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 (April 3, 2025) is NIST's guidance for building incident response into cybersecurity risk...



What it is

NIST SP 800-61 Revision 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, is NIST's incident response guidance. NIST published it as final on April 3, 2025 after a public draft of April 3, 2024. It supersedes SP 800-61 Rev. 2, the Computer Security Incident Handling Guide of August 6, 2012, 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.

At a glance

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

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

Why it matters

- **Incident response inside risk management** Fig. 2 places Govern, Identify and Protect as preparation, Detect, Respond and Recover as incident response, and the Improvement Category (ID.IM) between them, so response sits in the same governance the rest of the program uses.
- **A shared vocabulary** Every recommendation is tied to a CSF 2.0 Function, Category and Subcategory, with identifiers such as GV.OC-03.R1, so incident response can be discussed with executives, auditors, insurers and regulators in terms they already know.
- **A model that reflects modern incidents** Section 2.1 assumes long, complex incidents and continuous improvement instead of a loop that restarts after each event, and says organizations should use the life cycle model that suits them best.
- **Roles beyond the response team** Section 2.2 names leadership, incident handlers, technology professionals, legal, public affairs, human resources, physical security and facilities, asset owners and contracted third parties.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST SP 800-61 Rev. 3

Community Profile Rows (Tables 2 and 3)

Hold every Function, Category and Subcategory as a record with its priority, its R, C and N items by identifier such as GV.OC-03.R1, and the organization's own priority and implementation status.

Incident Response Plan and Policy (Section 2.3)

Keep the policy elements, from management commitment to performance measures, the plan and the playbooks as linked records with owners and review dates.

Roles and Third-Party Responsibilities (Section 2.2)

Record who holds each role, from leadership to asset owners, and the contracted MSSP, cloud and other providers with their contract-defined duties and authority to act.

Incident Records and Notifications

Capture each incident's timeline, decisions, containment and recovery actions and the notification and breach reporting obligations GV.OC-03.R1 points to, with evidence and reviewers.

Exercises and Lessons Learned (ID.IM)

Plan exercises and post-incident reviews, record findings and route lessons learned to the Improvement Category as tracked actions that update the plan and playbooks.

Leadership and Regulator Reporting

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

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 changed between NIST SP 800-61 Rev. 2 and Rev. 3?

Rev. 2 of August 6, 2012 described incident response as a cycle of preparation, detection and analysis, containment, eradication and recovery, and post-incident activity (Fig. 1). Rev. 3, final on April 3, 2025, replaces that with a model built on the six CSF 2.0 Functions (Fig. 2), reorganizes the content as a CSF 2.0 Community Profile and moves most how-to detail and links to the online Incident Response project page and the CPRT. Appendix C lists the changes.

How does Table 1 map the old life cycle phases to CSF 2.0?

Preparation maps to Govern, Identify (all Categories) and Protect. Detection and Analysis maps to Detect and the Identify Improvement Category. Containment, Eradication and Recovery maps to Respond, Recover and Identify (Improvement). Post-Incident Activity maps to Identify (Improvement), which is why Section 2.1 shows lessons learned flowing from every Function rather than only at the end.

 © 2026 SmartSuite Inc. All rights reserved.

What do the priorities and the R, C and N tags in the Profile mean?

Section 3 gives each row a priority: High means a core incident response activity for most organizations, Medium directly supports incident response and Low indirectly supports it. The last column holds recommendations (R, something the organization should do), considerations (C, something it should consider doing) and notes (N). The tag and number appended to the CSF ID, for example GV.OC-03.R1, give a unique identifier, and organizations are encouraged to customize the priorities.

Who is responsible for incident response under NIST SP 800-61 Rev. 3?

Section 2.2 lists leadership, incident handlers (on staff, on contract such as an outsourced SOC or MSSP, or available when needed), technology professionals, legal, public affairs and media relations, human resources, physical security and facilities management, and asset owners. Third parties may perform primary or partial roles under a shared responsibility model, with responsibilities, information flows and authority to act defined in the contract.

Is NIST SP 800-61 Rev. 3 mandatory, and does it define what an incident is?

It is guidance, not a regulation or a certifiable standard; Section 3 says the Community Profile is intended for most organizations regardless of sector or size and is to be customized. Section 1 defines a cybersecurity incident with the FISMA 2014 wording, an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality or availability of information or an information system, or violates law, security policies or acceptable use policies, and distinguishes it from events and adverse events.

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-considerations

 © 2026 SmartSuite Inc. All rights reserved.