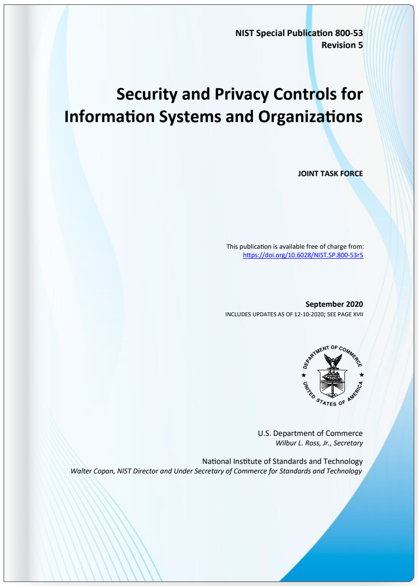
NIST SP 800-53 r5
Risk Assessment

ecfirst



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

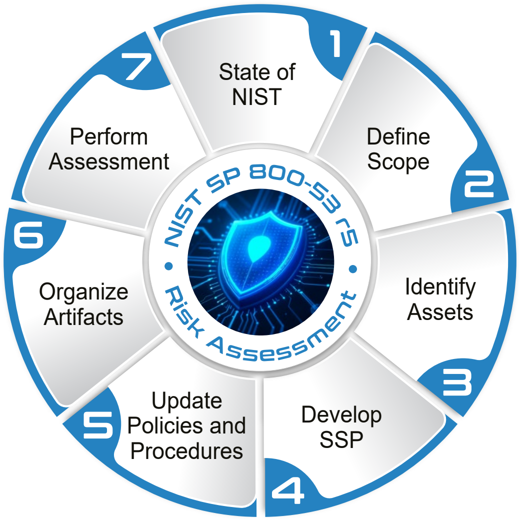
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

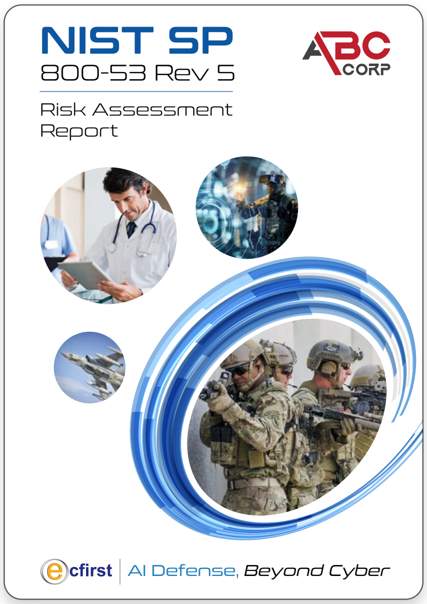
September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST *Signature* Methodology





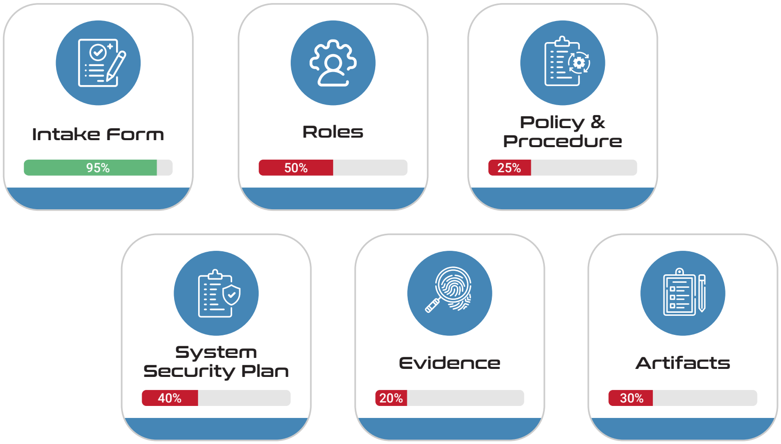
NIST SP
800-53 Rev 5

Risk Assessment Report

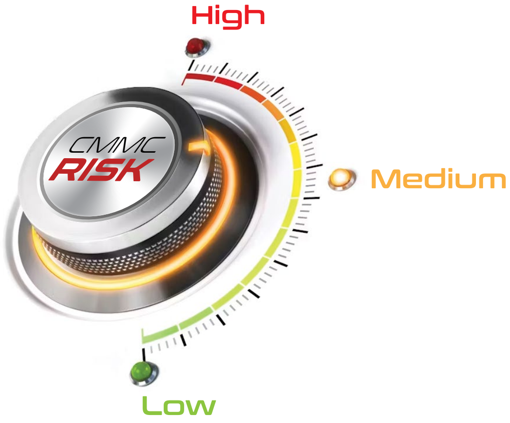
ABC CORP

ecfirst | AI Defense, *Beyond Cyber*

TRACER℠ ASSET RISK MANAGEMENT | NIST SP 800-53 r5 Risk Assessment Portal | ABC CORP



Intake Form	95%
Roles	50%
Policy & Procedure	25%
System Security Plan	40%
Evidence	20%
Artifacts	30%



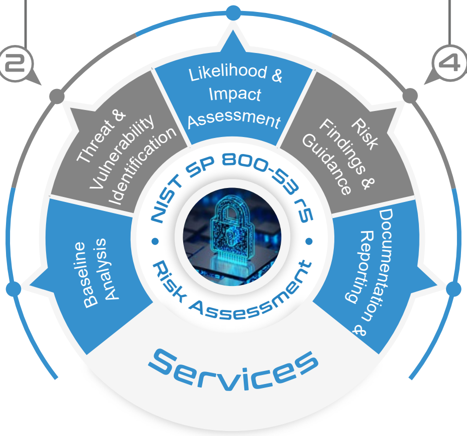
Evaluate risk severity and align with organizational risk tolerance ③

- Analyze internal/external threats
- Detect vulnerabilities via scans and manual review ②

④
- Determine risk levels (low, moderate, high)
- Deliver a prioritized mitigation plan

- Map controls to NIST SP 800-53
- Review security categorization per FIPS 199 ①

⑤ Provide Risk Assessment Report, POA&Ms, and SSP updates


Likelihood & Impact Assessment
Threat & Vulnerability Identification
Risk Findings & Guidance
Baseline Analysis
Documentation & Reporting
NIST SP 800-53 r5
Risk Assessment
Services

NIST SP 800-53 r5
Risk Assessment

ecfirst

NIST SP 800-171 r3 Dashboard

#	Family	Assessment Score	Risk Rating
1	Access Control	Met	Low
2	Awareness and Training	Met	Medium
3	Audit and Accountability	Met	Low
4	Configuration Management	Met	Low
5	Identification and Authentication	Met	Low
6	Incident Response	Met	Medium
7	Maintenance	Met	Low
8	Media Protection	Met	Low
9	Personal Security	Met	Low
10	Physical Protection	Met	High

Weaknesses

Partial Control Alignment Gaps. Certain controls have been identified as partially met and are being actively tracked through a defined Plan of Action and Milestones (POA&M) for remediation.

Threats

Evolving Threat Landscape. The healthcare sector continues to face persistent threats including ransomware, social engineering, and insider threats. These risks require constant adaptation of security controls and user education.

Opportunities

Policy Refinement and Role-Specific Enhancements. Continued refinement of policies especially those addressing advanced technologies such as AI, mobile device management, and BYOD will strengthen compliance posture.

Strengths

Mature Access Control and Account Management Framework. CareSource enforces strong access controls, including account provisioning/deprovisioning through SailPoint, role-based access assignments, and session timeout policies for all major platforms (Facets, NetworX, CES).

NIST SP 800-53 r5 Dashboard

#	Family	Assessment Score	Risk Rating
1	Access Control (AC)	Met	Low
2	Awareness and Training (AT)	Met	Medium
3	Audit and Accountability (AU)	Met	Low
4	Assessment, Authorization, and Monitoring (CA)	Met	Medium
5	Configuration Management (CM)	Met	High

Strengths

Culture of Compliance. CareSource demonstrates a strong commitment to compliance, supported by leadership and the Board of Directors. The organization fosters a culture that values privacy, security, risk management, and regulatory alignment, which is evident across multiple operational levels.

Opportunities

Policy Enhancement. CareSource has incorporated ecfirst-provided templates covering Ransomware Readiness, AI Risk Management, and Online Tracking Technologies. These templates present an opportunity for deeper refinement of existing policies, helping the organization strengthen emerging risk domains.

CAP

It is recommended that CareSource update relevant policy documents to establish an annual POA&M review schedule aligned with control assessment activities. To support this cadence, the organization may consider enhancing the POA&M itself by ensuring milestones are well-defined, completion dates are identified, and progress is regularly reviewed and updated.

Report Card

Low — Risk Rating

Met 4.84 — Assessment Score

Threats

General Threats to the Healthcare Environment - Not Specific to CareSource

Health Industry Top 5 Cybersecurity Threats. HHS has defined these top five threats: social engineering; ransomware; loss or theft of equipment; insider threats; accidental or malicious data loss; and attacks against medical devices that are connected to the network.

Weaknesses

Partial Gaps in NIST 800-53 Rev. 5 Compliance. While CareSource has implemented a broad array of security controls, some remain partially aligned with the NIST 800-53 Revision 5 Moderate Baseline. These gaps are tracked in the organization's Plan of Action and Milestones (POA&M), and remediation efforts are actively underway.

✉ Peter.Harvey@ecfirst.com

www.ecfirst.com