# Nist 800 53 Mapping To 800 171

| # | CMMC Practice | SP 800-171A Assessment Objective | SP 800-53 Control | Appendix C | FedRAMP Moderate specifications |
|---|---|---|---|---|---|
| 1 | AC.L1-3.1.1[a.] | Determine if authorized users are identified; | AC-2 | O | |
| 2 | AC.L1-3.1.1[b.] | Determine if processes acting on behalf of authorized users are identified; | AC-3 | O | |
| 3 | AC.L2-3.1.1[c.] | Determine if devices (and other systems) authorized to connect to the system are identified; | IA-3 | S | |
| 4 | AC.L1-3.1.1[d.] | Determine if system access is limited to authorized users; | AC-3 | S | |
| 5 | AC.L1-3.1.1[e.] | Determine if system access is limited to processes acting on behalf of authorized users; and | AC-3 | S | |
| 6 | AC.L1-3.1.1[f.] | Determine if system access is limited to authorized devices (including other systems). | AC-3 | S | |
| 7 | AC.L1-3.1.2[a.] | Determine if the types of transactions and functions that authorized users are permitted to execute are defined; and | AC-3 | O | |
| 8 | AC.L1-3.1.2[b.] | Determine if system access is limited to the defined types of transactions and functions for authorized users. | AC-3 | O | |
| 9 | AC.L2-3.1.3[a.] | Determine if information flow control policies are defined; | AC-4 | S | |
| 10 | AC.L2-3.1.3[b.] | Determine if methods and enforcement mechanisms for controlling the flow of CUI are defined; | AC-4 | S | |
| 11 | AC.L2-3.1.3[c.] | Determine if designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified; | AC-4 | S | |
| 12 | AC.L2-3.1.3[d.] | Determine if authorizations for controlling the flow of CUI are defined; and | AC-4 | S | |
| 13 | AC.L2-3.1.3[e.] | Determine if approved authorizations for controlling the flow of CUI are enforced. | AC-4 | S | |
| 14 | AC.L2-3.1.4[a.] | Determine if the duties of individuals requiring separation are defined; | AC-5 | O | |
| 15 | AC.L2-3.1.4[b.] | Determine if responsibilities for duties that require separation are assigned to separate individuals; and | AC-5 | O | |
| 16 | AC.L2-3.1.4[c.] | Determine if access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals. | AC-5 | O | |
| 17 | AC.L2-3.1.5[a.] | Determine if privileged accounts are identified; | AC-6 | O | |
| 18 | AC.L2-3.1.5[b.] | Determine if access to privileged accounts is authorized in accordance with the principle of least privilege; | AC-6(5) | O | |
| 19 | AC.L2-3.1.5[c.] | Determine if security functions are identified; and | AC-6(1) | O | |
| 20 | AC.L2-3.1.5[d.] | Determine if access to security functions is authorized in accordance with the principle of least privilege. | AC-6(1) | O | |
| 21 | AC.L2-3.1.6[a.] | Determine if nonsecurity functions are identified; and | AC-6(2) | O | |
| 22 | AC.L2-3.1.6[b.] | Determine if users are required to use non-privileged accounts or roles when accessing nonsecurity functions. | AC-6(2) | O | |
| 23 | AC.L2-3.1.7[a.] | Determine if privileged functions are defined; | AC-6(10) | S | |
| 24 | AC.L2-3.1.7[b.] | Determine if non-privileged users are defined; | AC-6(10) | S | |
| 25 | AC.L2-3.1.7[c.] | Determine if non-privileged users are prevented from executing privileged functions; and | AC-6(10) | S | |
| 26 | AC.L2-3.1.7[d.] | Determine if the execution of privileged functions is captured in audit logs. | AC-6(9) | S | |
| 27 | AC.L2-3.1.8[a.] | Determine if the means of limiting unsuccessful logon attempts is defined; and | AC-7 | S | 3 consecutive invalid attempts during a time period |
| 28 | AC.L2-3.1.8[b.] | Determine if the defined means of limiting unsuccessful logon attempts is implemented. | AC-7 | S | |
| 29 | AC.L2-3.1.9[a.] | Determine if privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category; and | AC-8 | O/S | |
| 30 | AC.L2-3.1.9[b.] | Determine if privacy and security notices are displayed. | AC-8 | O/S | |
| 31 | AC.L2-3.1.10[a.] | Determine if the period of inactivity after which the system initiates a session lock is defined; | AC-11 | S | 15 minutes of inactivity |
| 32 | AC.L2-3.1.10[b.] | Determine if access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity; and | AC-11 | S | |

**NIST 800-53 Mapping to 800-171** is a critical aspect of information security compliance, particularly for organizations that handle Controlled Unclassified Information (CUI). The National Institute of Standards and Technology (NIST) has developed a series of publications aimed at enhancing the security and privacy of federal information systems. Among these publications, NIST Special Publication 800-53 provides a catalog of security and privacy controls, while NIST Special Publication 800-171 outlines the necessary requirements for protecting CUI in non-federal systems and organizations. This article will delve into the mapping process between these two frameworks, highlighting their significance, methodologies for mapping, and practical steps organizations can take to ensure compliance.

## Understanding NIST 800-53 and 800-171

### NIST 800-53 Overview

NIST 800-53, officially titled "Security and Privacy Controls for Information Systems and Organizations," provides a comprehensive set of controls designed to protect federal information systems and the data they handle. The framework includes over 900 individual controls divided into 18 families, addressing a wide array of security and privacy needs. Key areas covered include:

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Incident Response
- Risk Assessment
- System and Communications Protection

These controls are intended to be tailored to an organization's specific risk environment, allowing for flexibility in implementation.

## NIST 800-171 Overview

NIST 800-171, titled "Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations," focuses on safeguarding CUI in environments outside federal oversight. It provides a set of 14 families of security requirements, derived from NIST 800-53, which organizations must implement to ensure compliance with federal regulations, particularly for contractors working with the Department of Defense (DoD) and other federal agencies. The 14 families of requirements include:

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity
- Maintenance

# The Importance of Mapping NIST 800-53 to 800-171

Mapping NIST 800-53 to NIST 800-171 is essential for several reasons:

1. Compliance: Organizations that handle CUI must comply with NIST 800-171 to meet contractual obligations with federal entities. Understanding how the controls in 800-53 map to those in 800-171 helps organizations demonstrate compliance.

2. Streamlined Implementation: By understanding the relationship between the two standards, organizations can implement security controls more efficiently, using existing controls in 800-53 to fulfill requirements in 800-171.

3. Risk Management: Mapping provides a clearer picture of an organization's overall risk posture, enabling more effective risk management strategies.

4. Resource Allocation: Organizations can better allocate resources when they understand which controls are duplicates or closely related, avoiding unnecessary expenditures.

# Mapping Methodology

The mapping process involves a detailed comparison of the controls and requirements in both publications. Here are key steps in the mapping methodology:

## 1. Control Identification

Begin by identifying the relevant controls from NIST 800-53 that are applicable to your organization's environment. This includes reviewing the 18 control families and selecting the controls that address the security needs of systems handling CUI.

## 2. Cross-Referencing Controls

Next, cross-reference the identified controls with the requirements outlined in NIST 800-171. This is typically done through a matrix that aligns each NIST 800-53 control with its corresponding NIST 800-171 requirement.

## 3. Gap Analysis

Conduct a gap analysis to identify any discrepancies between the controls in NIST 800-53 and the requirements in NIST 800-171. This involves assessing whether existing controls adequately address the requirements or if additional controls are needed.

## 4. Implementation and Documentation

Once gaps have been identified, develop a plan for implementing any additional controls necessary to meet NIST 800-171 requirements. Document the mapping process, including justifications for control selections and implementations, to facilitate audits and reviews.

# Example Mapping of Controls

To illustrate how NIST 800-53 controls map to NIST 800-171 requirements, consider the following examples:

- Access Control (AC):
- NIST 800-53 AC-1 (Access Control Policy and Procedures) maps to NIST 800-171 3.1.1 (Limit information system access to authorized users).

- Incident Response (IR):
- NIST 800-53 IR-1 (Incident Response Policy and Procedures) maps to NIST 800-171 3.6.1 (Establish an incident response capability).

- Media Protection (MP):
- NIST 800-53 MP-1 (Media Protection Policy and Procedures) maps to NIST 800-171 3.8.1 (Protect digital CUI stored on digital media).

This mapping allows organizations to see how existing security controls can satisfy multiple

compliance requirements, thereby streamlining their security posture.

## Challenges in Mapping

While mapping NIST 800-53 to 800-171 is beneficial, organizations may face several challenges:

- Complexity: The extensive nature of NIST 800-53 can make it difficult to identify relevant controls and their mapping to NIST 800-171.
- Resource Constraints: Smaller organizations may lack the resources or expertise to conduct thorough mapping and implementation.
- Dynamic Environments: Changes in technology, business processes, and regulatory requirements can affect the relevance and applicability of certain controls.

## Best Practices for Successful Mapping

To overcome the challenges associated with mapping, organizations can adopt the following best practices:

1. Establish a Cross-Functional Team: Involve stakeholders from IT, compliance, risk management, and operational departments to ensure a comprehensive approach to mapping.

2. Leverage Automation Tools: Utilize compliance management software that can help automate the mapping process, making it more efficient and less prone to human error.

3. Regularly Review and Update: As NIST updates its publications and as organizational needs evolve, regularly review and update the mapping to ensure continued compliance.

4. Engage in Training and Awareness: Provide training programs for staff to understand the significance of NIST 800-53 and 800-171, enhancing their ability to contribute to compliance efforts.

5. Seek External Expertise: When necessary, consider consulting with security compliance experts to assist with mapping and implementation.

## Conclusion

In conclusion, the mapping of NIST 800-53 to NIST 800-171 is a vital process for organizations that handle Controlled Unclassified Information. By understanding the relationship between these two frameworks, organizations can ensure compliance, enhance their security posture, and effectively manage risks. Through a structured methodology, including control identification, cross-referencing, gap analysis, and documentation, organizations can successfully navigate the complexities of compliance. By adopting best practices and engaging stakeholders across the organization, they can streamline their efforts and ultimately protect sensitive information more effectively.

# Frequently Asked Questions

## What is the purpose of NIST 800-53 and how does it relate to NIST 800-171?

NIST 800-53 provides a catalog of security and privacy controls for federal information systems, while NIST 800-171 outlines specific requirements for protecting Controlled Unclassified Information (CUI) in non-federal systems. NIST 800-171 is derived from NIST 800-53, focusing on a subset of controls tailored for non-federal organizations.

## How can organizations effectively map NIST 800-53 controls to NIST 800-171 requirements?

Organizations can create a mapping document that aligns each NIST 800-171 requirement with the corresponding NIST 800-53 control. This involves analyzing both frameworks to identify relevant controls, ensuring that the mapping addresses all aspects of CUI protection while maintaining compliance with federal standards.

## What are the main differences between NIST 800-53 and NIST 800-171?

The main differences lie in their scope and target audience. NIST 800-53 is comprehensive and designed for federal agencies and contractors, while NIST 800-171 is specifically aimed at non-federal organizations handling CUI, emphasizing a streamlined approach to security controls.

## What are some common challenges organizations face when mapping NIST 800-53 to NIST 800-171?

Common challenges include understanding the context of each control, ensuring all relevant controls are addressed, and adapting the more extensive NIST 800-53 controls to fit the specific needs and capabilities of non-federal systems under NIST 800-171.

## Why is it important for organizations to understand the mapping between NIST 800-53 and NIST 800-171?

Understanding the mapping is crucial for organizations to ensure compliance with federal regulations when handling CUI, to implement adequate security measures, and to effectively manage risks associated with information security in a non-federal context.

## Are there tools available to assist organizations in mapping NIST 800-53 to NIST 800-171?

Yes, there are various tools and frameworks available, including spreadsheets, compliance management software, and templates provided by security consultancies, which help organizations systematically map controls and track compliance efforts.

## How often should organizations review and update their mappings between NIST 800-53 and NIST 800-171?

Organizations should review and update their mappings at least annually or whenever there are significant changes in regulations, business processes, or technology. This ensures that the controls remain relevant and effective in addressing current security threats.



# Nist 800 53 Mapping To 800 171

Qu'est-ce que le cadre de cybersécurité du NIST - IBM
Découvrez le cadre de cybersécurité du NIST et les solutions qui permettent d'améliorer la sécurité de l'information et la gestion des risques de cybersécurité

**O que é o NIST Cybersecurity Framework? - IBM**
O National Institute of Standards and Technology (NIST) é uma agência não reguladora que promove a inovação por meio do avanço da ciência, padrões e tecnologia de medição. O ...

¿Qué es el marco de ciberseguridad del NIST? | IBM
El marco de ciberseguridad del NIST proporciona una guía completa y las mejores prácticas que las organizaciones del sector privado pueden seguir para mejorar la seguridad de la ...

**What is the NIST Cybersecurity Framework? - IBM**
Oct 14, 2021 · The NIST Cybersecurity Framework provides comprehensive guidance and best practices for improving information security and cybersecurity risk management.

什么是 **NIST** 网络安全框架? **- IBM**
NIST 网络安全框架 (NIST CSF) 由标准、指南和最佳实践组成，可帮助组织改善网络安全风险管理。 NIST CSF 的设计灵活，可与各行各业任何组织中的现有安全流程相集成。这是一个良好 ...

如何看待网传*NIST*原子谱学组被集体裁员、*NIST*原子分子数据库有 ...
如题，NIST原子分子数据库的意义有多么重要？网传美国国家标准技术研究院 (NIST)的原子谱学组被集体裁员，其维护的原子分子物理数据库服务面临存亡危...

*Was ist das NIST Cybersecurity Framework? - IBM*
Das NIST Cybersecurity Framework (NIST CSF) besteht aus Standards, Richtlinien und Best Practices, die Unternehmen dabei helfen, ihr Management von Cybersicherheitsrisiken zu ...

*NIST*是一个什么样的组织？ - 知乎
NIST拥有美国标准时间源的NIST-F1原子喷泉钟。 NIST和科罗拉多州大学的联合实验室JILA拥有全世界最准确的光钟，准确度在1E-18，这个应该是和巴黎天文台光钟的指标交替上升。 ...

**How AI can be hacked with prompt injection: NIST report - IBM**

NIST closely observes the AI lifecycle for good reason. As AI proliferates, so does the discovery and exploitation of AI cybersecurity vulnerabilities.

**Cos'è il NIST Cybersecurity Framework? | IBM**
Il NIST (National Institute of Standards and Technology) è un'agenzia non regulatoria che promuove l'innovazione attraverso il progresso della scienza, degli standard e della tecnologia …

*Qu'est-ce que le cadre de cybersécurité du NIST - IBM*
Découvrez le cadre de cybersécurité du NIST et les solutions qui permettent d'améliorer la sécurité de l'information …

**O que é o NIST Cybersecurity Framework? - IBM**
O National Institute of Standards and Technology (NIST) é uma agência não reguladora que promove a inovação …

*¿Qué es el marco de ciberseguridad del NIST? | IBM*
El marco de ciberseguridad del NIST proporciona una guía completa y las mejores prácticas que las …

**What is the NIST Cybersecurity Framework? - IBM**
Oct 14, 2021 · The NIST Cybersecurity Framework provides comprehensive guidance and best practices for …

什么是 **NIST** 网络安全框架？ **- IBM**
NIST 网络安全框架 (NIST CSF) 由标准、指南和最佳实践组成，可帮助组织改善网络安全风险管理。 NIST CSF 的设计灵活，可与各行各业任 …

Discover how NIST 800-53 mapping to 800-171 enhances your cybersecurity framework. Learn more about compliance and best practices to protect your data.

Back to Home