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. It defines a risk model built on threat sources, threat events, vulnerabilities, predisposing conditions, likelihood, and impact, and sets out a four-step process for preparing, conducting, communicating, and maintaining an assessment.

NIST published Revision 1 in September 2012 through the Joint Task Force Transformation Initiative, superseding the 2002 edition. It is written for U.S. federal agencies and their contractors, where it supports the Risk Management Framework, but it is used voluntarily by organizations of every kind as the reference method for a defensible risk assessment.

At a glance

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

Source: https://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 once and used the same way in every assessment.
- **Assessments at every tier** The same process works at the organization, mission and business process, and information system levels, so results roll up and inform each other.
- **Defensible risk ratings** Rating scales for likelihood and impact, with worked tables in the appendices, let teams show how each risk level was determined.
- **Direct input to the RMF** Assessment results feed security categorization, control selection, and authorization decisions under NIST SP 800-37.

How SmartSuite supports NIST SP 800-30 Rev. 1

Risk Assessment Library

Hold assessment scope, assumptions, constraints, and the risk model for every assessment in one structured record set.

Ownership, Cadence, and Accountability

Assign assessment owners, set review cycles, and track the maintain step so no assessment goes stale.

Evidence Collection and Audit Trail

Attach threat intelligence, scan results, and interview notes to each finding with timestamps and reviewers.

Likelihood and Impact Scoring

Score likelihood, impact, and risk on the Appendix G, H, and I scales and record how each rating was reached.

Risk and Control Alignment

Link identified risks to NIST SP 800-53 controls, systems, and third parties to inform risk response.

Risk Reporting

Produce the Appendix K risk assessment report and dashboards for authorizing officials and leadership.

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 is NIST SP 800-30 Rev. 1?

NIST SP 800-30 Rev. 1 is the Guide for Conducting Risk Assessments, published by the National Institute of Standards and Technology in September 2012. It describes how to prepare, conduct, communicate, and maintain an information security risk assessment. It supersedes the original SP 800-30 from 2002.

Who is required to use NIST SP 800-30?

U.S. federal agencies and organizations that operate federal information systems follow it as part of the Risk Management Framework. Other organizations adopt it voluntarily because it gives a defensible, repeatable method for assessing risk. Many auditors and customers recognize it as the reference approach.

What are the four steps of an SP 800-30 risk assessment?

The steps are prepare for the assessment, conduct the assessment, communicate and share the results, and maintain the assessment. Preparing sets purpose, scope, assumptions, and the risk model. Conducting identifies threats, vulnerabilities, likelihood, impact, and risk; maintaining keeps the results current through monitoring.

What is the SP 800-30 risk model?

The risk model defines the factors to assess and how they relate: threat sources and threat events, vulnerabilities and predisposing conditions, likelihood of occurrence, and impact. Risk is determined by combining likelihood and impact. The appendices supply example taxonomies and rating scales for each factor.

How does SP 800-30 relate to NIST SP 800-37 and SP 800-39?

SP 800-39 sets the organization-wide approach to managing information security risk, and SP 800-30 amplifies its guidance on the assessment component. SP 800-37 Rev. 2 is the Risk Management Framework, which uses SP 800-30 assessments to inform categorization, control selection, authorization, and monitoring.

Can SP 800-30 be used with ISO/IEC 27005 or ISO 31000?

Yes. ISO/IEC 27005:2022 and ISO 31000:2018 describe risk assessment processes with the same identification, analysis, and evaluation activities. Organizations map the SP 800-30 risk factors and scales to those standards so one assessment can satisfy both NIST-based and ISO-based programs.

How does SmartSuite support NIST SP 800-30?

SmartSuite runs each assessment through the four SP 800-30 steps, with threat, vulnerability, likelihood, and impact records scored on the guide's scales. Findings link to the systems, controls, and third parties they affect, and the risk register feeds remediation tasks and reporting for authorizing officials.

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

