

Table of Contents

NIST SP 800-171r2

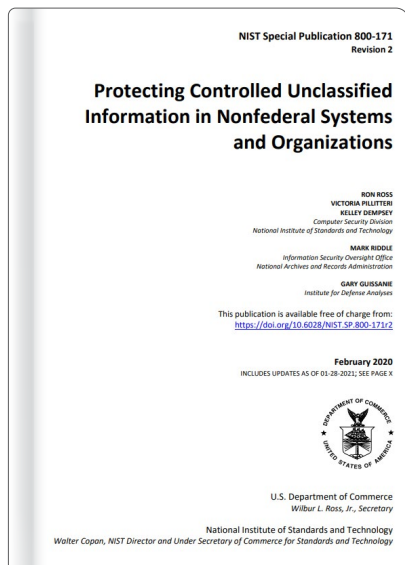
Readiness	2
Risk Assessment	3
SSP Portal	5
Playbook	6
Toolkit	7



Peter.Harvey@ecfirst.com

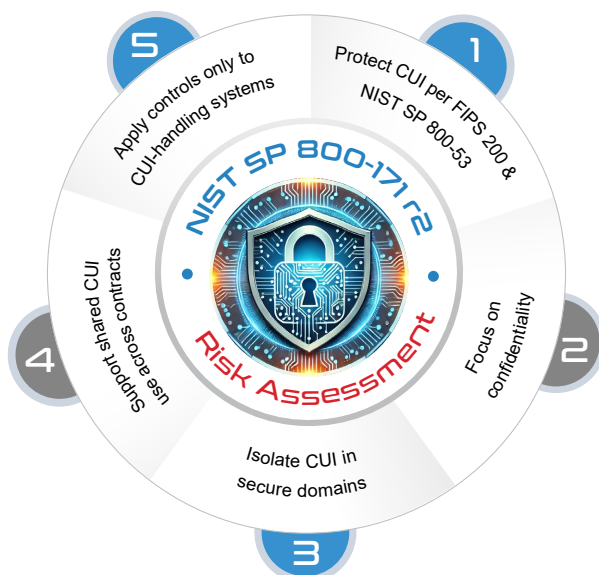
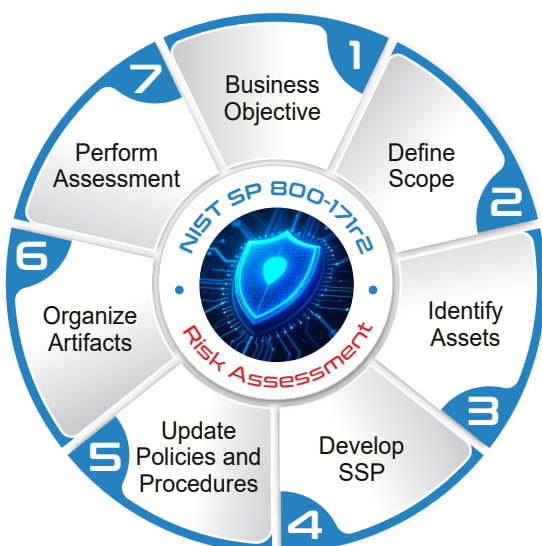


www.ecfirst.com



NIST SP 800-171r2 **Readiness**

- NIST SP 800-171r2 establishes 110 security requirements across 14 control families to protect CUI in nonfederal systems and organizations.
- Based on NIST SP 800-53 r4 and provides a risk-based framework for implementing safeguards such as access control, incident response, configuration management, and system integrity.
- Served as the foundation for compliance with DFARS 252.204-7012 and the CMMC 2.0 program.



NIST SP 800-171r2 | Risk Assessment Portal

Back

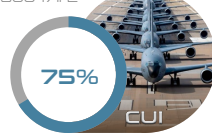


NIST SP
800-171r2



Intake Form

NIST SP
800-171r2



Organization Information

NIST SP
800-171r2



Roles

NIST SP
800-171r2



Assessment Questionnaire

NIST SP
800-171r2



POA&M

NIST SP
800-171r2



Reference Documents

NIST SP
800-171r2
Risk Assessment
Report



ecfirst | AI Defense, Beyond Cyber

Dashboard

TRACERSM
ASSET RISK MANAGEMENT

My Modules

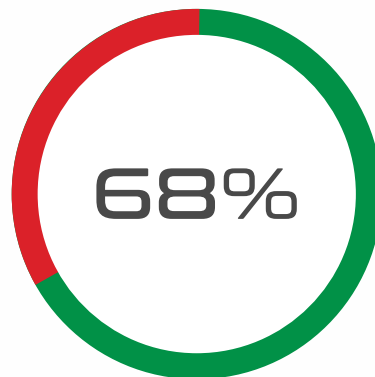
File Dashboard

Data Collection Forms

Compliance DCF
↳ NIST SP 800-171r2

- ↳ Intake Form
- ↳ Organization Information
- ↳ Roles
- ↳ Assessment Questionnaire
- ↳ POA&M
- ↳ Reference Documents

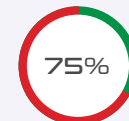
NIST SP 800-171r2 Status



Download Report

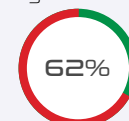
Data Collection Form Status

Access Control
Security Requirement 1



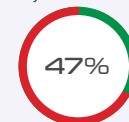
Details

Awareness & Training
Security Requirement 2



Details

Audit & Accountability
Security Requirement 3



Details

Input

Intake Form	15%
Assessment Info	20%
Roles	10%
Assessment Questions	5%

Reference

Client Uploaded Files	1	View
ecfirst Uploaded Files	2	View
Export DCF		Export

NIST SP 800-171r2 Assessment Planning

Intake Form

Contractor Details

Assessment Scope

Not Applicable (N/A) Practices

Inherited Practices

FCI Confirmation

CUI Confirmation

Other Contractor Details

Information Systems

Client Information

Contractor Information

Document Control Information

Document Approver(s) and Reviewer(s)

Document History

Executive Summary

Organization Information

NIST SP 800-171r2 Readiness Assessment Team (Username and Password will send to their Email ID)

Assessment Scope

Key Staff Roles

ISO or Key Security Executive

CIO or IT Director

IT Network Administrator

IT Server Administrator

IT Desktop/Enduser Administrator

IT Disaster Recovery

Security Incident Response Manager

Assessment Questionnaire

Export

Access Control1/22

Security Requirements Family14

Access Control22

Awareness and Training3

Audit and Accountability9

Configuration Management9

Identification and Authentication11

Incident Response3

Maintenance6

Media Protection9

Personal Security2

Physical Protection6

3.1.1

Does your organization enforce controls to ensure that system access is limited to only authorized users, processes, and devices?

Policy Implementation Status

YesNoNot ApplicableProcess Only, No Documentation Available

Uploaded Files

NIST.SP.800-171r2 (7).pdf

Overall Status

110Questions0Completed109Not Started

110Total Questions

Current Question1

Not Answered109

Answered Question(s)

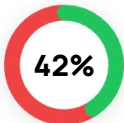
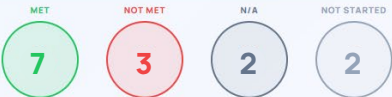
Incomplete Question(s)

NIST SP 800-171 r2 Executive Dashboard

14 Domains 110 Practices 320 Assessment Objectives Overall Tracker

SUMMARY

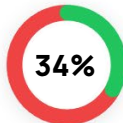
Overall Domain Status



Domain 1 - Access Control



Domain 2 - Awareness and Training



Domain 3 - Audit and Accountability



Preparation

SSP.ai
System Security Plan

FAVORITES

Dashboard

SSP Builder

Reports

COMPLIANCE

Controls Matrix

Evidence Library

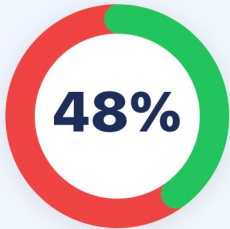
POA&M Tracker

ADMIN

Workflow Designer

NIST SP 800-171 r2 Executive Dashboard

OVERALL STATUS



Generate SSP
NIST SP 800-171 r2

GAP Analysis
NIST SP 800-171 r2

NIST SP 800 171 r2
SSP Report

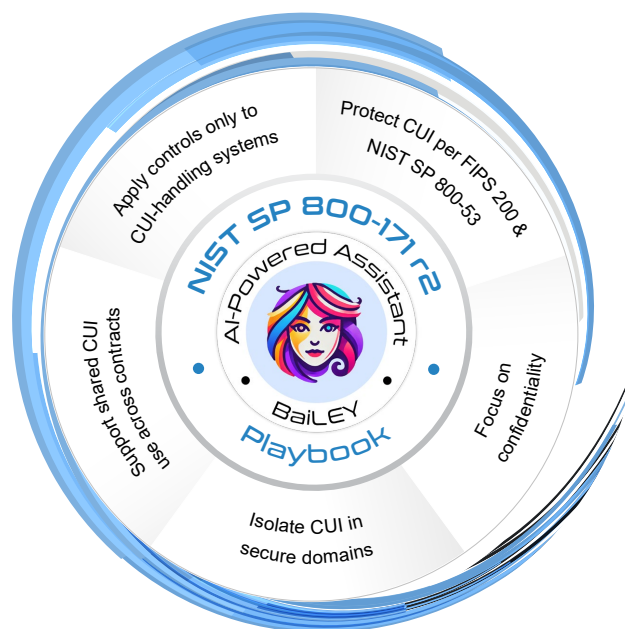
ABC
CORP



SSP.ai
System Security Plan



Quick Links

[Home](#)
[NIST SP 800-171r2](#)
[Source](#)
[Control Families](#)
[Reference](#)
[CMMC Level 2](#)
[Source \(Version 2.13\)](#)
[Policy Index](#)


Source



NIST SP 800-171r2



NIST SP 800-171A

Reference



Brochure



Infographics

Control Families

Control Families

1 ACCESS CONTROL (AC)

Basic (2)

Derived (20)

1.1: Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

Discussion: Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security.

1.2: Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Discussion: Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination. System account types include individual, shared, group, system, anonymous, guest, emergency, developer, manufacturer, vendor, and temporary. Other attributes required for authorizing access include restrictions on time-of-day, day-of-week, and point-of-origin.

2 AWARENESS AND TRAINING (AT)

Basic (2)

Derived (1)

3 AUDIT AND ACCOUNTABILITY (AU)

Basic (2)

Derived (7)

4 CONFIGURATION MANAGEMENT (CM)

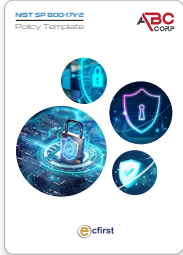
Basic (2)

Derived (7)

NIST SP 800-171r2 Toolkit



Policy Template



NIST SP 800-171r2 Report



Procedure Template



Home Course Access My Dashboard karthick

Quick Links

Home

NIST SP 800-171r2

Source

Control Families

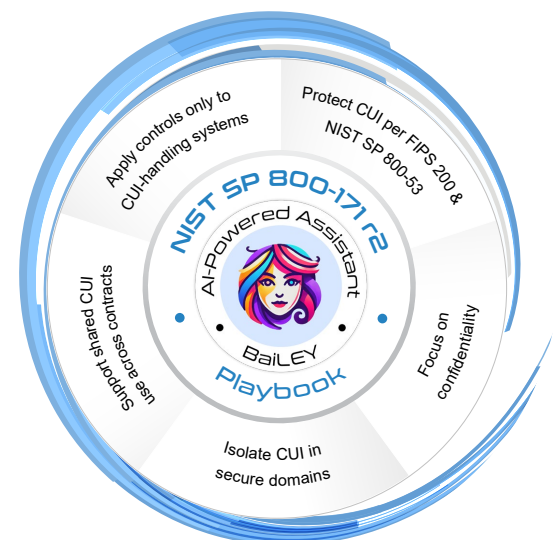
Reference

CMMC Level 2

Source (Version 2.13)

Policy Index

NIST SP 800-171r2 Playbook



Peter.Harvey@ecfirst.com



www.ecfirst.com