

# NIST IR 8374

NIST IR 8374 guides organizations in identifying, assessing, and addressing cybersecurity risks from emerging technologies and sector-specific threats.



## What it is

NIST IR 8374 is a guidance document that helps organizations identify, assess, and address cybersecurity risks associated with emerging technologies and sector-specific threats. It provides a structured approach for evaluating how new digital innovations and industry contexts affect an organization’s security posture and risk management strategies.

Published by the National Institute of Standards and Technology (NIST), the report is used by cybersecurity professionals, risk managers, and compliance teams across public and private sectors. NIST IR 8374 focuses on evaluating emerging risks, implementing appropriate cybersecurity controls, and supporting compliance with broader frameworks such as the NIST Risk Management Framework (RMF) and sector-specific regulations.

## At a glance

|                                                                                       |                                                      |                                                          |
|---------------------------------------------------------------------------------------|------------------------------------------------------|----------------------------------------------------------|
| <div>PUBLISHER</div> <div>National Institute of Standards and Technology (NIST)</div> | <div>TYPE</div> <div>Guidance</div>                  | <div>VERSION</div> <div>NIST IR 8374</div>               |
| <div>EFFECTIVE</div> <div>June 2024</div>                                             | <div>DOMAIN</div> <div>Cybersecurity</div>           | <div>FAMILY</div> <div>NIST Special Publications</div>   |
| <div>REGION</div> <div>United States</div>                                            | <div>ADOPTION MODEL</div> <div>Risk Management</div> | <div>IMPLEMENTATION COMPLEXITY</div> <div>Moderate</div> |

Source: <https://csrc.nist.gov/pubs/ir/8374/final>

## Why it matters

- **Strengthen cybersecurity governance** Establishes a structured approach for identifying and prioritizing risks unique to new technologies and industry sectors.
- **Enhance regulatory alignment** Provides guidance that supports compliance with the NIST Risk Management Framework and relevant sector-specific requirements.
- **Improve risk assessments** Enables organizations to conduct comprehensive evaluations of threats associated with both established and emerging digital environments.
- **Promote operational resilience** Encourages adaptive security controls and risk mitigation strategies to reduce potential disruptions caused by novel cyber threats.

## How SmartSuite supports NIST IR 8374

### GenAI Use Case Inventory and Approvals

Catalog GenAI use cases, owners, approvals, and scope boundaries.

### GenAI Risk Assessments and Controls

Track risks like leakage, misuse, and reliability with mitigations and decisions.

### Testing and Evaluation Evidence

Capture evaluation results, red teaming outputs, and safety testing proof.

### Monitoring and Misuse Detection

Schedule monitoring tasks for drift, misuse, and policy compliance with evidence.

### Incident Response and Escalation Workflow

Run GenAI incidents with timelines, decisions, and corrective actions.

### Reporting and Readiness Dashboards

Report posture, open risks, and readiness across GenAI systems and teams.

## Common framework mappings

CIS Controls v8.1

ISO 27001:2022

ISO 27002:2022

ISO 27701

MITRE ATT&CK

NIST CSF 2.0

NIST 800-53 Rev.5

SOC 2

## Official resources

### NIST IR 8374 Document

Defines cybersecurity considerations for emerging and sector-specific risks, published by NIST.

[csrc.nist.gov/publications/detail/nistir/8374/final](https://csrc.nist.gov/publications/detail/nistir/8374/final)

### NIST Risk Management Framework

Describes the framework for integrating supply chain risk management into system lifecycle.

[csrc.nist.gov/publications/detail/sp/800-37/rev-2/final](https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final)

### NIST Cybersecurity Framework

Describes common policies to improve cybersecurity risk management.

[nist.gov/cyberframework](https://nist.gov/cyberframework)

### NIST SP 800-53 Revision 5

Defines the security and privacy controls for federal information systems.

[csrc.nist.gov/publications/detail/sp/800-53/rev-5/final](https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final)

## Frequently asked questions

### What is NIST IR 8374 used for?

NIST IR 8374 is designed to help organizations identify, assess, and manage cybersecurity risks associated with emerging technologies and sector-specific threats. It provides structured guidance for integrating novel digital risks into an organization's existing cybersecurity and risk management programs.

### Is NIST IR 8374 a mandatory or certifiable standard?

NIST IR 8374 is a guidance document and is not mandatory or certifiable on its own. However, following its recommendations can support compliance with mandatory sector-specific regulations and recognized frameworks like the NIST Risk Management Framework (RMF).

### What organizations should use NIST IR 8374?

NIST IR 8374 is intended for organizations in both the public and private sectors that use emerging technologies or face unique sector-specific cybersecurity risks. It is especially relevant for industries with evolving threats or rapidly changing technology landscapes.

### What are the key components or artifacts of NIST IR 8374?

Key components of NIST IR 8374 include structured risk assessments, mapping of security controls to sector-specific risks, and integration of tailored safeguards. Organizations are also expected to document risk findings, control implementation, and governance actions as part of their risk management artifacts.

## How does implementation of NIST IR 8374 work in practice?

Organizations implement NIST IR 8374 by embedding its risk assessment methodologies into existing cybersecurity practices, mapping sector-specific threats to control frameworks, and updating governance processes. This involves targeted assessments, ongoing documentation, and adaptation of controls as new technologies or threats emerge.

## How does NIST IR 8374 relate to other cybersecurity frameworks?

NIST IR 8374 is intended to complement broader NIST frameworks such as the Cybersecurity Framework (CSF) and RMF by providing sector- and technology-specific guidance. It helps organizations align foundational cybersecurity controls with unique industry requirements and regulatory mandates.

## What are the ongoing compliance requirements under NIST IR 8374?

Ongoing compliance with NIST IR 8374 involves regularly reviewing emerging risks, updating risk assessments, monitoring the effectiveness of controls, and aligning with relevant sector regulations. Maintaining documentation and evidence of these activities is crucial for governance and audit purposes.

## How would SmartSuite support NIST IR 8374?

SmartSuite enables organizations to operationalize NIST IR 8374 by facilitating risk tracking, control management, and evidence collection tailored to sector-specific threats. The platform supports audit readiness with documentation capabilities, policy governance, and dynamic reporting dashboards to monitor compliance and risk management outcomes.

License included / downloadable: Yes NIST IR 8374 is published by the National Institute of Standards and Technology and is publicly available through official NIST publications.

Full framework page and mappings: [smartsuite.com/frameworks/nist-ir-8374-cybersecurity-considerations-for-emerging-and-sector-specific-risks](https://smartsuite.com/frameworks/nist-ir-8374-cybersecurity-considerations-for-emerging-and-sector-specific-risks)