SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-61 Rev. 3 – Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile

NIST SP 800-61 Rev. 3 is NIST's April 2025 guidance for building incident response into cybersecurity risk management, organized as a CSF 2.0 Community Profile.

What it is

NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, is the April 2025 revision of NIST's incident handling guide. It replaces the 2012 Revision 2 and reframes incident response as an integral part of cybersecurity risk management rather than a separate activity run by a separate team, organizing its recommendations as a Community Profile of the NIST Cybersecurity Framework (CSF) 2.0.

The publication is produced by the National Institute of Standards and Technology (NIST) and written by Alexander Nelson, Sanjay Rekhi, and Murugiah Souppaya of NIST with Karen Scarfone. It is voluntary guidance: U.S. federal agencies use it to satisfy incident response expectations under FISMA and OMB policy, and organizations of every size and sector adopt it because the CSF 2.0 vocabulary already anchors their security programs, contracts, and regulatory reporting.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	VERSION Revision 3
EFFECTIVE April 2025	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: https://csrc.nist.gov/pubs/sp/800/61/r3/final

Why it matters

- **Integrate incident response with risk management** Preparation, detection, response, recovery, and lessons learned sit inside the same governance and risk activities the rest of the security program already uses.
- **Speak a shared vocabulary** Every recommendation is tied to a CSF 2.0 Function, Category, and Subcategory, so incident response can be discussed with executives, auditors, insurers, and regulators in terms they already know.
- **Reflect modern incidents** The life cycle model assumes long, complex incidents and continuous improvement instead of a closed loop that restarts after each event.
- **Clarify roles and responsibilities** Section 2 sets out the internal teams, leadership, and third parties that carry incident response duties across all six Functions.

How SmartSuite supports NIST SP 800-61 Rev. 3

Incident Response Profile Library

Hold every Function, Category, and Subcategory of the Community Profile as a structured record with its recommendations and the organization's implementation status.

Ownership, Cadence, and Accountability

Assign owners for preparation and response outcomes, set review dates for plans and playbooks, and track exercise schedules.

Evidence Collection and Audit Trail

Capture incident tickets, timelines, decisions, notifications, and post-incident reports with timestamps and reviewers linked to the Subcategories they evidence.

Exercises and Post-Incident Reviews

Plan tabletop exercises and reviews, record findings, and route lessons learned to the Improvement Category as tracked actions.

Risk and Vendor Alignment

Connect incident scenarios, risk register entries, and third-party dependencies to the Profile outcomes they affect.

Leadership and Regulator Reporting

Generate status views of preparation and response outcomes, open incidents, and notification obligations for executives and auditors.

Common framework mappings

NIST CSF 2.0 | NIST 800-53 Rev.5 | NIST 800-37 Rev.2 | NIST SP 800-30 Rev. 1 | ISO 27001:2022 | ISO 27002:2022 | CIS Controls v8.1 | SOC 2 (AICPA TSC 2017) | NIST CSF v1.1

Official resources

NIST SP 800-61 Rev. 3 publication page

The NIST Computer Security Resource Center record for Revision 3, with status, abstract, keywords, authors, and the document it supersedes.

csrc.nist.gov/pubs/sp/800/61/r3/final

NIST SP 800-61 Rev. 3 (PDF)

The full text of the April 2025 publication, including the CSF 2.0 Community Profile tables, glossary, and change log.

nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

NIST Incident Response project

The NIST project page that hosts the publication, its online resources, and related incident response guidance.

csrc.nist.gov/projects/incident-response

NIST Cybersecurity and Privacy Reference Tool (CPRT)

The tool through which the Profile's Subcategories link to implementation resources and mappings to other standards.

csrc.nist.gov/projects/cprt

Frequently asked questions

What is NIST SP 800-61 Rev. 3?

NIST SP 800-61 Rev. 3 is NIST's April 2025 guide to incident response, titled Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. It explains how to build incident response into an organization's wider cybersecurity risk management and organizes its recommendations using the Functions, Categories, and Subcategories of NIST CSF 2.0.

What changed between Revision 2 and Revision 3 of NIST SP 800-61?

Revision 2 (2012) described incident response as a separate cycle of preparation, detection and analysis, containment, eradication and recovery, and post-incident activity. Revision 3 replaces that model with one based on the six CSF 2.0 Functions, treats incident response as part of continuous cybersecurity risk management, and moves detailed technical guidance and playbooks to online resources that NIST keeps current through the Cybersecurity and Privacy Reference Tool.

What is a CSF 2.0 Community Profile?

A CSF 2.0 Community Profile is a set of CSF outcomes selected and annotated for a particular community or use case. In NIST SP 800-61 Rev. 3 the Profile lists, for each relevant Subcategory, the recommendations and considerations that support incident response, split into a preparation and lessons learned table and an incident response table.

Is NIST SP 800-61 Rev. 3 mandatory?

It is voluntary guidance. U.S. federal agencies are expected to follow NIST guidelines when meeting their FISMA incident response obligations, and many regulators, insurers, and customers reference it, but there is no certification against it. Most organizations adopt it because it aligns with NIST CSF 2.0 and NIST SP 800-53 programs they already run.

How does NIST SP 800-61 Rev. 3 define the incident response life cycle?

Govern, Identify, and Protect are preparation activities that prevent some incidents, ready the organization for those that occur, and limit their impact. Detect, Respond, and Recover are the incident response activities themselves. The Improvement Category within Identify receives lessons learned from every Function as soon as they are identified, so improvement is continuous rather than a final phase.

Where did the technical detail and playbooks from NIST SP 800-61 Rev. 2 go?

NIST moved them online. Each Function, Category, and Subcategory in the Profile links through the NIST Cybersecurity and Privacy Reference Tool (CPRT) to implementation guidance, mappings to other incident response and risk management standards, and other resources that NIST can update without reissuing the publication.

How does NIST SP 800-61 Rev. 3 relate to NIST SP 800-53 and ISO/IEC 27035?

It provides the how-to for the Incident Response (IR) control family in NIST SP 800-53 Rev. 5 and complements the risk management process in NIST SP 800-37 and NIST SP 800-30. Internationally, ISO/IEC 27035 and the incident management controls of ISO/IEC 27002:2022 cover the same ground, and the CPRT publishes mappings between them and the Profile.

License included / downloadable: Yes NIST SP 800-61 Rev. 3 is a U.S. government publication available free of charge from NIST, and its CSF 2.0 Community Profile structure is included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-61-rev-3-incident-response-recommendations-and-considerations