

Table of Contents

Why ecfirst for NIST?.....	2
Assessments.....	3
Toolkit	5
Certification Training.....	6
References.....	8

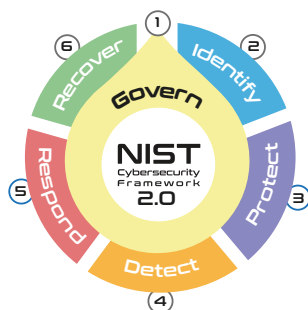
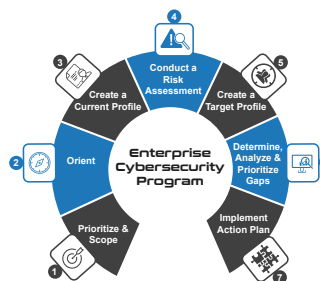


John.Schelewitz@ecfirst.com



www.ecfirst.com

NIST Signature Methodology



NIST 2.0 Assessment

Industry Leading Cybersecurity Certification Training



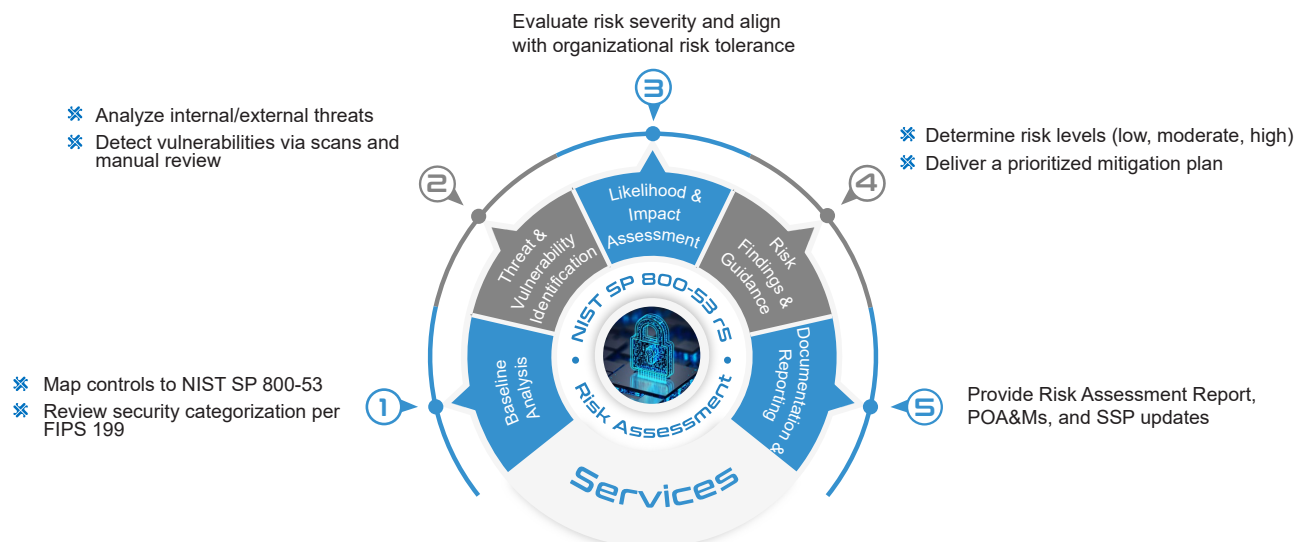
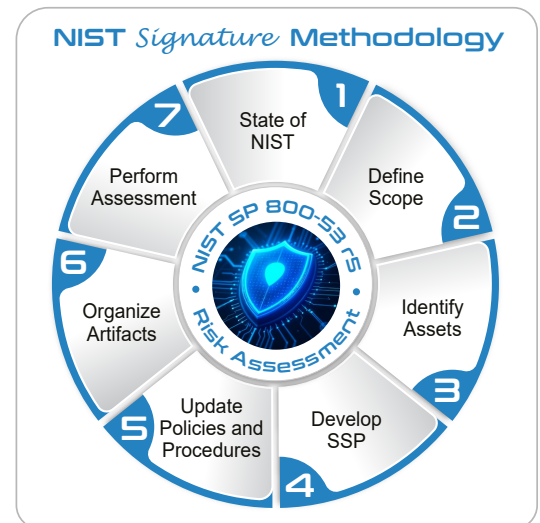
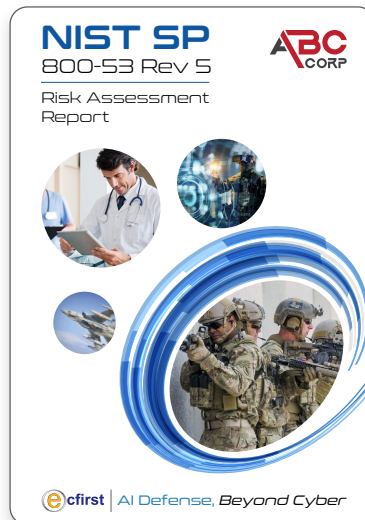
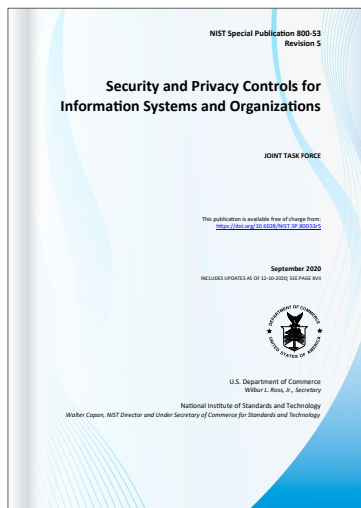
NIST Risk Assessment Report

NIST Compliance Attestation



NIST SP 800-53 r5

Risk Assessment



NIST Special Publication 800
NIST SP 800-171r3

**Protecting Controlled Unclassified
Information in Nonfederal Systems and
Organizations**

Ron Ross
Victoria Pillitteri
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-171r3>

May 2024



U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locantore, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST SP 800-171
Assessment Report

August 13, 2025



ecfirst | AI Defense, Beyond Cyber

NIST Signature Methodology



The diagram shows a circular process with 7 steps: 1. State of NIST, 2. Define Scope, 3. Identify Assets, 4. Develop SSP, 5. Update Policies and Procedures, 6. Organize Artifacts, 7. Perform Assessment. The center features a shield icon with 'NIST SP 800-171 Assessment' text.

TRACERSM
ASSET RISK MANAGEMENT

NIST SP 800-171 r3
Assessment Portal

ABC
CORP

NIST SP 800-171r3

Home | Data Collection Forms | NIST SP 800-171r3 | Phase 1 - Planning

NIST SP 800-171r3
100%
CUI
Intake Form

NIST SP 800-171r3
100%
CUI
Assessment Information

NIST SP 800-171r3
100%
CUI
Roles

NIST SP 800-171r3
100%
CUI
Assessment Questionnaire

NIST SP 800-171r3
100%
CUI
Planning

NIST SP 800-171r3
100%
CUI
POA&M

Reference Documents



A risk gauge with 'High' at the top, 'Medium' in the middle, and 'Low' at the bottom. The needle points towards the 'High' end. The text 'NIST SP 800-171r3 RISK' is on the gauge.

Requirements used in federal contracts/agreements

Protects CUI confidentiality in nonfederal systems

Organized into 17 security families (expanded from 14)


Applies when CUI is present & no specific safeguarding regulation exists

ODPs provide flexibility to tailor security requirements

Consistent protections: Federal and nonfederal systems treated the same

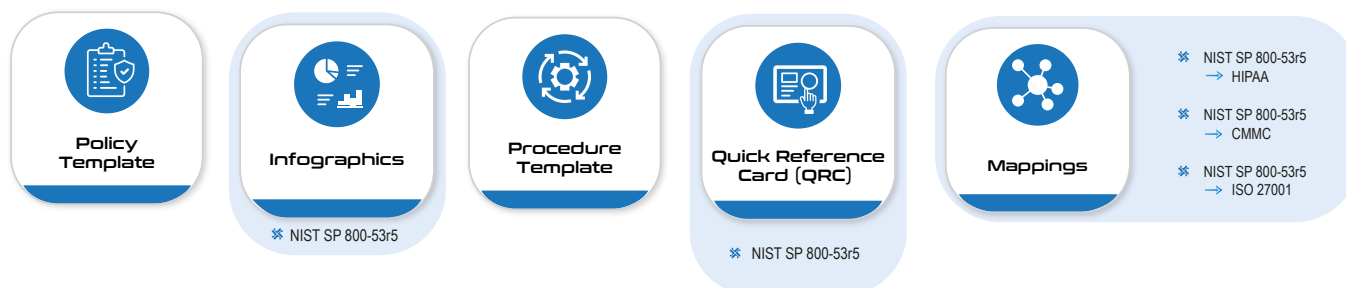
Applies only to components handling CUI

Confidentiality impact ≥ Moderate

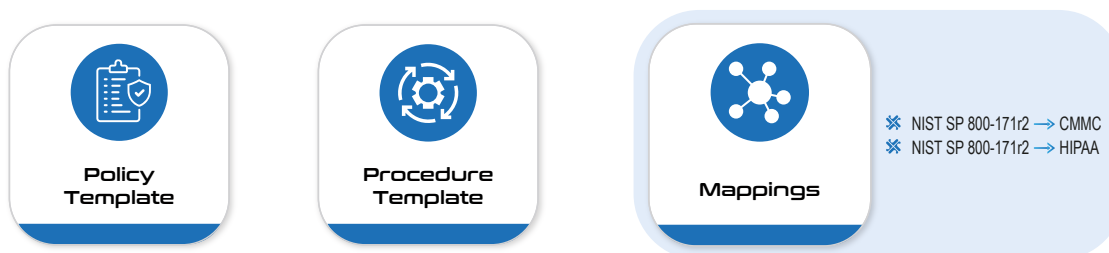


The diagram shows a circular process with 8 steps (1-8) around a central shield icon with a keyhole. The text 'NIST SP 800-171r3 Protect CUI' is in the center.

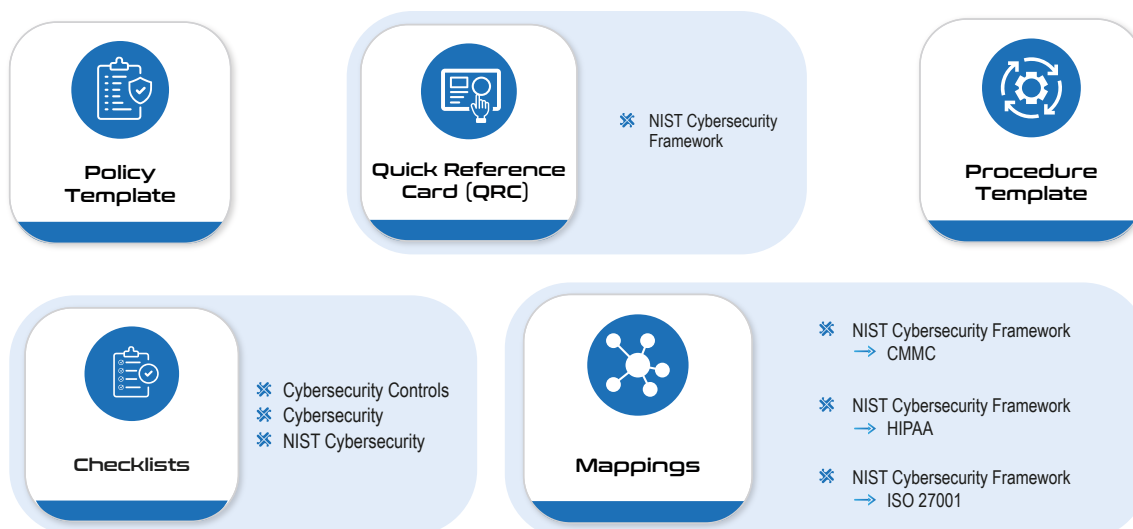
NIST SP 800-53r5 Toolkit



NIST SP 800-171r2 Toolkit



NIST Cybersecurity Framework Toolkit



The Industry's First Program Focused on
 Compliance and Cybersecurity Mandates



“Global perspective, extensive coverage of cyber mandates. Excellent updates on key security regulations.”

What's in it for you?

- ✘ Step through industry standards such as PCI DSS, GDPR, CCPA, CPRA, ISO 27001, and HIPAA
- ✘ Evaluate America's standard for compliance: NIST guidance and special publications
- ✘ Understand U.S. state government information security mandates (e.g. Texas, California, New York, and others)
- ✘ Explore best practices to build a credible compliance and cybersecurity program

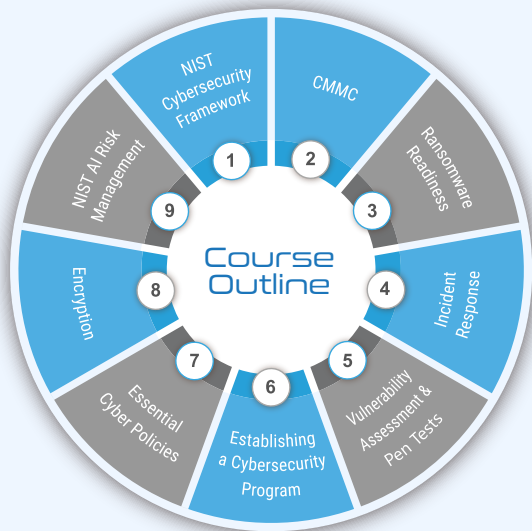


Digital Badge

ecfirst also offers a Digital Badge with your certification. There is no fee for this service and acceptance is totally up to you.



An Executive Cybersecurity Program



“ **Comprehensive cybersecurity program.** Excellent coverage of the NIST Cybersecurity Framework, CMMC & more. **Relevant scenarios & policies covered**, including encryption & ransomware. ”

What's in it for you?

- ✦ Examine how to establish a cybersecurity program based on the NIST Cybersecurity Framework
- ✦ Learn how to establish a credible Ransomware Readiness Program based on NIST Standards
- ✦ Walk through core components, organization, and CMMC Levels
- ✦ Review encryption implementation across the enterprise to mitigate business risk
- ✦ Examine NIST guidance for AI Risk Management



Digital Badge

ecfirst also offers a Digital Badge with your certification. There is no fee for this service and acceptance is totally up to you.



Learned a lot
Global coverage of topics
Excellent CSCS Academy Portal
Content focus applicable across industries

References

Complex topic made understandable
Refresher for cyber regulations
Tons of valuable information
Very relevant content

“

Highly informative and relevant—one of the best training programs I’ve attended.

”

“

Excellent material, exceptional presentation, and awesome case studies.

”

“

Good information and materials to elevate our compliance program.

”

“

Covered important frameworks and laws in cybersecurity.

”

“

CSCS Course was invaluable for building our compliance and security program.

”

“

Instructor made a complex topic more understandable. Highly recommended.

”

“

I appreciated the examples and scenarios that brought the material to life.

”

“

The training provided clarity on complex cloud compliance issues.

”

I loved the training

Prepared me for exam

Privileged to participate

Excellent introduction to NIST

References

Clear concise and to the point

Well organized and informative

CMMC was well covered

Great course!

“

Very knowledgeable instructor, provided timely and relevant examples and resources.

”

“

Great overview of cloud security with real-world relevance.

”

“

A crash course covering cybersecurity assessment, NIST and more.

”

“

The training was point on for the core material.

”



John.Schelewitz@ecfirst.com



www.ecfirst.com