk Management Framework.

Appendix K Report and Maintenance (Tasks 3-1 to 4-2)

Produce the executive summary, body and appendices of the Appendix K report, and schedule the monitoring and update tasks that keep the assessment current.

Common framework mappings

NIST 800-37 Rev.2 · NIST SP 800-39 · NIST CSF 2.0 · NIST 800-53 Rev.5 Baselines · ISO 27005:2022 · ISO 31000:2018

Official resources

NIST SP 800-30 Rev. 1 publication page

The NIST Computer Security Resource Center record for the guide, with status, abstract, keywords, and download links.

csrc.nist.gov/pubs/sp/800/30/r1/final

NIST SP 800-30 Rev. 1 (PDF)

The full text of Guide for Conducting Risk Assessments, September 2012, including all appendices.

nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST Risk Management Framework project

The NIST project page for the RMF, which SP 800-30 supports at the risk assessment step.

csrc.nist.gov/projects/risk-management

NIST SP 800-39 publication page

Managing Information Security Risk, the organization-wide guidance that SP 800-30 amplifies.

csrc.nist.gov/pubs/sp/800/39/final

Frequently asked questions

What are the four steps and 15 tasks of a NIST SP 800-30 risk assessment?

Chapter Three defines four steps: prepare (Section 3.1, Tasks 1-1 to 1-5), conduct (Section 3.2, Tasks 2-1 to 2-6), communicate and share (Section 3.3, Tasks 3-1 and 3-2) and maintain (Section 3.4, Tasks 4-1 and 4-2). Preparing sets the purpose, scope, assumptions and constraints, information sources and risk model; conducting identifies threat sources, threat events, vulnerabilities and predisposing conditions and determines likelihood, impact and risk. Table L-1 in Appendix L summarizes all 15 tasks.

What is the risk model in NIST SP 800-30 Rev. 1?

Section 2.3.1 says a risk model defines the risk factors to be assessed and the relationships among them. The typical factors are threat, vulnerability, impact, likelihood and predisposing condition, with threats decomposed into threat sources and threat events. Risk is a function of the adverse impact if an event occurs and the likelihood of occurrence (Section 2.3).

 © 2026 SmartSuite Inc. All rights reserved.

How does NIST SP 800-30 rate likelihood, impact and risk?

The appendices give exemplary five-level scales from Very Low to Very High. Likelihood of initiation or occurrence and likelihood of adverse impact are rated on Tables G-2 to G-4 and combined in Table G-5; impact is rated on Table H-3; Table I-2 combines overall likelihood and impact into a level of risk described in Table I-3. Organizations may use qualitative, semi-quantitative or quantitative values (Section 2.3.2).

At which tiers can a NIST SP 800-30 risk assessment be conducted?

Section 2.4 says assessments can be conducted at all three tiers of the SP 800-39 hierarchy: Tier 1 (organization), Tier 2 (mission/business process) and Tier 3 (information system). It notes that traditional assessments focus on Tier 3 and can overlook factors better assessed at Tiers 1 and 2, such as the exposure of a core mission to an adversary through system interconnections.

What goes into a risk assessment report under NIST SP 800-30?

Appendix K sets the essential elements in three parts. The executive summary gives the date, purpose, scope, whether the assessment is initial or subsequent, the overall level of risk and the number of risks at each level. The body records the purpose, assumptions and constraints, risk tolerance inputs, the risk model and analytic approach, uncertainties, the summarized results and the time frame for which the assessment is valid; the appendices list sources, the assessment team and supporting detail.

License included / downloadable: Yes NIST SP 800-30 Rev. 1 is a U.S. government publication available free of charge from NIST, and its risk assessment process and taxonomies are included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-30-rev-1

 © 2026 SmartSuite Inc. All rights reserved.