Program CATALOG

ecfirst





aiCRP
AI Cyber Risk Professional

HITRUST
Authorized External Assessor

CYBER AB
CMMC CERTIFICATION
AUTHORIZED C3PAO

CYBER AB
CMMC CERTIFICATION
REGISTERED PRACTITIONER ORGANIZATION
RPO

HIPAA™ Academy

TRACER℠
ASSET RISK MANAGEMENT

Message from the Chief Executive

Welcome to ecfirst!

We deliver solutions where **precision** in execution is not optional - it's the standard.

Why ecfirst?

With **humility** at our core, we approach every engagement with **passionate** dedication and unwavering **devotion**. Your priorities become our priorities—executed with surgical focus and relentless follow-through.

We proudly serve organizations across all 50 states and worldwide, always anchored in a single mission: to earn and deepen your trust at every step. Our relationships are built to last, and every project is an opportunity to deliver measurable, meaningful value.

Our commitment is unconditional. Your satisfaction is not a goal - it's our guarantee. We would be honored to collaborate on your AI, cyber risk, and compliance initiatives, bringing the full force of the **ecfirst DNA** to your success.

Let's make it happen!



Uday Ali Pabrai

Global AI Cyber Defense Thought Leader

LCCA · Virtual CAIO Chief Artificial Intelligence Officer · CCP · CISSP · HITRUST CCSFP

© ecfirst. All Rights Reserved. 2026

Leadership



Ali Pabrai
Chairman & CEO



Allen Nguyen
President & Co-founder



Debbie Burke
VP of Operations and Finance



Mike Turpin
VP of Global Assessments



Casey McLoughlin
Chief of Staff



Ben Miller
Director of Cybersecurity &
Sr. Security Engineer



Nicole Kramer
Director, Global Assessment Services



Will Allen
Team Lead, Assessments



Dave Ekstrom
Team Lead, HITRUST



Nathan Nelson
Team Lead, HITRUST



Audra Curtis
Team Lead, Business Development &
Certification Program Management



Heather Orbich
Team Lead, Client Operations &
Digital Marketing



Arshiyaan Pabrai
AI Governance &
CMMC Cyber Advisor

© ecfirst. All Rights Reserved. 2026

Table of Contents

AI
- Why ecfirst for AI 5
- Virtual CAIO Program 6
- AI Risk Management Assessment 7
- aiCRP Certification 8

Certification Training
- AI | HIPAA | Cyber Defense 9
- CHP Certification 10
- CSCS™ Certification 11
- CCSA℠ Certification 12
- CMMC for Executives 13

HITRUST
- Why ecfirst for HITRUST 14
- HITRUST e1 Certification 15
- HITRUST i1 Certification 16
- HITRUST r2 Certification 17

HIPAA
- Why ecfirst for HIPAA 18
- Risk Assessment 19
- HIPAA End-User Training 20

NIST
- Why ecfirst for NIST 21
- NIST Risk Assessment 22
- NIST Cybersecurity Framework 2.0 23
- NIST SP 800-53 r5 24
- NIST SP 800-171 r2 25
- NIST SP 800-171 r3 26
- NIST SP 800-161 r1 27

Cyber Defense
- Cybersecurity Assessment 28
- CloudFirst Assessment 29
- Pen Test 30
- Red Team Exercise 31
- Online Tracking Assessment 32
- Social Engineering 33
- TRACER℠ Portal 34

CMMC
- Why ecfirst for CMMC 35
- CCP Training 36
- CCA Training 37
- CMMC Advisory Services 38
- CMMC Assessment Process 41
- CMMC Readiness 42

Compliance
- Ransomware Readiness BIA | DRP 43
- Managed Compliance 44
- On Demand Consulting 45
- VISO & Infosec Staffing Program 46
- PCI DSS Pre-Assessment 47
- GDPR Compliance Pre-Assessment 48

Online Store
- Online Store 49
- Toolkits Cyber | CMMC | HIPAA | NIST 50
- Playbooks HIPAA | CMMC | CAP | CUI | AI | HITRUST 62
- SSP Playbook | Template | Portal 68

Client References
- AI 72
- CHP 73
- CSCS™ 74
- CCSA℠ 75
- HITRUST 76
- HIPAA 77
- CMMC 78
- CCP 79
- CCA 80

© ecfirst. All Rights Reserved. 2026

AI | Why ecfirst ?

ecfirst



AI Governance Methodology

Virtual AI Governance and Risk Management Program

Virtual CAIO
Chief Artificial Intelligence Officer



aiCRP
AI Cyber Risk Professional
Online | Self-Paced

AI Cyber Risk Certification Training

AI Governance Reference









AI Governance Playbook

AI-Powered Assistant BaiLEY

Learn More

AI and Gen AI Governance Playbook

AI Risk Management Assessment
AI Cyber Certification

HITRUST
Authorized External Assessor







AI Toolkit
www.ecfirst.biz/ai

© ecfirst. All Rights Reserved. 2026

AI | Why ecfirst ?

ecfirst



AI Governance Methodology

Virtual AI Governance and Risk Management Program

Virtual CAIO
Chief Artificial Intelligence Officer



aiCRP
AI Cyber Risk Professional
Online | Self-Paced

AI Cyber Risk Certification Training

AI Governance Reference









AI Governance Playbook

AI-Powered Assistant BaiLEY

Learn More

AI and Gen AI Governance Playbook

AI Risk Management Assessment
AI Cyber Certification

HITRUST®
Authorized External Assessor







AI Toolkit
www.ecfirst.biz/ai

© ecfirst. All Rights Reserved. 2026

AI | Why ecfirst ?

ecfirst



AI Governance Methodology

Virtual AI Governance and Risk Management Program

Virtual CAIO
Chief Artificial Intelligence Officer



aiCRP
AI Cyber Risk Professional
Online | Self-Paced

AI Cyber Risk Certification Training

AI Governance Reference









AI Governance Playbook

AI-Powered Assistant BaiLEY

Learn More

AI and Gen AI Governance Playbook

AI Risk Management Assessment
AI Cyber Certification

HITRUST®
Authorized External Assessor







AI Toolkit
www.ecfirst.biz/ai

© ecfirst. All Rights Reserved. 2026

AI Governance

Establish a customized AI Governance and Risk Management program, tailored for your organization. The virtual CAIO program from ecfirst, provides opportunities in the following areas,

- Establish an AI Governance program
- Build a customized AI acceptable use policy
- Develop an AI risk management policy
- Access to aiCRP an online, self-paced training program (Complimentary)
- Tailored presentations to senior leadership and the Board
- Perform an AI cyber risk assessment based on the NIST AI RMF

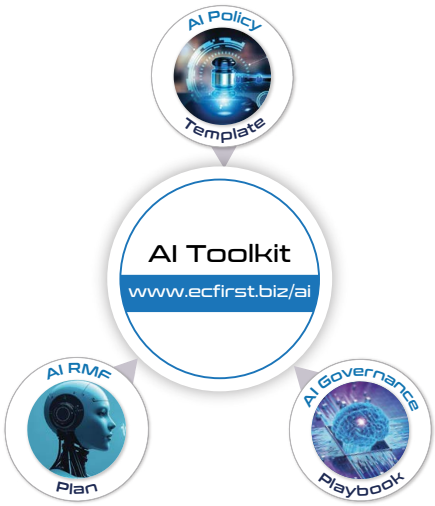
Customized | Flat Rate | Fixed Cost | Flexible

AI Governance Program









© ecfirst. All Rights Reserved, 2026

AI Risk Management
Assessment

ecfirst

1



2



3



NIST AI 100-1 • ISO 23894 • ISO 42001

AI Risk Assessment

raksha defense

ABC CORP

- Organization Questionnaire
- Scoping Questionnaire
- Policy
- Assessment
- Report Dashboard



Certificate

Sources



ISO 23894



NIST AI 100-1



ISO 42001

© ecfirst. All Rights Reserved, 2026

aiCRP
AI Cyber Risk Professional
Online | Self-Paced

ecfirst

The Industry's First AI Cyber Risk Management Training Program

HIMSS | CEU 8 Hours



AI Governance Risk Management Playbook

Gen AI Playbook



What's in it for you?

- Review valued AI framwork resources
  - NIST AI RMF
  - ISO 42001
  - New York
  - Colorado
  - Texas
  - Utah
- Understand EU AI Act requirements and risk classifications
- Step through a sample AI risk management policy
- Identify AI cyber defense controls
- Determine key phases for an enterprise AI risk assessment

AI Exam Specifications



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.

aiCRP

© ecfirst. All Rights Reserved, 2026

Healthcare Industry's First & Leading HIPAA Credential

CEU 16 Hours

- Analyze the latest updates in HIPAA Privacy, HIPAA Security, and HITECH Breach mandates
- Examine OCR HIPAA settlements to understand the bar for HIPAA compliance
- Review HIPAA compliance challenges and best practices for Covered Entities and Business Associates
- Understand HIPAA Safe Harbor
- Understand AI governance, risk management, and compliance considerations for healthcare organizations

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

CEU 16 Hours

- 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

An Executive Cybersecurity Program

CEU 8 Hours

- 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

An Executive CMMC Program

CEU 8 Hours

- Identify and apply official CMMC implementation and assessment guidance
- efine scope by identifying CUI systems and mapping assets to workflows for compliance
- Maintain an SSP outlining control responsibilities and provide evidence to validate implementation during assessment
- Manage and sustain CMMC compliance through continuous governance

© ecfirst. All Rights Reserved. 2026

CHP Certified HIPAA Professional
HIPAA Academy
Virtual | Online | Public

ecfirst

Healthcare Industry's First & Leading HIPAA Credential

HIMSS CEU 16 Hours



HIPAA Playbook

AI-Powered Assistant BaiLEY



What's in it for you?

- Analyze the latest updates in HIPAA Privacy, HIPAA Security, and HITECH Breach mandates
- Examine OCR HIPAA settlements to understand the bar for HIPAA compliance
- Review HIPAA compliance challenges and best practices for Covered Entities and Business Associates
- Understand HIPAA Safe Harbor
- Understand AI governance, risk management, and compliance considerations for healthcare organizations

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

CHP Certified HIPAA Professional
HIPAA Academy

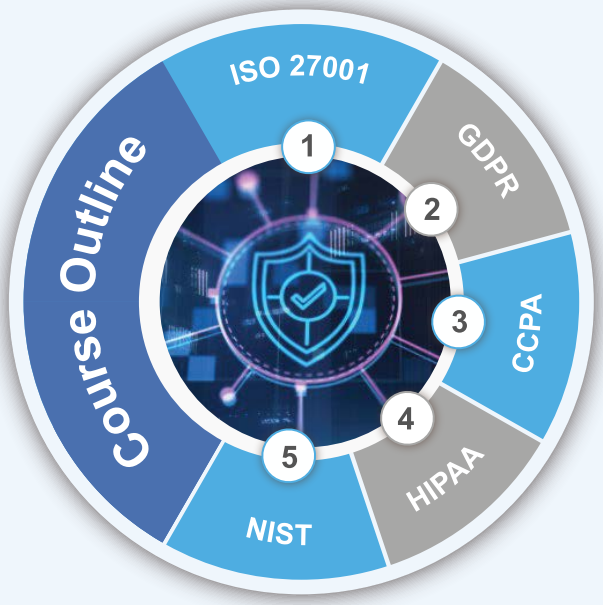
© ecfirst. All Rights Reserved. 2026

CSCS™
CERTIFIED SECURITY COMPLIANCE SPECIALIST
Online | Self-Paced

ecfirst

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

HIMSS APPROVED EDUCATION PARTNER | CEU 16 Hours



> **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

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

CSCS™
CERTIFIED SECURITY COMPLIANCE SPECIALIST

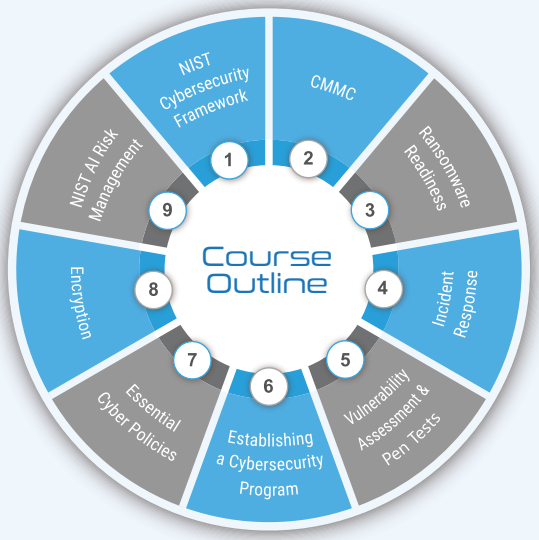
© ecfirst. All Rights Reserved. 2026

CCSA SM
Certified Cyber Security Architect
Online | Self-Paced

ecfirst

An Executive Cybersecurity Program

HIMSS APPROVED EDUCATION PARTNER | CEU 8 Hours



> **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.

CCSA SM
Certified Cyber Security Architect

© ecfirst. All Rights Reserved. 2026

CMMC
For Management
Virtual | Online

ecfirst



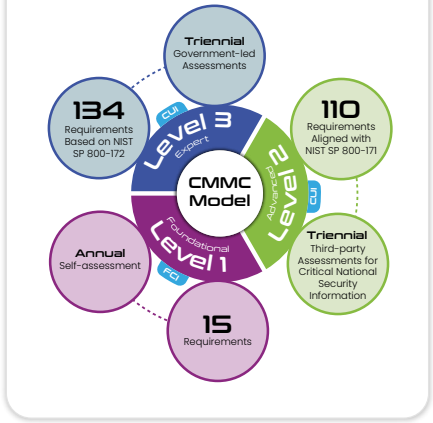
Learning Objectives

- Identify and use official CMMC guidance for implementation and assessment.
- Define scope by locating systems and assets handling CUI.
- Map assets to systems and workflows for compliance readiness.
- Create and maintain an SSP detailing control implementation and responsibilities.
- Prepare and present evidence to demonstrate control implementation during assessment.

CMMC Academy
Cybersecurity Maturity Model Certification

Welcome Home Dashboard Logout

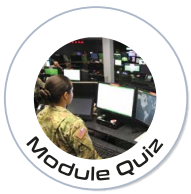
CMMC Playbook



CMMC For Management









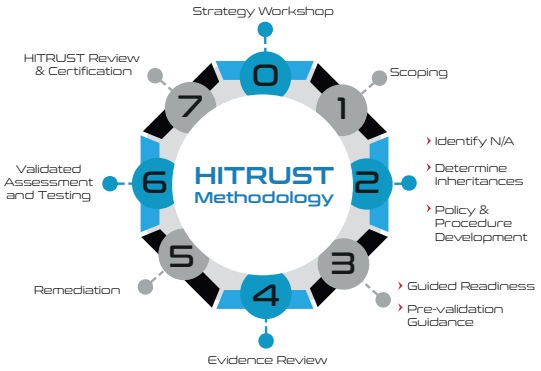
© ecfirst. All Rights Reserved, 2026

HITRUST
Why ecfirst?

HITRUST Authorized External Assessor | ecfirst

ecfirst is one of the few HITRUST External Assessment Organizations to achieve HITRUST Certification for our own company.

Signature Methodology



> "ecfirst walked us through every step of the way in achieving our organization's HITRUST goal"

Devoted to Client Success

HITRUST Assessor Council

Member, AI Committee

HITRUST Commitment

COLLABORATE '24 CHARTING THE PATH FORWARD | ISACA CONFERENCE

HITRUST Thought Leadership

Knowledge Transfer

At every step ensures cost and time efficiency

Frequent updates and Touch-point calls

Weekly HITRUST Status

Single Point-of-Contact

For HITRUST Engagements

HITRUST Queries

Swift Team Response

Flexible Terms

e1 · i1 · r2 · AI

e1 HITRUST CERTIFIED | i1 HITRUST CERTIFIED | r2 HITRUST CERTIFIED

Monthly Payment

Multi year Engagement

Flat Price

© ecfirst. All Rights Reserved. 2026

HITRUST e1 Certification

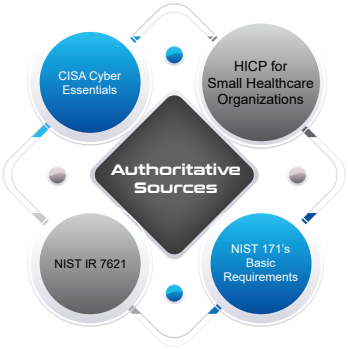
HITRUST Authorized External Assessor | ecfirst

e1 Essentials

Essentials, 1-year (e1) Validated Assessment Foundational Cybersecurity

44 HITRUST e1





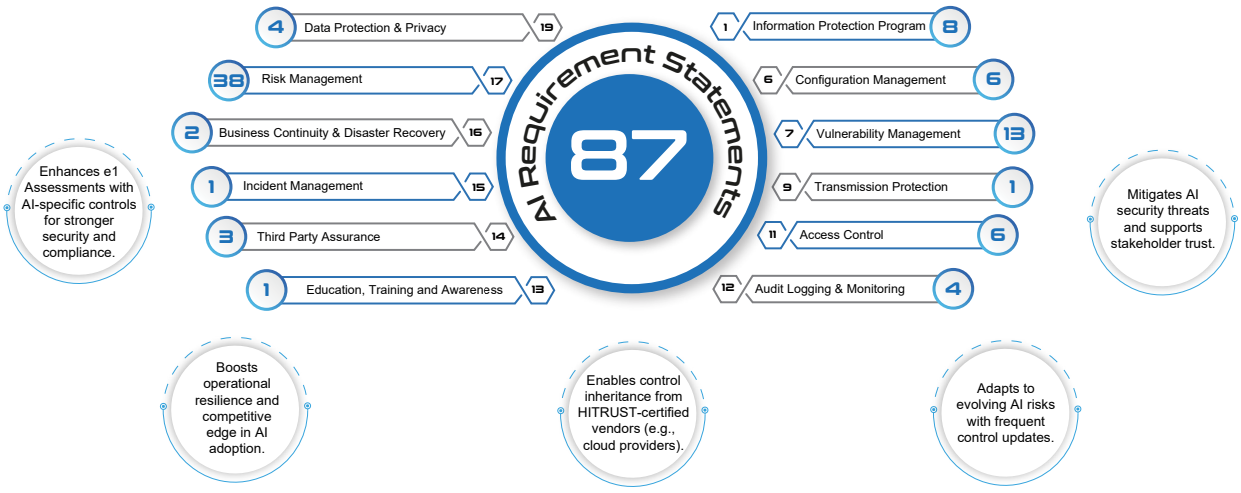
HITRUST e1 and HIPAA

- Aligns with HIPAA Security Rule
  Provides essential controls for securing ePHI
- Covers access control, audit logging, data integrity, and transmission security
- Ideal for Small Organizations
- Cost-Effective
- Ensures Structured Policies
- Supports mitigation and compliance with HIPAA core requirements
- Provides evidence-based confirmation of HIPAA alignment

Requirement Statements

	BA	CE
HIPAA Privacy, Security, and Breach	130	220
HIPAA Security and Breach	115	118
HIPAA Privacy and Breach	175	171
HIPAA Privacy and Security	125	215
HIPAA Privacy	67	154
HIPAA Security	109	108
HITECH Breach	51	55

HITRUST e1 and AI



© ecfirst. All Rights Reserved. 2026

HITRUST i1 Certification

HITRUST Authorized External Assessor | ecfirst

i1 Key Highlights

- Leading security practices with HITRUST-curated controls
- Reliable assurance against evolving cyber threats
- Threat-adaptive controls aligned with HITRUST assessments
- Operational maturity through pre-set control requirements
- Flexible implementation with carve-outs and third-party inclusions

i1 Compliance Mandates



i1 Requirements

	Domain	
1	Information Protection Program	15
2	Endpoint Protection	7
3	Portable Media Security	6
4	Mobile Device Security	6
5	Wireless Security	7
6	Configuration Management	9
7	Vulnerability Management	12
8	Network Protection	9
9	Transmission Protection	9

	Domain	
10	Password Management	6
11	Access Control	21
12	Audit Logging & Monitoring	9
13	Education, Training, and Awareness	6
14	Third Party Assurance	8
15	Incident Management	7
16	Business Continuity & Disaster Recovery	10
17	Risk Management	10
18	Physical & Environmental Security	15
19	Data Protection & Privacy	10

182 HITRUST i1

HITRUST i1 Rapid Certification

Organizations must have an i1 Validated Assessment with Certification and a full MyCSF subscription. Lite Bundle users must upgrade to a Professional subscription.

Scope

Includes all current i1 requirements, with some scores carried over. Evaluates new requirements (if applicable), a sample of 60 prior requirements, and N/A statements. Optional updates for non-required statements.

60 HITRUST i1 Rapid

Timeline

180 Before Expiration — Eligibility Questionnaire becomes available.

Assessment object auto-generated in MyCSF, with a **30-day** planning period and a **90-day** fieldwork period.

120 Before Expiration

© ecfirst. All Rights Reserved. 2026

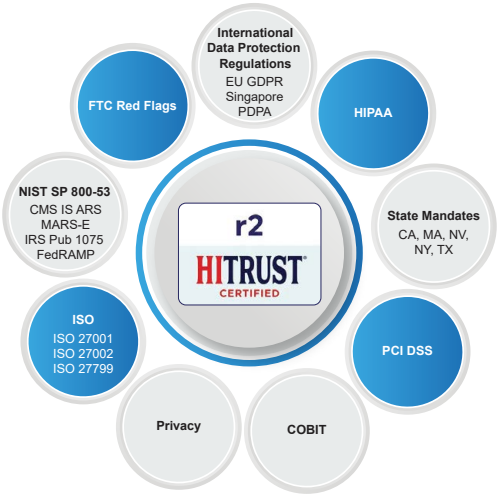
HITRUST r2 Certification

HITRUST Authorized External Assessor | ecfirst

r2 Key Highlights

Comprehensive Controls	Up to 250 aligned with major standards
Customizable	Select controls based on risk and compliance needs
HIPAA & NIST CSF Reporting	Automated evidence collection and compliance reports
Proven Assurance	Transparent results for stakeholder confidence
Control Inheritance	Reuse prior assessments and cloud provider assurances
Efficient Remediation	Identify and fix control gaps

HITRUST r2 Certification



HITRUST AI Risk Requirements





HITRUST AI Cybersecurity Requirements



HITRUST's AI Assurance program provides certification and an insight report, integrating AI frameworks into MyCSF to streamline assessments and enhance security.

© ecfirst. All Rights Reserved. 2026

HIPAA
Why ecfirst?

HIPAA™ Academy | ecfirst



HIPAA *Signature* Methodology

Industry Leading HIPAA Certification Training

Updated with NPRM

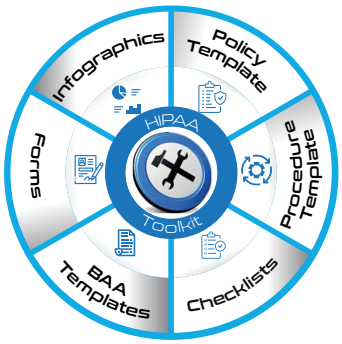
CHP Certified HIPAA Professional
HIPAA Academy

HITRUST
Authorized External Assessor

Delivering HITRUST Certification Since 2016

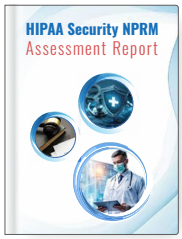
AI Powered HIPAA Playbook





HIPAA Toolkit
www.ecfirst.biz

HIPAA NPRM Assessment





HIPAA Compliance Attestation

© ecfirst. All Rights Reserved, 2026

Risk Assessment

HIPAA | NIST Cybersecurity Framework 2.0
Online Tracking | Cyber Assessment | Pen Test

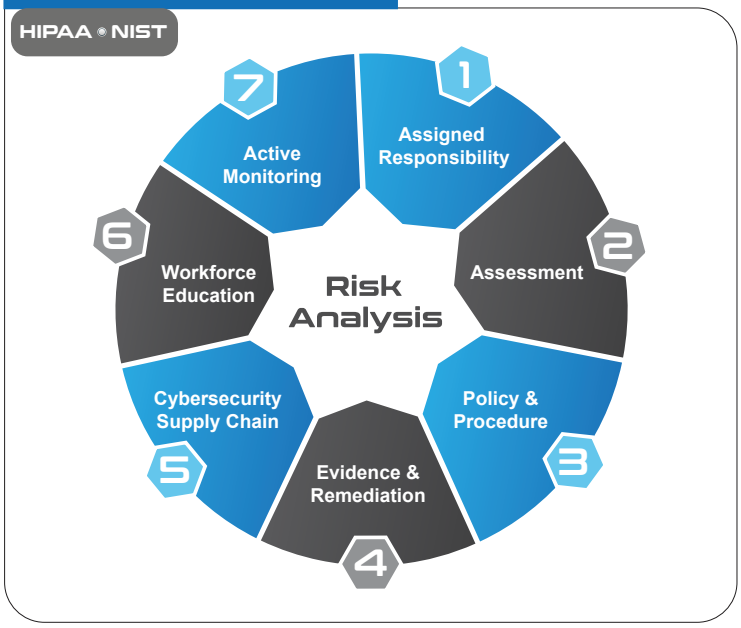
ecfirst

Every organization must conduct a thorough and comprehensive assessment of the potential risk and vulnerability to the confidentiality, integrity and availability of all PII.

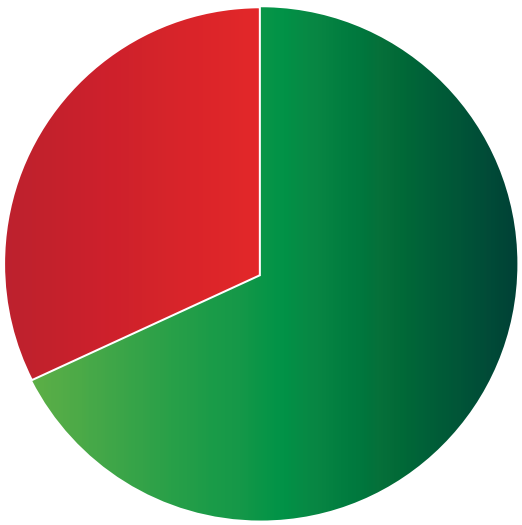
HIPAA Mandates

Grade	Security Rule
D	Administrative Safeguards
F	Physical Safeguards
A	Technical Safeguards
B	Organizational Requirements
F	Policies, Procedures, and Documentation
Privacy Rule	
B	Administrative Requirements
A-	Uses and Disclosures
Breach Notification	
C	Reporting

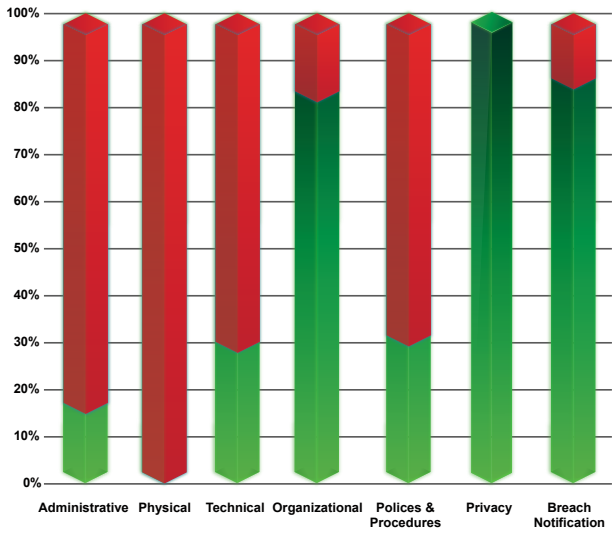
Signature Methodology



Compliance Status



Implementation Specifications



Met Not Met

© ecfirst. All Rights Reserved. 2026

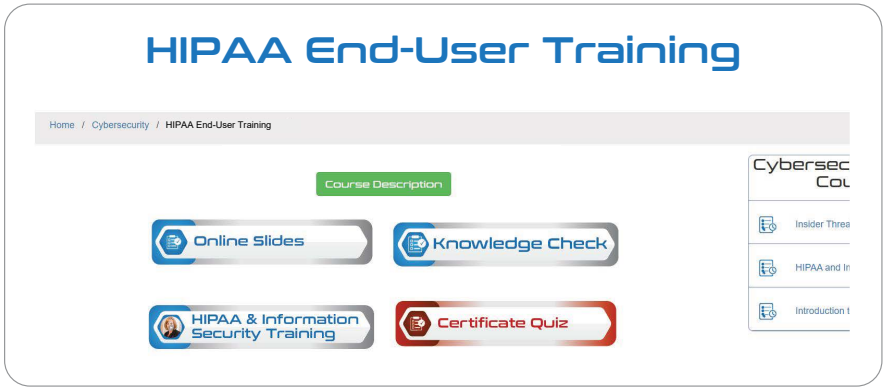
HIPAA
End-User Training

HIPAA™ Academy | ecfirst

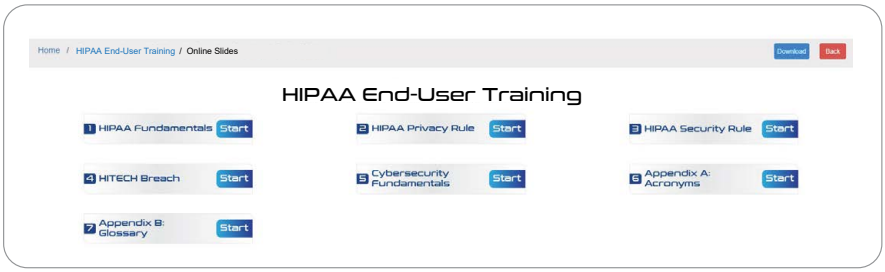
HIPAA End-User Package

- End-to-end training content covering HIPAA Privacy, HIPAA Security, HITECH Breach, the HIPAA Final Rule, and more
- Practice quiz to emphasize important concepts
- HIPAA End-User Certificate Exam
- Several sample documents for reference including HIPAA quick reference cards, flash cards, and more

HIPAA™ Academy Portal





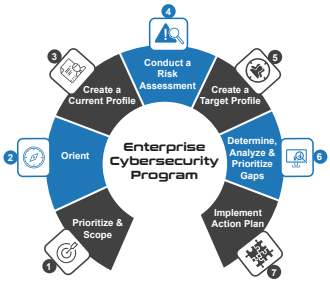


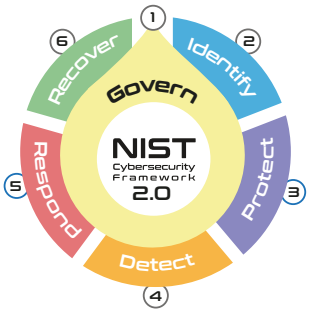
© ecfirst. All Rights Reserved, 2026

NIST
Why ecfirst?

ecfirst

NIST *Signature* Methodology





NIST 2.0 Assessment

Industry Leading Cybersecurity Certification Training

CCSA℠
Certified Cyber Security Architect



NIST Risk Assessment Report

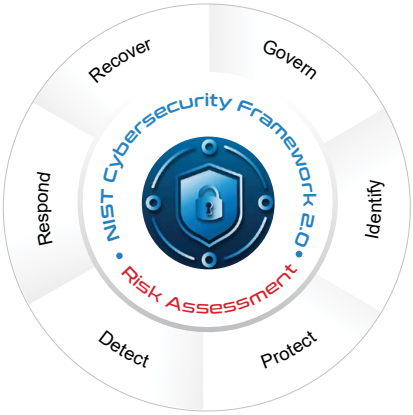
NIST Compliance Attestation



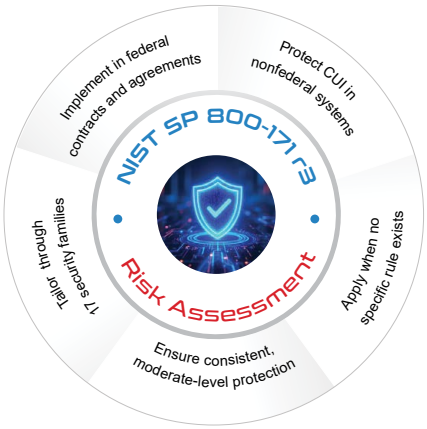
© ecfirst. All Rights Reserved, 2026

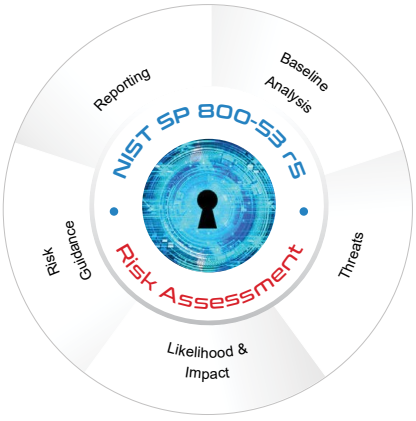


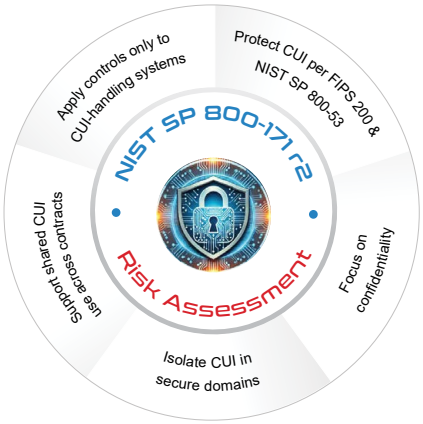






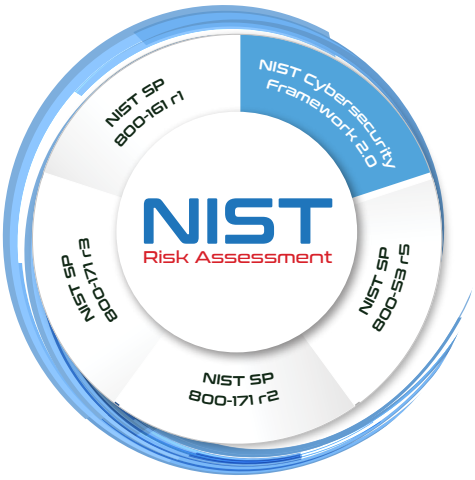


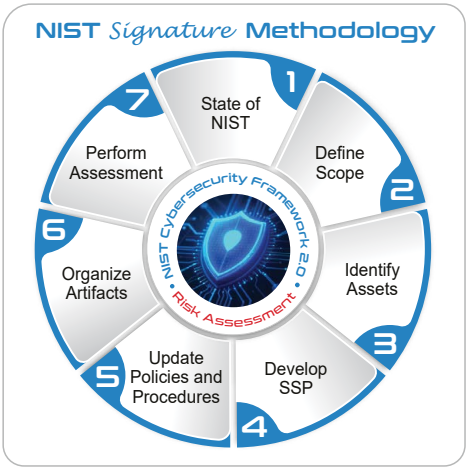




© ecfirst. All Rights Reserved, 2026

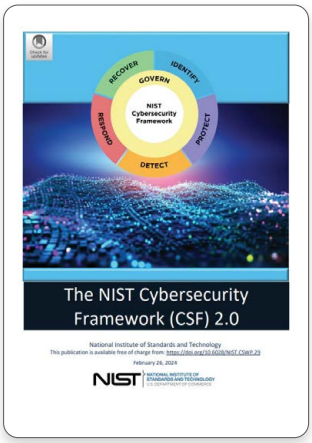
NIST Cybersecurity Framework 2.0 Risk Assessment

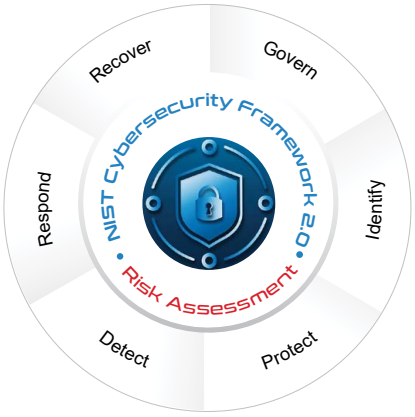






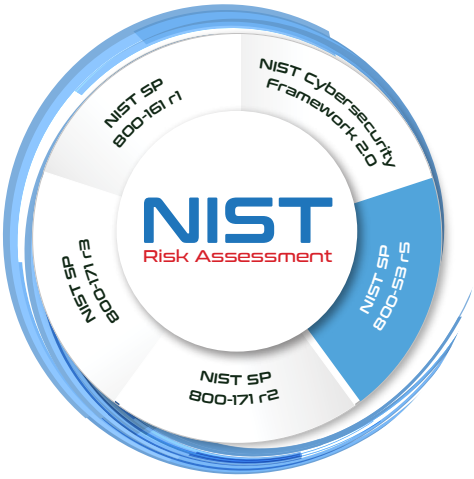


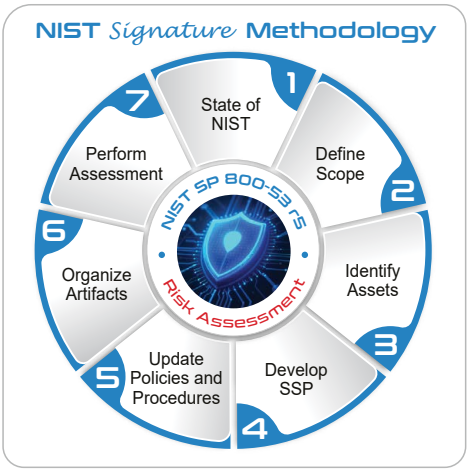




© ecfirst. All Rights Reserved, 2026

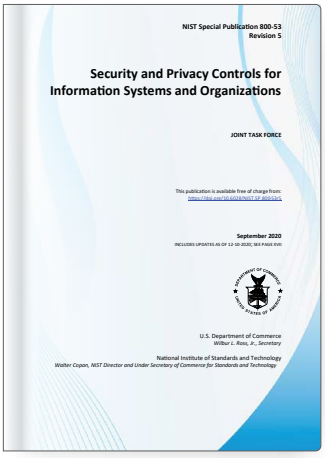
NIST SP 800-53r5
Risk Assessment

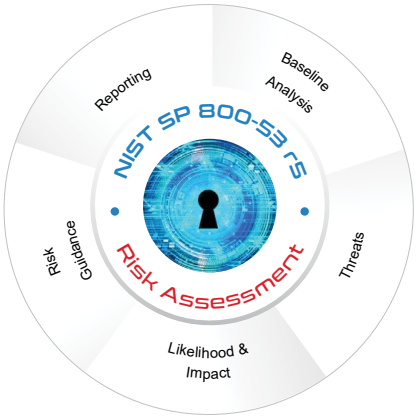








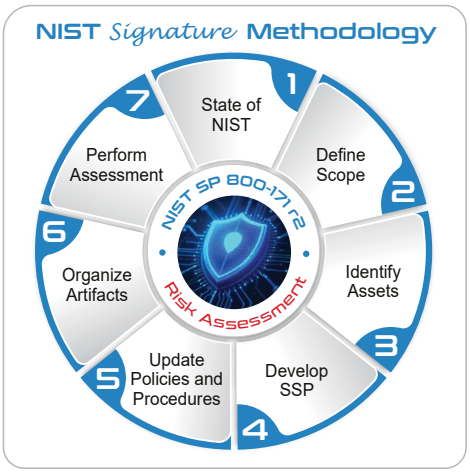




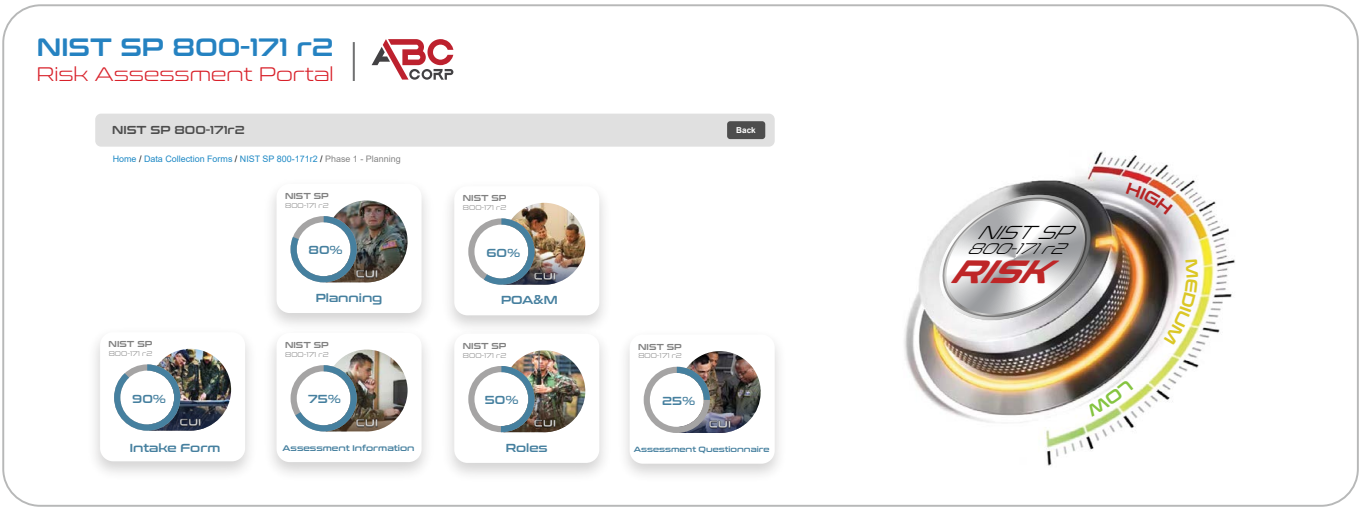
© ecfirst. All Rights Reserved. 2026

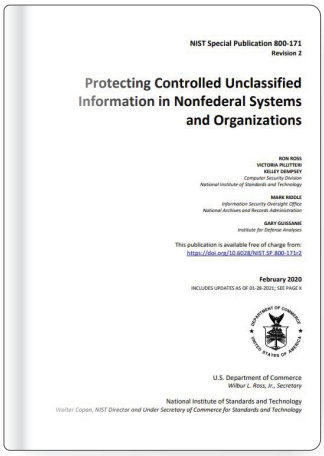
NIST SP 800-171r2
Risk Assessment

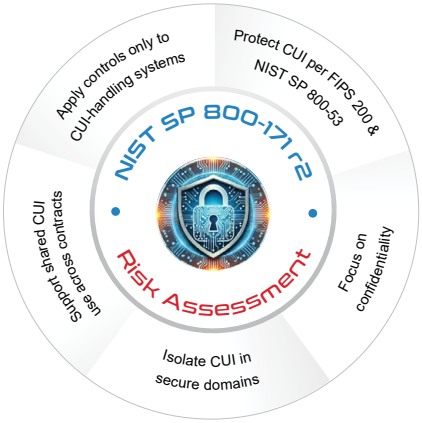








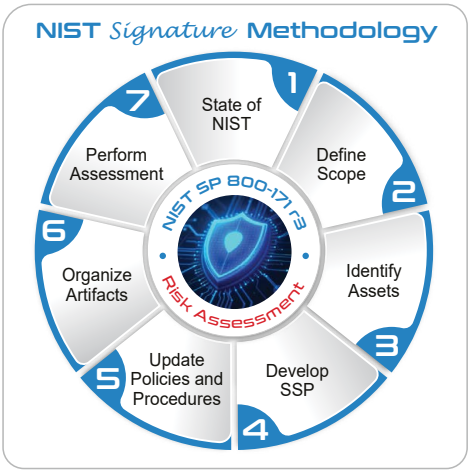


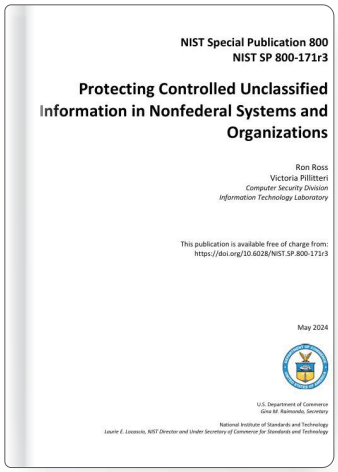


© ecfirst. All Rights Reserved, 2026

NIST SP 800-171r3
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

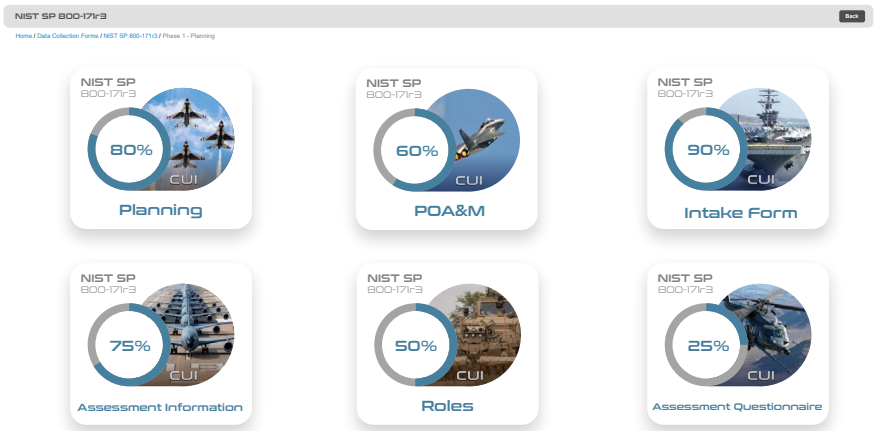
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r3

May 2024

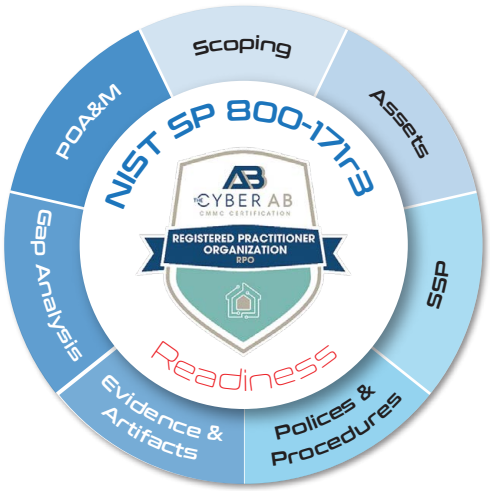
U.S. Department of Commerce
Gina M. Raimondo, Secretary

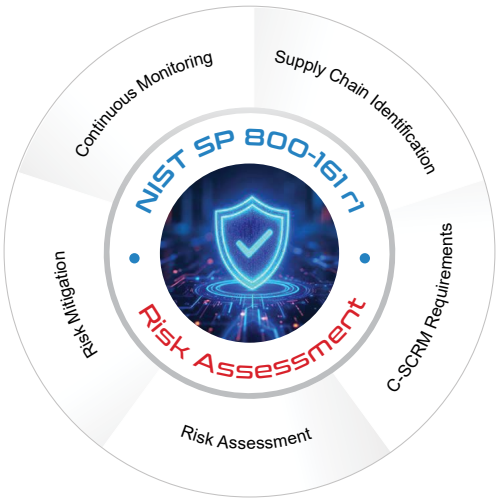
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST SP 800-171r3
Risk Assessment Portal | ABC CORP





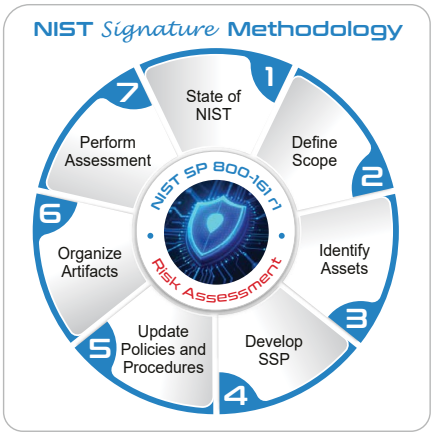




© ecfirst. All Rights Reserved, 2026

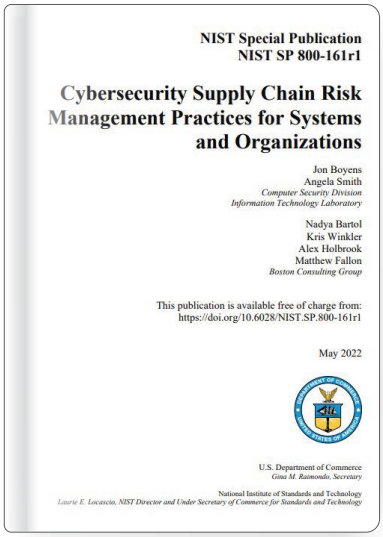
NIST SP 800-161r1
Risk Assessment










NIST Special Publication
NIST SP 800-161r1

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Jon Boyens
Angela Smith
Computer Security Division
Information Technology Laboratory

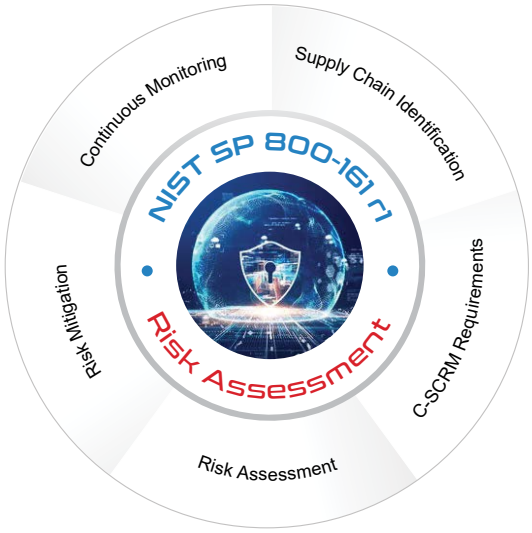
Nadya Bartol
Kris Winkler
Alex Holbrook
Matthew Fallon
Boston Consulting Group

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-161r1

May 2022

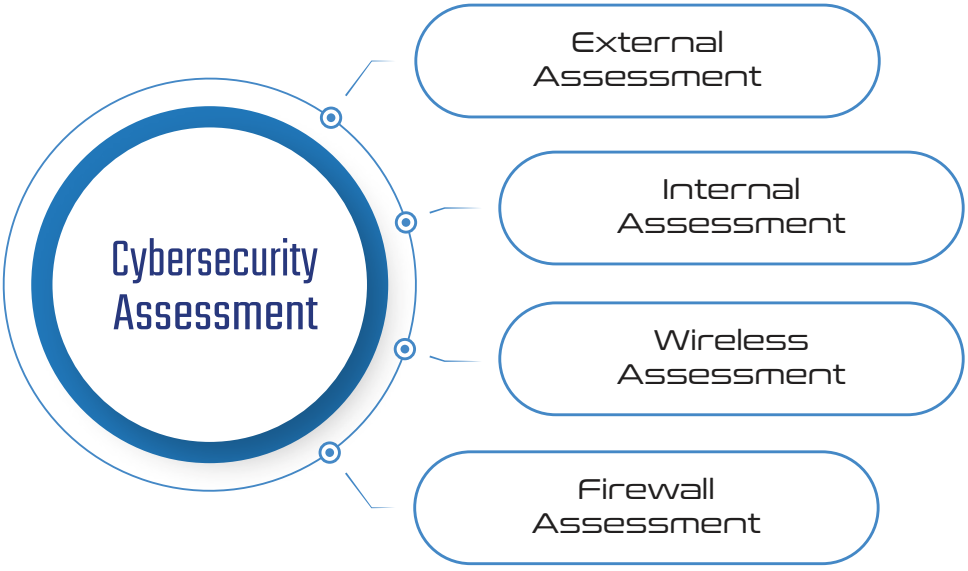
U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology



© ecfirst. All Rights Reserved, 2026

Cybersecurity Assessment



External Assessment

- AI-assisted open-source intelligence gathering
- DNS misconfiguration review
- Publicly leaked credentials search
- Anonymous external vulnerability scanning
- Website security testing (OWASP Top 10)

Wireless Assessment

- Facility walkthrough for rogue wireless networks
- Wireless security settings & Pre-Shared Key strength analysis

Internal Assessment

- Authenticated vulnerability scans of internal systems
- Identity & Access Management (Active Directory review)
- Password policy & strength analysis
- Offline password cracking attempts using a custom wordlist
- SNMP and default credential testing
- Security software enumeration

Firewall Assessment

- OS vulnerability analysis
- Security configuration & rule review

CYBERSECURITY ASSESSMENT SCOPE	TITANIUM	PLATINUM	GOLD	SILVER	BRONZE
External Assessment	✓ Customized	✓	✓	✓	✓
Internal Assessment	✓ Customized	✓	✓	✗	✗
Firewall Assessment	✓ Customized	✓	✓	✓	✗
Wireless Assessment	✓ Customized	✓	✗	✗	✗
Detailed Analysis	✓	✓	✓	✓	✗
Corrective Action Plan (CAP)	✓	✓	✓	✗	✗
Detailed Remediation Steps	✓	✓	✓	✗	✗
Executive Brief	✓	✓	✗	✗	✗

© ecfirst. All Rights Reserved. 2026

CloudFirst Assessment

CloudFirst Assessment



CloudFirst Risk Status



Compliance Status Example



Compliant | Not Compliant | N/A

Area	Compliant	Not-Compliant	N/A
IAM	1	3	1
DefenderCloud	5	0	0
StorageAccounts	1	2	0
Database	0	0	5
Log Monitor	1	3	0
Networking	2	3	0
VM	2	0	0
KeyVault	0	0	4
AppService	0	0	7

CloudFirst Scope

The ecfirst CloudFirst Cybersecurity Assessment is organized into two (2) distinct areas of analysis:

External Assessment
- Up to 32 IP addresses

Internal Assessment
- An Active Directory (AD) domain is tested

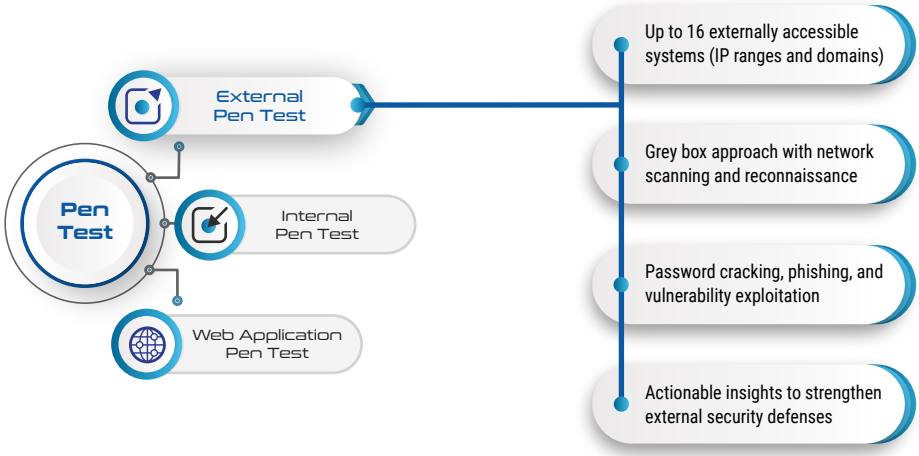
Significant Findings



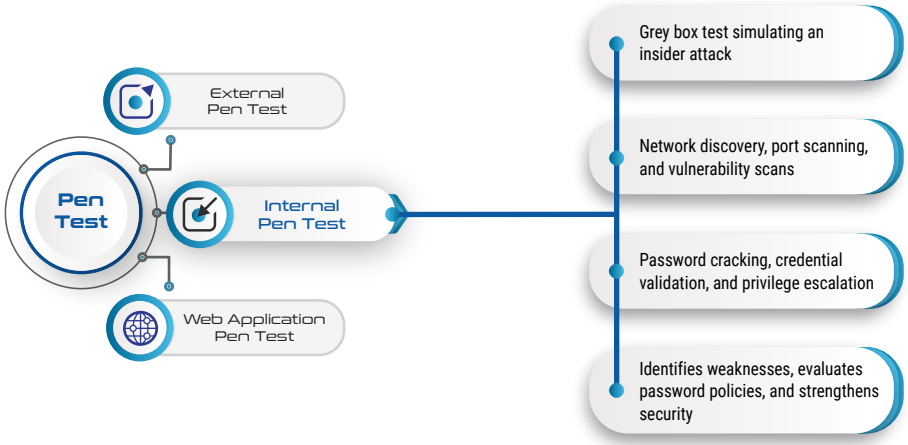
© ecfirst. All Rights Reserved, 2026

Pen Test

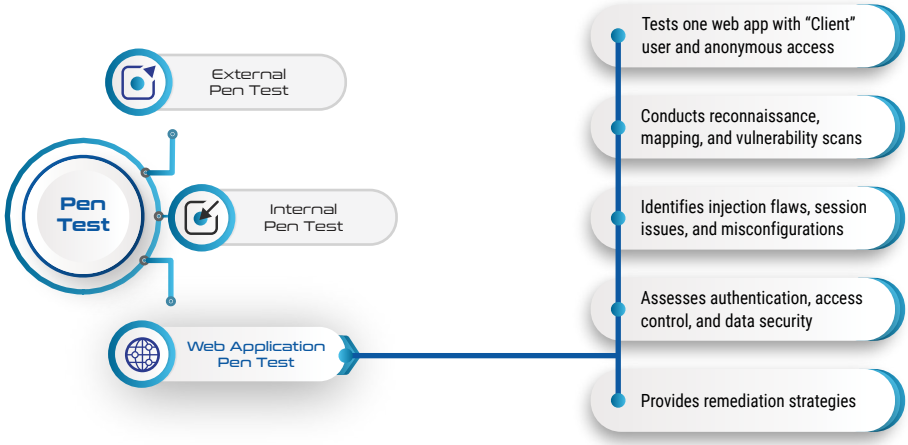
External Pen Test



Internal Pen Test

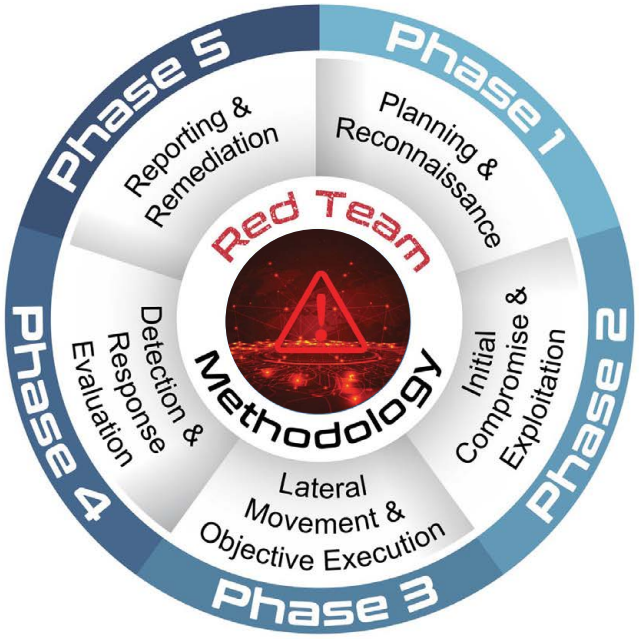


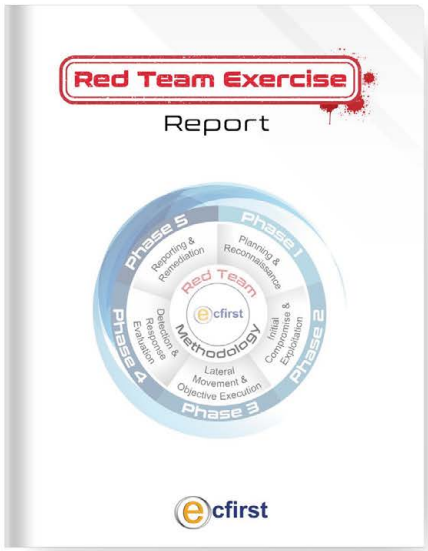
Web Application Pen Test



© ecfirst. All Rights Reserved. 2026

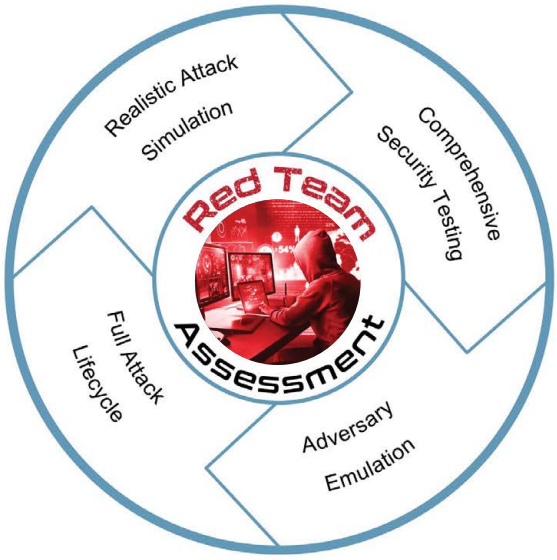
Red Team Exercise

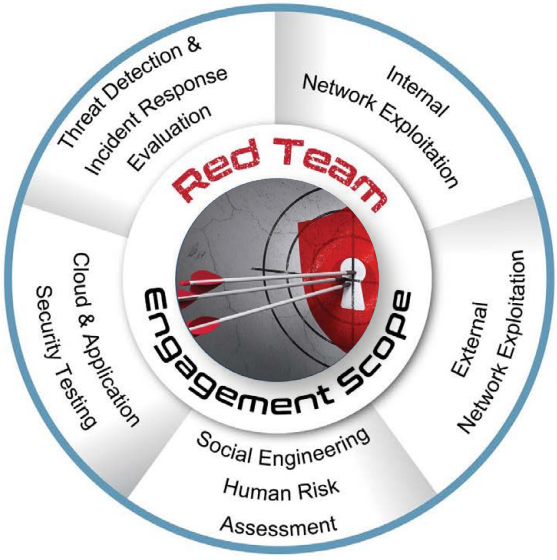




Red Team Exercise

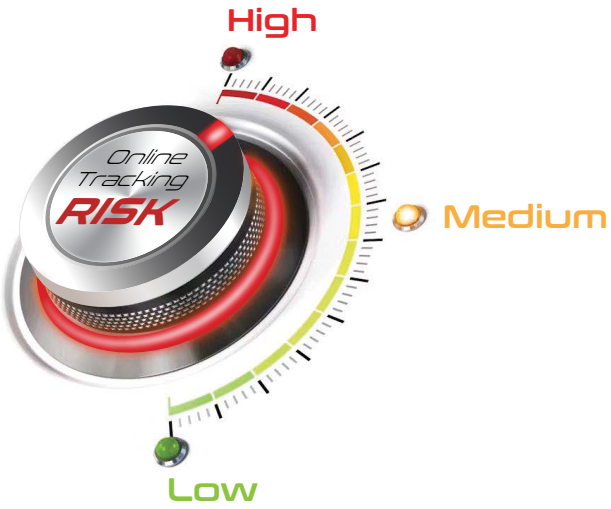
A simulated adversarial exercise that mimics real-world attacks to assess an organization's security capabilities and resilience of its systems and operations.





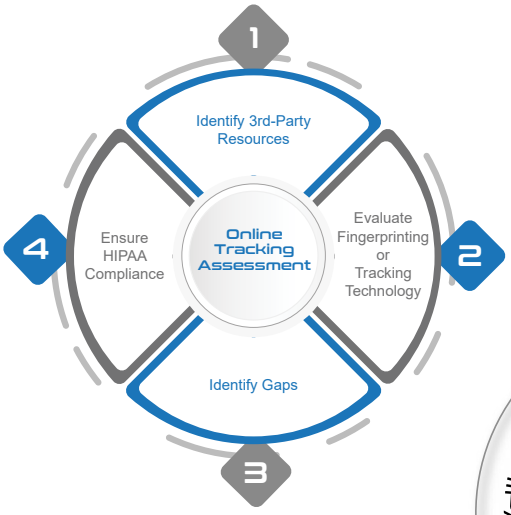
© ecfirst. All Rights Reserved, 2026

Online Tracking Assessment

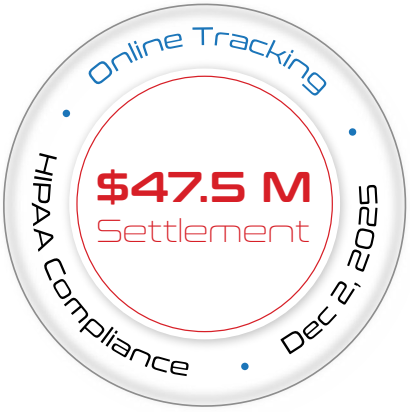


Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates

> "Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."















© ecfirst. All Rights Reserved. 2026

Social Engineering

- Customized phishing campaigns to identify % of phish-prone users
- Targeted end user security awareness training to reduce risk from phish-prone users
- Development of tailored phishing, vishing, pretexting, CEO Fraud cam paigns to understand business risk
- Detailed reports that describe findings from social engineering campaigns
- Access to security awareness emails for compliance with mandates such as HIPAA, CCPA, GDPR

Executive Dashboard

Significant Findings

Industry Benchmark Data

- Phish-prone % **23.9%**

Phishing emails sent to users that did not fall victim in the previous 4 weeks	
Campaign Start Date	Number of Phishing Victims
Dec 6, 2021	11

Phishing emails sent to users that fell victim in the previous 4 weeks	
Campaign Start Date	Number of Phishing Victims
Dec 3, 2021	1
Nov 19, 2021	0

Risk Summary

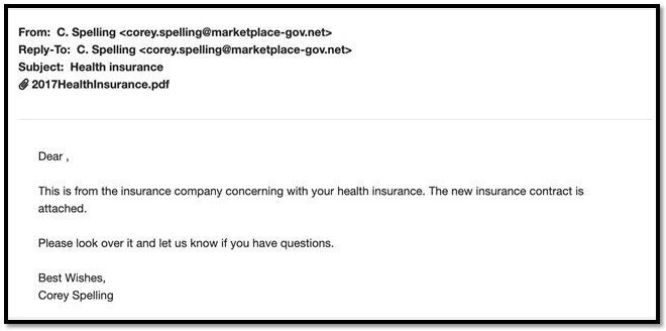
- Based on the number of users that fell victim to the phishing performed, ecfirst estimates the risk of a successful Social Engineering attack against to be a Medium risk.



Findings

ecfirst was successful in the Social Engineering campaign by enticing 15 users to open and interact with phishing emails we sent. Users that interacted with the emails were then presented information informing them they had fallen victim to a phishing test and identified “red flags” in the email they received that could have indicated the email was not legitimate. Had the users interacted with real phishing emails, the attackers could potentially have performed a number of malicious actions, such as collecting sensitive data or delivering malware to the user.

Sample email sent to user:


From: C. Spelling <corey.spelling@marketplace-gov.net>
Reply-To: C. Spelling <corey.spelling@marketplace-gov.net>
Subject: Health insurance
2017HealthInsurance.pdf

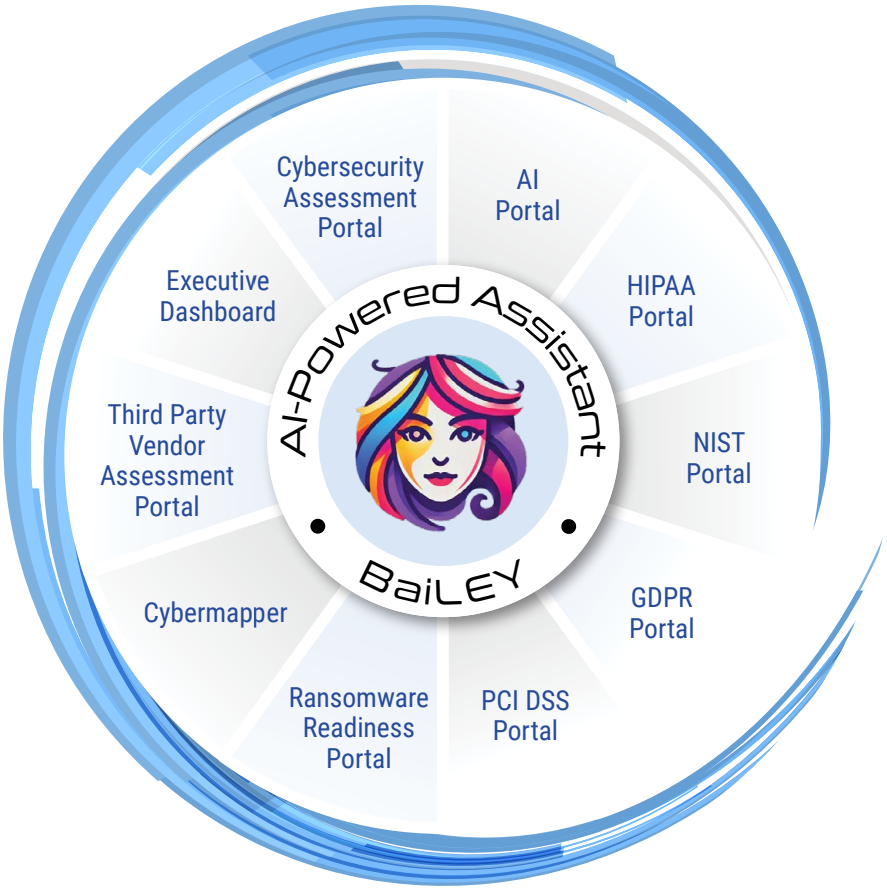
Dear ,

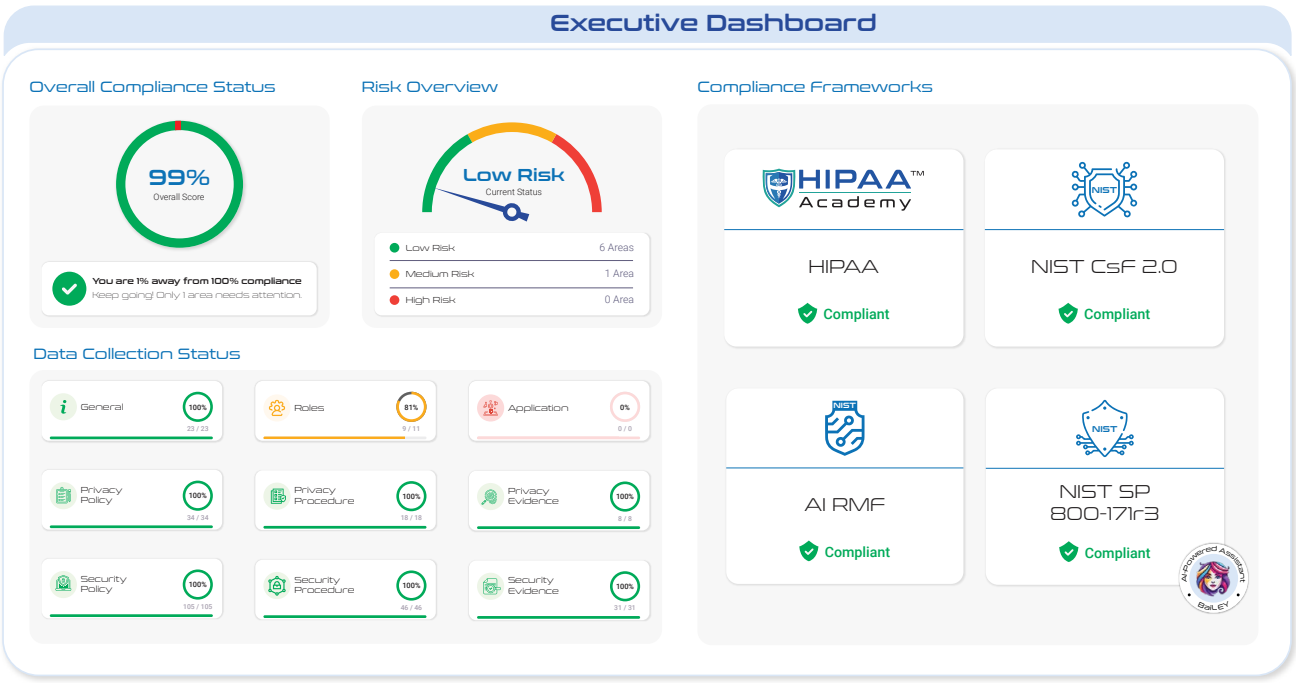
This is from the insurance company concerning with your health insurance. The new insurance contract is attached.

Please look over it and let us know if you have questions.

Best Wishes,
Corey Spelling

© ecfirst. All Rights Reserved, 2026





© ecfirst. All Rights Reserved, 2026

CMMC
Why ecfirst?

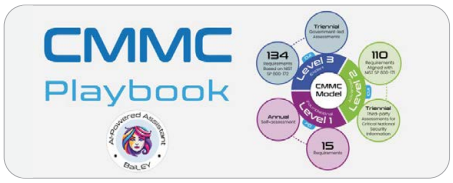
ecfirst

Credentialed Staff

- Master of Science, Electrical Engineering
- CISSP (ISSAP, ISSMP)
- CISA
- CISM
- CCSP
- HITRUST CCSFP

CCA
Lead | Higher Level Certifications

AI Powered CMMC Playbook



Surgically Defined CMMC Assessment Process

CYBER AB
AUTHORIZED C3PAO

CMMC Thought Leadership

CMMC DAY | CMMC CEIC EAST | CMMC CEIC WEST

CCP Reference

"I am happy to let you know I passed the CMMC CCP exam on my first attempt. The CCP prep process was easier than I expected - thanks to the fantastic training class and study materials from the Pabrai CCP Academy! I appreciated my ecfirst experience."

CCP

CCA

CCA Reference

"The Pabrai CCA Program was extensive with excellent assessment resources.

Practical, real-world CMMC assessment scenarios presented, including insight on a credible SSP."

CMMC Readiness Mock Assessment

CYBER AB
REGISTERED PRACTITIONER ORGANIZATION

CAICO APP

DoD CMMC Certification Training Content
Approved and Authorized

CAICO ATP

DoD CMMC Certification Training Provider
Approved and Authorized

© ecfirst. All Rights Reserved. 2026

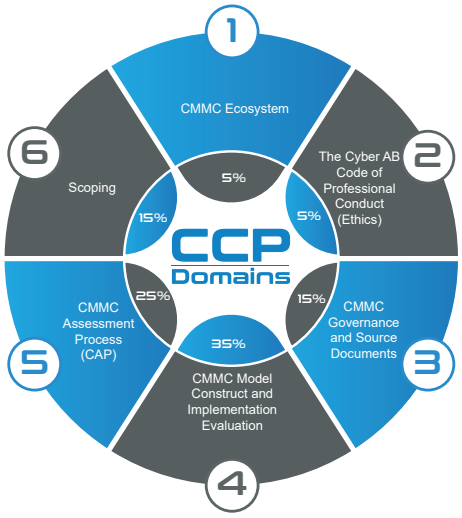
CMMC CCP

Public | Virtual | Onsite

Summary

The CMMC Certified Professional (CCP) credential will verify a candidate's knowledge of the Cybersecurity Maturity Model Certification (CMMC), relevant supporting materials, and applicable legal and regulatory requirements to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The CCP exam will assess the candidate's understanding of the CMMC ecosystem. A passing score on the exam is a prerequisite to CMMC Certified Assessor (CCA) and CMMC Certified Instructor certifications.

CMMC Certified Professional (CCP)



CCP Exam Specifications



This is not an open book exam

Intended Audience

- Employees of Organizations Seeking CMMC Certification (OSC)
  - IT and Cybersecurity Professionals
  - Regulatory Compliance Officers
  - Legal and Contract Compliance Professionals
  - Management Professionals
- Cybersecurity and Technology Consultants
- Federal Employees
- CMMC Assessment Team Members

Domain Exam Weight

#	Domain	Exam Weight	CCP Program	Hours 36
1	CCP Pre Program Prep			Hours 2
2	CMMC Ecosyst`em Blueprint Domain 1	5%	Domain 1, 2 & 3 Tuesday, Day 1 8:30 am - 4:30 pm Offline Prep: 2 Hours	Hours 10
3	The Cyber AB Code of Professional Conduct (Ethics) Blueprint Domain 2	5%		
4	CMMC Governance and Source Documents Blueprint Domain 3	15%		
5	CMMC Model Construct and Implementation Evaluation Blueprint Domain 4	35%	Domain 4 Wednesday, Day 2 8:30 am - 4:30 pm Offline Prep: 2 Hours	Hours 10
6	CMMC Assessment Process (CAP) Blueprint Domain 5	25%	Domain 5 Thursday, Day 3 8:30 am - 4:30 pm Offline Prep: 2 Hours	Hours 10
7	Scoping Blueprint Domain 6	15%	Domain 6 & Review Friday, Day 4 8:30 am - 12:30 pm	Hours 4
8	Practice Exam & Review			

Client Reference

> "I am happy to let you know **I passed** the CMMC **CCP exam** on my **first attempt.** The CCP prep process was **easier** than I expected - thanks to the **fantastic training class** and **study materials** from the **ecfirst CCP Academy!** I appreciated **my Pabrai** experience."

© ecfirst. All Rights Reserved, 2026

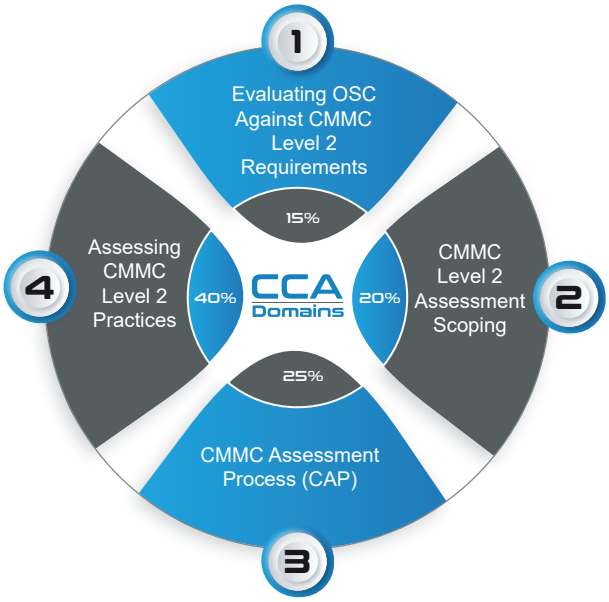
CMMC CCA

Public | Virtual | Onsite

Summary

The CMMC Certified Assessor (CCA) exam will verify a candidate's readiness to perform as an effective Certified Assessor of Organizations Seeking Certification (OSC) at CMMC Level 2. A passing score on the CCA exam is a prerequisite to a CMMC Lead Assessor designation.

CMMC Certified Assessor (CCA)



CCA Exam Specifications



This is not an open book exam

Domain Exam Weight

#	Domain	Exam Weight	CCA Program	Hours 36
1	CCA Pre Program Prep			Hours 2
2	Welcome Introductions, About the Portal and Pre-Quiz Introduction Evaluating OSC Against CMMC Level 2 Requirements Blueprint Domain 1	15%	**Domain 0, 1, 2** Tuesday, Day 1 8:30 am - 4:30 pm Group Exercises: 8 | 40 Minutes Offline Prep: 2 Hours	Hours 10
3	CMMC Level 2 Assessment Scoping Blueprint Domain 2	20%		
4	CMMC Assessment Process (CAP) Blueprint Domain 3	25%	**Domain 3** Wednesday, Day 2 8:30 am - 4:30 pm Group Exercises: 7 | 35 Minutes Offline Prep: 2 Hours	Hours 10
5	Assessing CMMC Level 2 Practices Blueprint Domain 4	40%	**Domain 4** Thursday, Day 3 8:30 am - 4:30 pm Group Exercises: 10 | 60 Minutes Offline Prep: 2 Hours	Hours 10
6	Practice Exam & Review		**Review and Final Quiz** Friday, Day 4 8:30 am - 12:30 pm	Hours 4

Intended Audience

- CMMC Certified Professional (CCP) seeking to advance to CCA
- CMMC Certified Instructors who wish to teach the CCA course

Client Reference

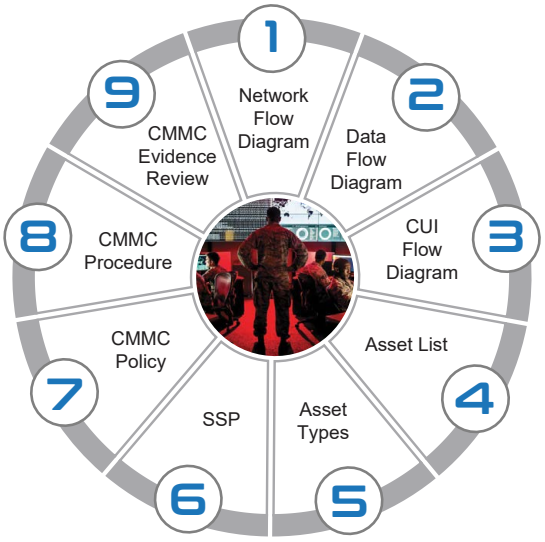
> The **Pabrai CCA Program** was extensive with excellent assessment resources.
>
> **Practical, real-world CMMC assessment** Scenarios presented, including insight on a credible SSP.

© ecfirst. All Rights Reserved. 2026

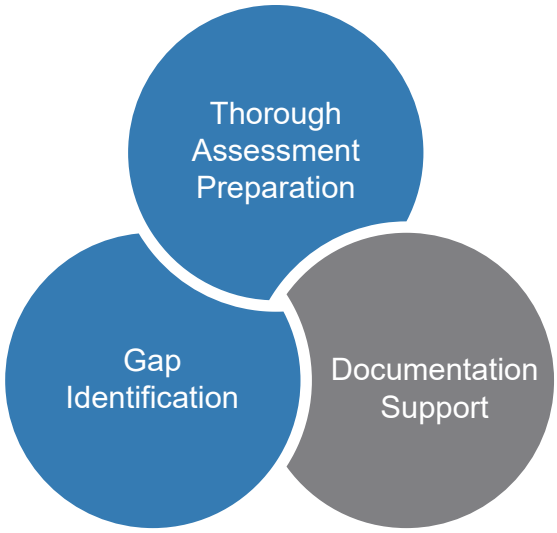
CMMC Advisory Services

Guidance | Documentation | Gap Analysis

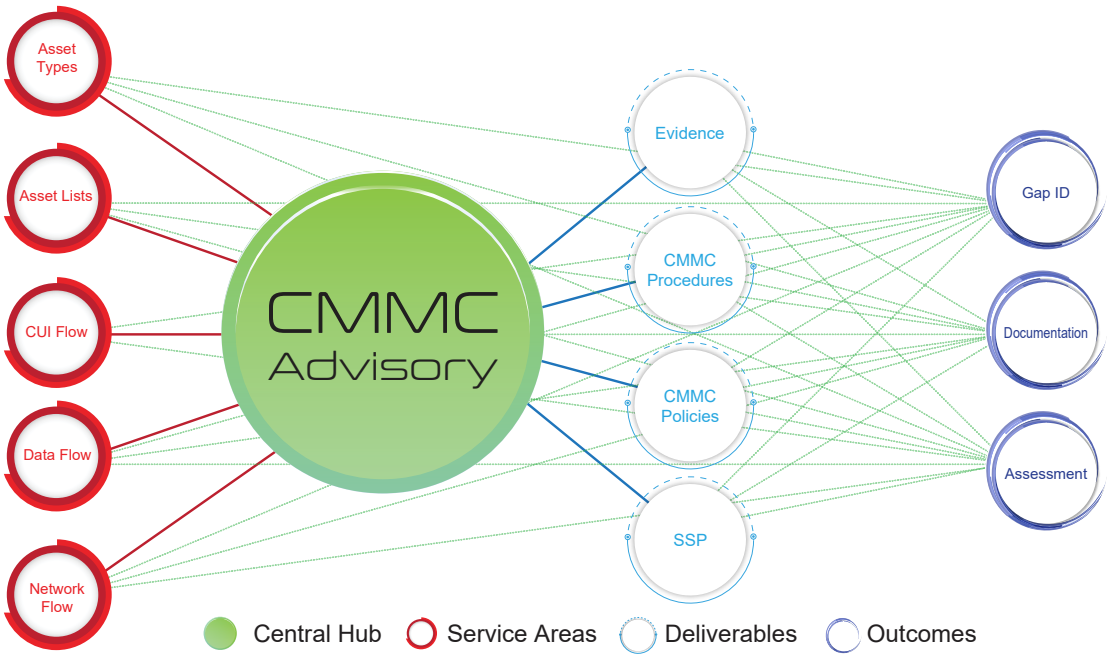
Advisory Guidance



Compliance Support



CMMC Advisory Services Flow



© ecfirst. All Rights Reserved, 2026

Purpose

Confirm CMMC Level 2 controls remain effective and that no compliance degradation has occurred between formal assessments.

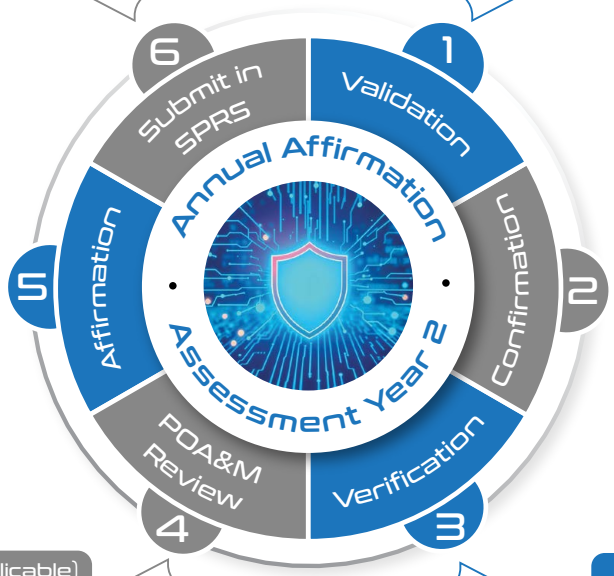
This is a formal assertion — not a re-assessment.

Submit Annual Affirmation in SPRS

- Enter/update:
  - Compliance status
  - Affirmation statement
- Ensure:
  - Linked to correct CMMC UID/system
  - **Submitted at least once every 12 months**

Validate Continuous Compliance

- Confirm the organization still meets all CMMC Level 2 (110 controls aligned with NIST SP 800-171)
- No regression in implemented controls
- All in-scope systems remain compliant



Executive Review & Affirmation

- Affirming Official must:
  - Review full compliance posture
  - Attest accuracy of the affirmation

Creates legal accountability

False declaration carries liability

Confirm No Significant Changes

- No major architectural changes
- No boundary/scope changes
- No degradation in security posture

Material changes may require a new assessment

Review POA&M Status (if Applicable)

- All POA&M items are closed
- No open critical/high-risk gaps

Conditional Level 2 must reach Final status

Verify Control Effectiveness

- Controls must be:
  - Implemented
  - Operating effectively
  - Continuously maintained
- Review supporting evidence:
  - Monitoring / SIEM logs
  - Access control enforcement
  - Incident response records
  - Training records

© ecfirst. All Rights Reserved. 2026

Purpose

Confirm CMMC Level 2 controls remain effective and that no compliance degradation has occurred between formal assessments.

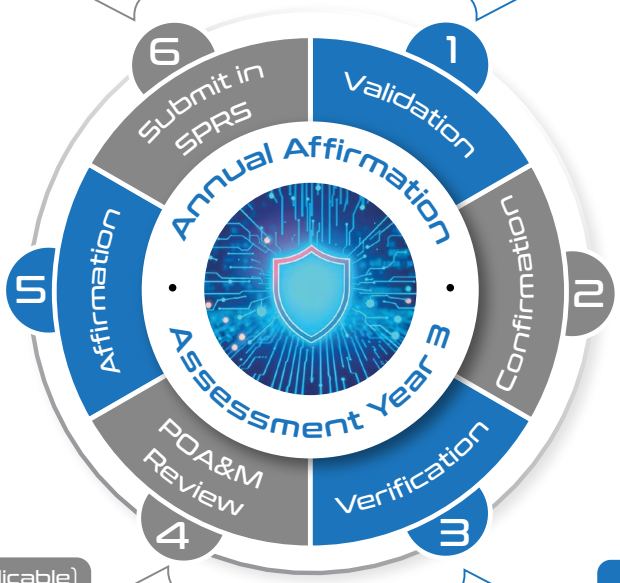
This is a formal assertion — not a re-assessment.

Submit Annual Affirmation in SPRS

- Enter/update:
  - Compliance status
  - Affirmation statement
- Ensure:
  - Linked to correct CMMC UID/system
  - **Submitted at least once every 12 months**

Validate Continuous Compliance

- Confirm the organization still meets all CMMC Level 2 (110 controls aligned with NIST SP 800-171)
- No regression in implemented controls
- All in-scope systems remain compliant



Executive Review & Affirmation

- Affirming Official must:
  - Review full compliance posture
  - Attest accuracy of the affirmation

Creates legal accountability

False declaration carries liability

Confirm No Significant Changes

- No major architectural changes
- No boundary/scope changes
- No degradation in security posture

Material changes may require a new assessment

Review POA&M Status (if Applicable)

- All POA&M items are closed
- No open critical/high-risk gaps

Conditional Level 2 must reach Final status

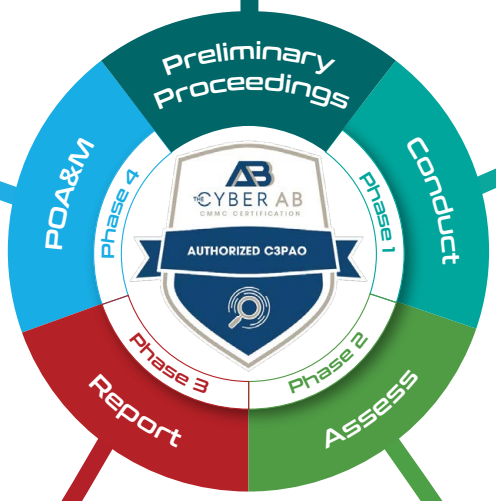
Verify Control Effectiveness

- Controls must be:
  - Implemented
  - Operating effectively
  - Continuously maintained
- Review supporting evidence:
  - Monitoring / SIEM logs
  - Access control enforcement
  - Incident response records
  - Training records

© ecfirst. All Rights Reserved. 2026

Preliminary

- Receive CMMC Assessment Request from OSC
- Confirm the Entity/Entities to be Assessed
- Frame the Assessment
- Identify and Manage Initial COI
- Execute Contractual Agreement



Phase 1

- Review the SSP
- Validate CMMC Assessment Scope
- Confirm Availability of Evidence
- Determine Readiness for Assessment
- Compose the Assessment Team
- Complete the Pre-Assessment Form
- Conduct Quality Assurance Review of Pre-Assessment and Planning Information
- Upload Pre-Assessment Form into CMMC eMASS
- Adverse Determination of Assessment Readiness

Phase 2

- Conduct In-Brief Meeting
- Assess Implementation of Security Requirements
- Apply Sampling Values for Depth and Coverage
- Conduct Assessment Scoring
- Address External Service Providers
- Address Cloud Service Providers
- Conduct Quality Assurance Reviews
- Convene Daily Checkpoint Meetings

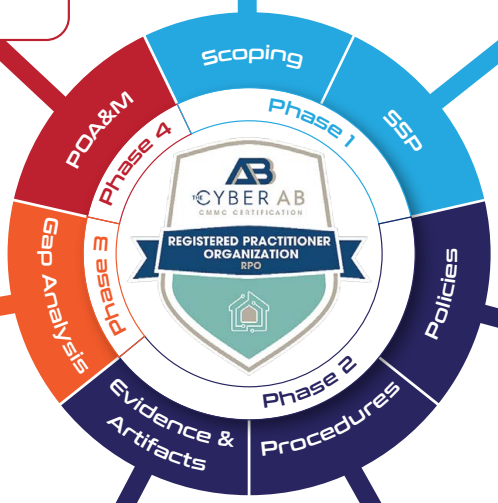
Phase 3

- Compile and Compose Assessment Results
- Conduct Quality Assurance Review
- Convene Out-Brief Meeting
- Upload Certification Assessment Results into CMMC eMASS
- Administer Assessment Appeals (if required)

Phase 4

- Generate Certificate of Status
- Issue Certificate of CMMC Status
- Close-Out POA&M

© ecfirst. All Rights Reserved, 2026



Phase 1

- Define assessment objectives, scope, and final boundaries
- Identify in-scope assets, systems, and data
- Confirm regulatory and contractual requirements

Phase 1

- Document system boundaries, security controls, and practices
- Align SSP with CMMC Level 2 requirements
- Conduct internal validation of SSP completeness

Phase 2

- Assess existing policies against CMMC L2 controls
- Identify gaps and implement necessary updates
- Train key personnel on policy implementation

Phase 2

- Assess existing procedures against CMMC L2 controls
- Identify gaps and implement necessary updates

Phase 2

- Develop/review data flow, CUI flow, Network, Boundary Diagrams
- Assist in putting together Customer Responsibility Matrix (CRM)
- Gather proof of security control implementation
- Ensure documentation of security practices and processes
- Validate operational effectiveness of controls

Phase 3

Conduct a comprehensive gap analysis against CMMC L2 requirements

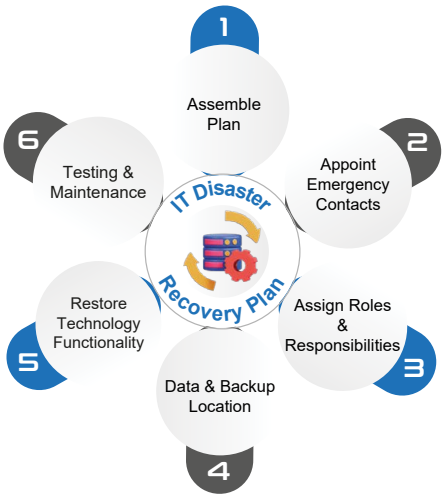
Phase 4

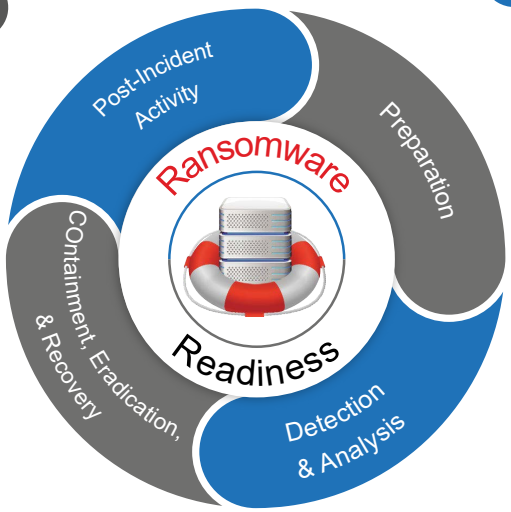
- Develop POA&Ms for identified deficiencies
- Provide remediation guidance to achieve full readiness

© ecfirst. All Rights Reserved, 2026



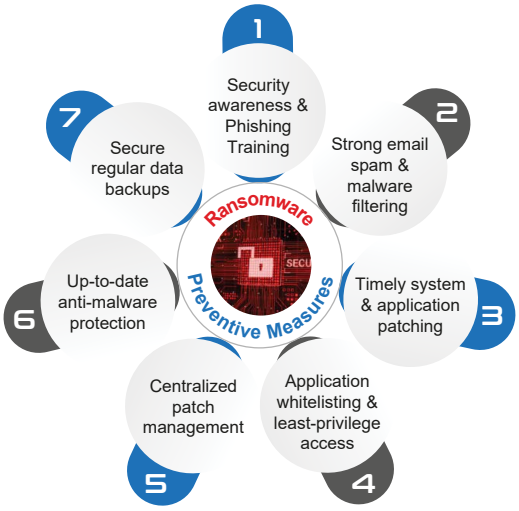




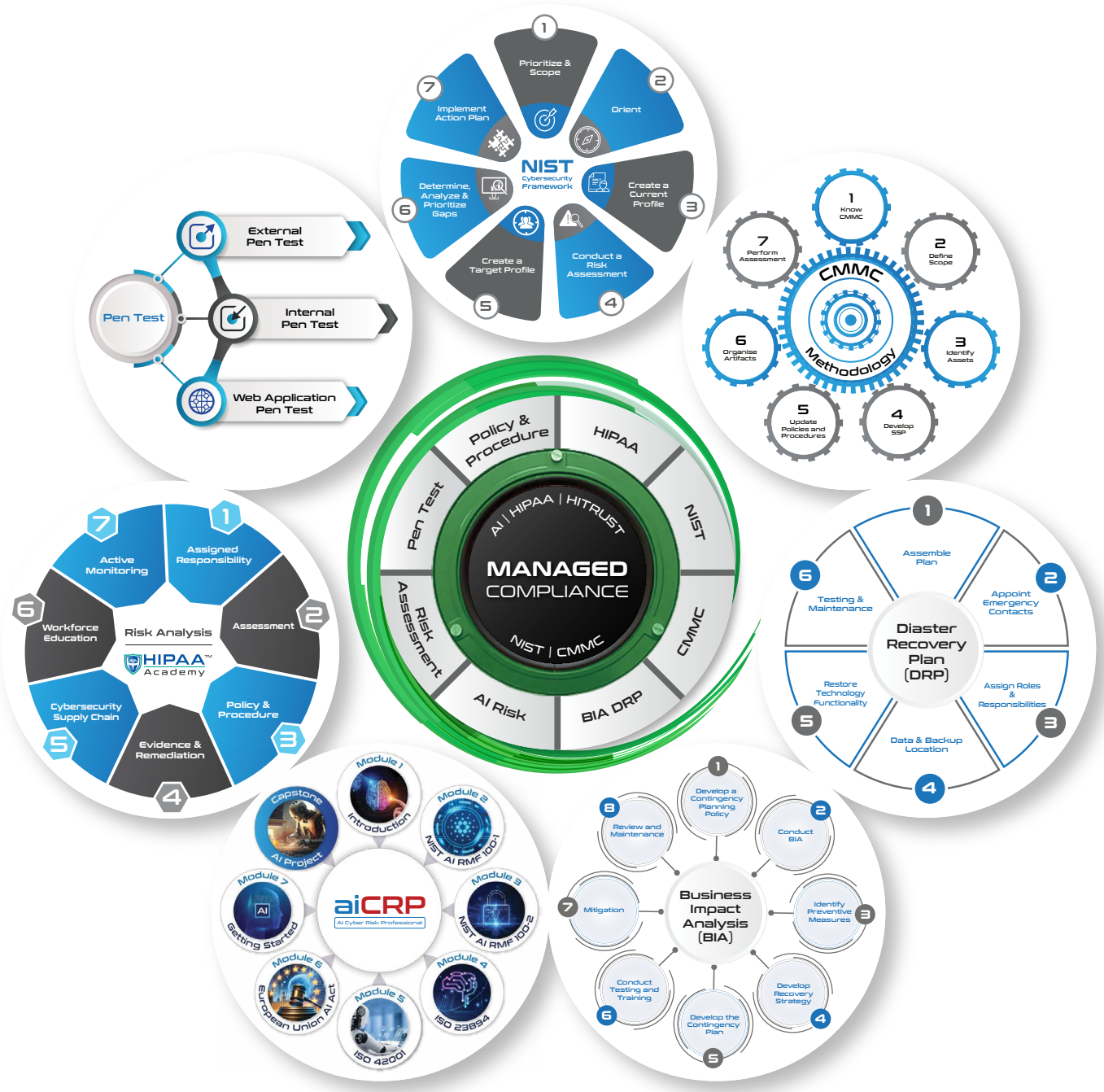








© ecfirst. All Rights Reserved, 2026



© ecfirst. All Rights Reserved, 2026

On Demand (OD)

Fixed-rate | **Expert Advisors** | **No Long-term Commitment**



AI Cyber Program



Policies and Procedures



© ecfirst. All Rights Reserved, 2026

VISO & InfoSec
Staffing Program









© ecfirst. All Rights Reserved. 2026

PCI DSS
Pre-Assessment

ecfirst

PCI DSS Readiness Assessment

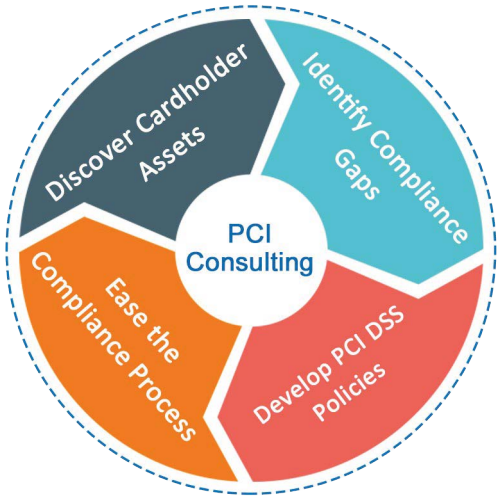
- Review of compliance against PCI DSS v4.0 requirements
- Identify gaps & risks in protecting cardholder data
- Deliver actionable assessment report with findings
- Provide prioritized remediation plan & timeline
- Executive summary for leadership & stakeholders



PCI Dss Goals

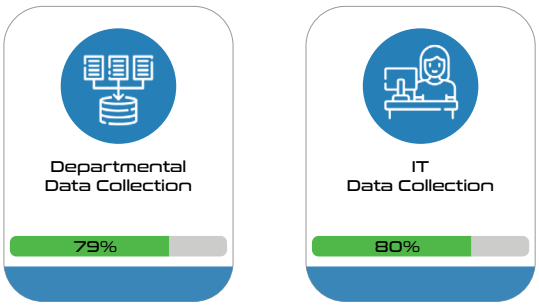


PCI Consulting



PCI DSS Portal

TRACER℠ ASSET RISK MANAGEMENT | ABC CORP





© ecfirst. All Rights Reserved, 2026

GDPR Compliance
Pre-Assessment

ecfirst

GAP Assessment

- Comprehensive and thorough GDPR Assessment to identify compliance gaps
- Review and optional update of GDPR policies and procedures
- Corrective Action Plan to guide remediation and establish priority

GDPR Services





GDPR: Who, What, Why?

- Applies to data controllers and processors if the data subject resides in the EU
- Individuals under the DPA are likely also subject to GDPR
- Processors must maintain records of personal data and processing activities
- "Personal data" covers information about an individual's private, professional, or public life

GDPR *Signature* Methodology



Purpose & Scope



Establish a Credible GDPR Program

7 GDPR Vendor Readiness

Conduct GDPR awareness training for execs & workforce 1

6 Update cyber incident response based on GDPR data breach specification



Assign responsibility for a Data Protection Officer (DPO) 2

5 Create procedures to align with GDPR requirements

GDPR Assessment 3

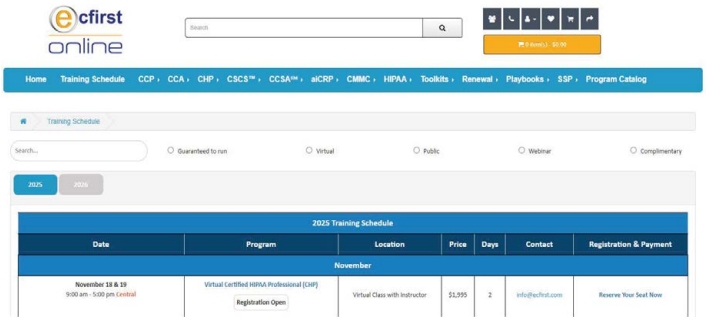
4 Develop policies, consent and other documents to address GDPR mandates

© ecfirst. All Rights Reserved, 2026

Online Store



www.ecfirst.biz



Training



Playbooks



Templates

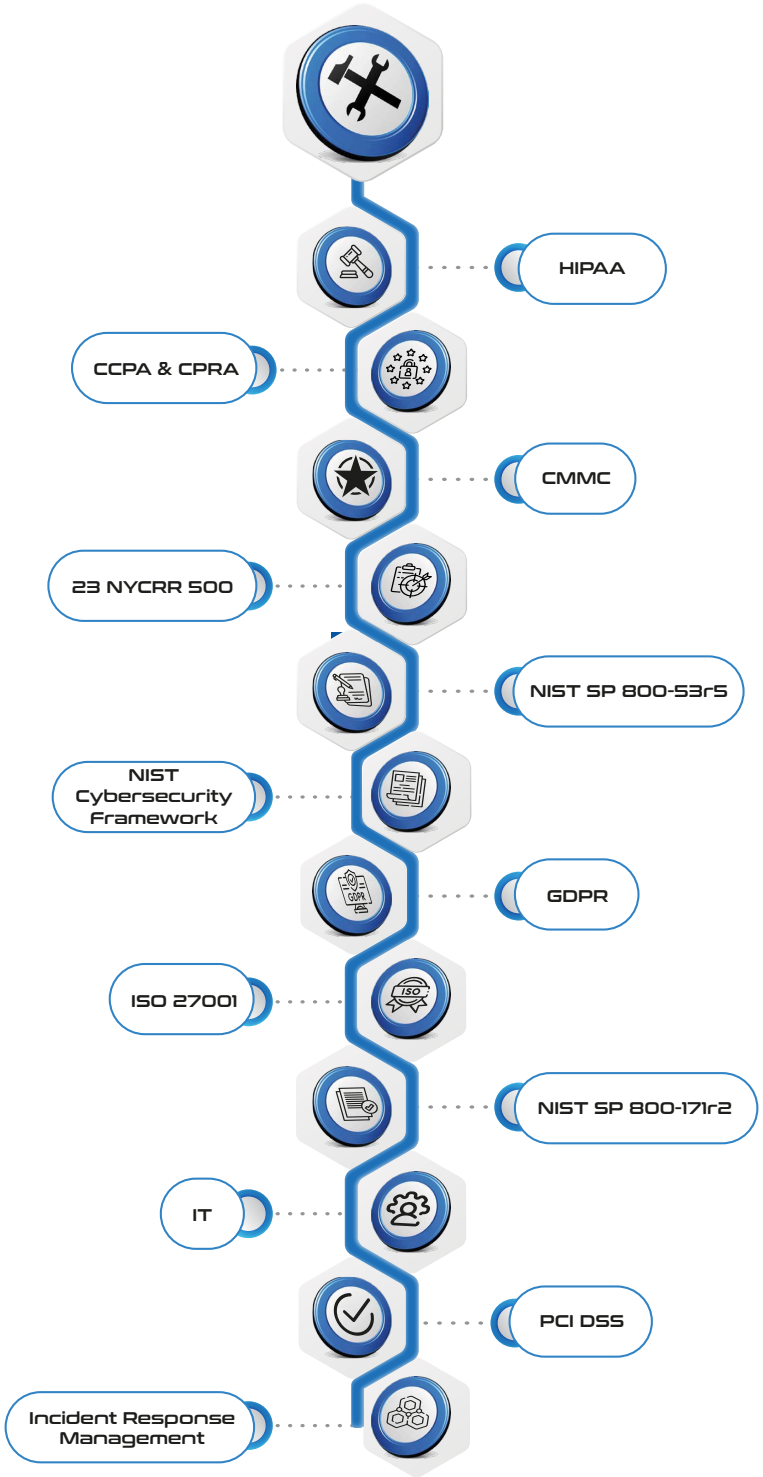
CMMC | HIPAA | GDPR | NIST | SSP

© ecfirst. All Rights Reserved, 2026

Compliance
and Cyber Toolkit

ecfirst

Toolkit Packages



Components



© ecfirst. All Rights Reserved, 2026

CMMC
Level 1 Toolkit





© ecfirst. All Rights Reserved, 2026

CMMC
Level 2 Toolkit





© ecfirst. All Rights Reserved, 2026

CMMC
Level 3 Toolkit





© ecfirst. All Rights Reserved, 2026

CMMC
Level 1 Portal

Home

CMMC 2.0 Level 1 Self-Assessment — Back

- Phase 1 — Planning
- Phase 2 — Questionnaire
- Phase 3 — Verification
- Phase 4 — Generate Report
- Dashboard
- CMMC Level 1 Playbook



Phase 1 Planning

Home / Assessment / CMMC 2.0 Level 1 / Phase 1: Planning — Back

- Intake Form — 100%
- Client Information — 87.1%
- Roles — 93.8%
- SSP Scope Document
- General Questionnarie — 25%

© ecfirst. All Rights Reserved, 2026

Phase 2 Questionnaire

CMMC 2.0 Level 1 / Phase 2 Questionnaire Back

Show 10 entries

Please click on the Action button to describe how each requirement is implemented!

Requirement ID	Requirement Description	Action
Access Control, Domain 1		
AC.L1-b.1.i	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	
AC.L1-b.1.ii	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	

Showing 1 to 2 of 21 entries

Previous 1 2 3 Next

Submit your Questionnaire

Phase 3 Verification

DTB CORP

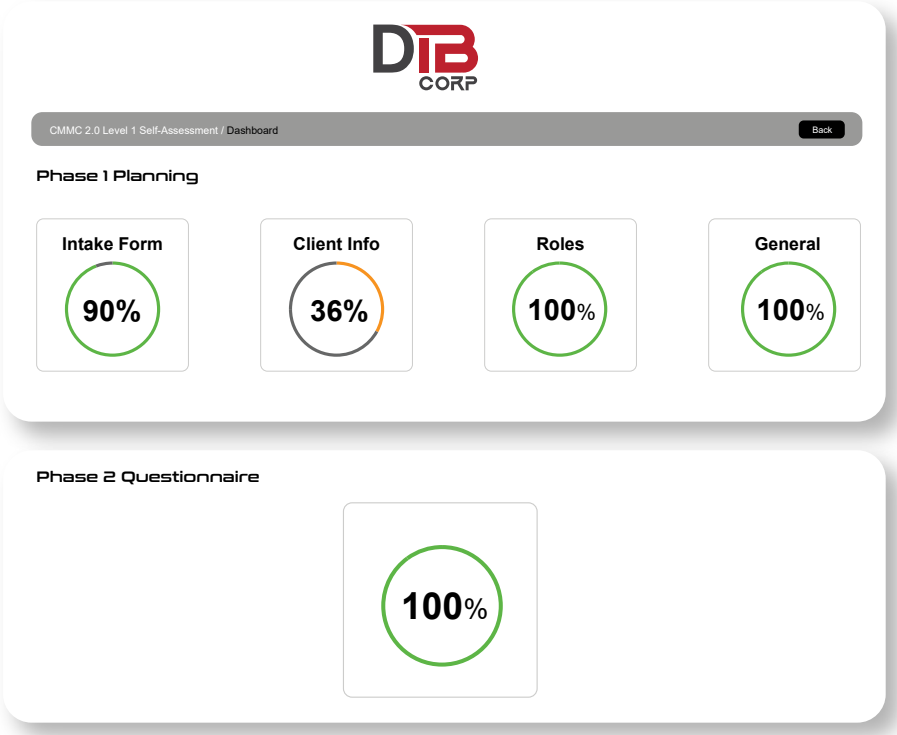
Home / Assessment / CMMC 2.0 Level 1 / Phase 3: Verification Back

Phase 3 Verification Phase 1

Phase 3 Verification Phase 2

© ecfirst. All Rights Reserved, 2026

Dashboard



Evidence

In this sample, an artifacts is provided to address CMMC requirements

Display Name	Account Enabled	Operating System	Operating System Version	Make/OEM	Join Type (trust Type)	MDM Display Name	is Compliant	Registration Time	Approximate Last SignIn Date/Time	Device ID	is Managed
Surface	TRUE	Windows	10.0.22000.194	Microsoft	Azure AD registered			08-10-2021 11:44	28-01-2022 13:37	59494c70-581e-4136-8e50-5fbd95175a5a	
iPhone	TRUE	iOS	14.4.2	Apple	Azure AD registered			04-05-2021 06:30	17-11-2021 04:51	4dfa4e6f-3126-42ae-8ca5-0292e98bb5f1	
Lenovo	TRUE	Windows	10.0.19043.1526	Lenovo	Azure AD joined			08-12-2020 22:30	26-02-2022 11:58	3e80794c-1d9f-4b75-beee-eb35225cb29d	
DESKTOP-0G62TC8	TRUE	Windows	10.0.19043.1526	Dell	Azure AD joined	Microsoft Intune	TRUE	27-07-2021 15:17	28-02-2022 16:49	13f00ad1-78ad-4844-b392-bf761bf3e405	TRUE
expiscor	TRUE	MacMDM	12.1 (21C52)	Apple	Azure AD registered	Microsoft Intune	FALSE	24-01-2022 12:58	24-01-2022 12:58	e612c780-5f58-4b9f-a80e-e08c204c3cdf	FALSE
system_01	TRUE	Windows	10.0.19043.1526	Dell	Azure AD registered			16-02-2022 19:40	16-02-2022 19:40	4be318f9-958f-4d6c-af95-a062149a760f	
SYSTEM_07	TRUE	Windows	10.0.19043.1466	Dell	Azure AD registered			06-02-2022 19:34	06-02-2022 19:34	425d30d1-62a1-4ad0-9678-3c7bf5be7078	
iPhone	TRUE	iOS	14.6	Apple	Azure AD registered			27-07-2021 07:58	18-02-2022 06:48	66f9e550-ca71-43bc-bc71-de8cd37fc47a	
DESKTOP-GGE14F2	TRUE	Windows	10.0.19043.1526	Dell	Azure AD joined	Microsoft Intune	TRUE	02-06-2021 09:55	23-02-2022 12:32	a69e58d-f8d3-4345-904f-cc146e328fdd	TRUE
VA-WL03	TRUE	Windows	10.0.19042.1566	Dell	Azure AD registered			04-03-2022 08:39	04-03-2022 08:39	ba79ddbf-9cc1-45d5-bce5-0fc43216d2eb	
SYSTEM18	TRUE	Windows	10.0.19043.985	Dell	Azure AD registered			04-06-2021 00:00	04-06-2021 00:00	cf4c5d7b-63ef-4104-9681-3c1a840b184c	
DESKTOP-CVN12JL	TRUE	Windows	10.0.19042.1415	Dell	Azure AD joined	Microsoft Intune	FALSE	19-07-2021 09:15	22-12-2021 16:24	ea2cd150-4cb3-401a-bf79-c69563818498	TRUE
System26	TRUE	Windows	10.0.19043.1526	Dell	Azure AD registered			16-02-2022 01:22	16-02-2022 01:22	37dfaf4b-7707-49f1-8307-58a85ef5d8b7	
SYSTEM08	TRUE	Windows	10.0.19044.1526	Dell	Azure AD registered			16-02-2022 20:07	16-02-2022 20:07	9fe557b5-091a-42e6-9c20-fa38263cb538	
DESKTOP-8JRU48Q	TRUE	Windows	10.0.19042.1237	Dell	Azure AD registered			05-10-2021 09:57	26-02-2022 11:35	b64c5ba9-5c4d-4a02-9167-f332d8ef624a	
expiscor	TRUE	MacMDM	12.2.1 (21D62)	Apple	Azure AD registered	Microsoft Intune	TRUE	24-01-2022 13:38	26-02-2022 15:18	82c0b66f-7d31-4af9-9877-2c95eeb39fa6	TRUE
Abdt.us	TRUE	MacMDM	12.2.1 (21D62)	Apple	Azure AD registered	Microsoft Intune	TRUE	17-05-2021 13:10	27-02-2022 02:50	f22a11ae-9acf-4f42-831a-819864c89af2	TRUE
System09	TRUE	Windows	10.0.19041.867	Dell	Azure AD registered			12-04-2021 21:33	05-07-2021 20:48	6fc7faa5-9399-49a1-be93-23676dd24ba1	
DESKTOP-FHV9EAE	TRUE	Windows	10.0.19043.1526	Dell	Azure AD joined	Microsoft Intune	TRUE	30-10-2020 10:45	26-02-2022 14:31	ed63d622-c183-4054-aaf0-f398f98b644a	TRUE
iPhone	TRUE	iOS	15.1.1	Apple	Azure AD registered			11-01-2022 15:29	03-03-2022 15:21	86d39fd2-5a05-46e1-88a8-aebdf533d365	
DESKTOP-GJDL0OV	TRUE	Windows	10.0.19042.1110	Dell	Azure AD joined	Microsoft Intune	TRUE	21-02-2020 13:50	27-07-2021 06:31	719ccc65-7aff-4e29-9d45-2e506e152a9d	FALSE
samsungSM-G973U	TRUE	Android	11	Samsung	Azure AD registered			21-04-2021 16:28	21-11-2021 16:59	aa5d082a-239d-4e58-af2f-10f4cd8c142b	
OPPOCPH2213	TRUE	Android	11	LG	Azure AD registered			28-05-2021 09:52	28-07-2021 10:25	ff9dba3a-53da-4e48-9e63-e057964ed5d4	
DESKTOP-3765D5K	TRUE	Windows	10.0.18363.0	Dell	Azure AD registered			25-05-2021 15:59	03-11-2021 04:34	be9978be-a083-42bd-9027-5794095bd589	
SYSTEM10	TRUE	Windows	10.0.19041.867	Dell	Azure AD registered			15-04-2021 05:20	23-09-2021 20:32	627401fd-c9e7-4628-872e-2371359f3b5a	
System09	TRUE	Windows	10.0.19043.1237	Dell	Azure AD registered			01-08-2021 20:40	06-03-2022 23:23	001ed6ae-3c9d-421b-beb5-126453ff7087	

SAMPLE

© ecfirst. All Rights Reserved, 2026

CMMC
Level 2 Portal

Home

Home / Assessment / CMMC 2.0 Level 2 Engagement Back

Phase 1 Planning
Phase 2 Assessor Review of Phase 1
Phase 3 Assessment
Phase 4 Report
Phase 5 POA&M

Client Phase
ecfirst | Assessor Phase

CMMC Reference
Readiness Portal
Policy Template



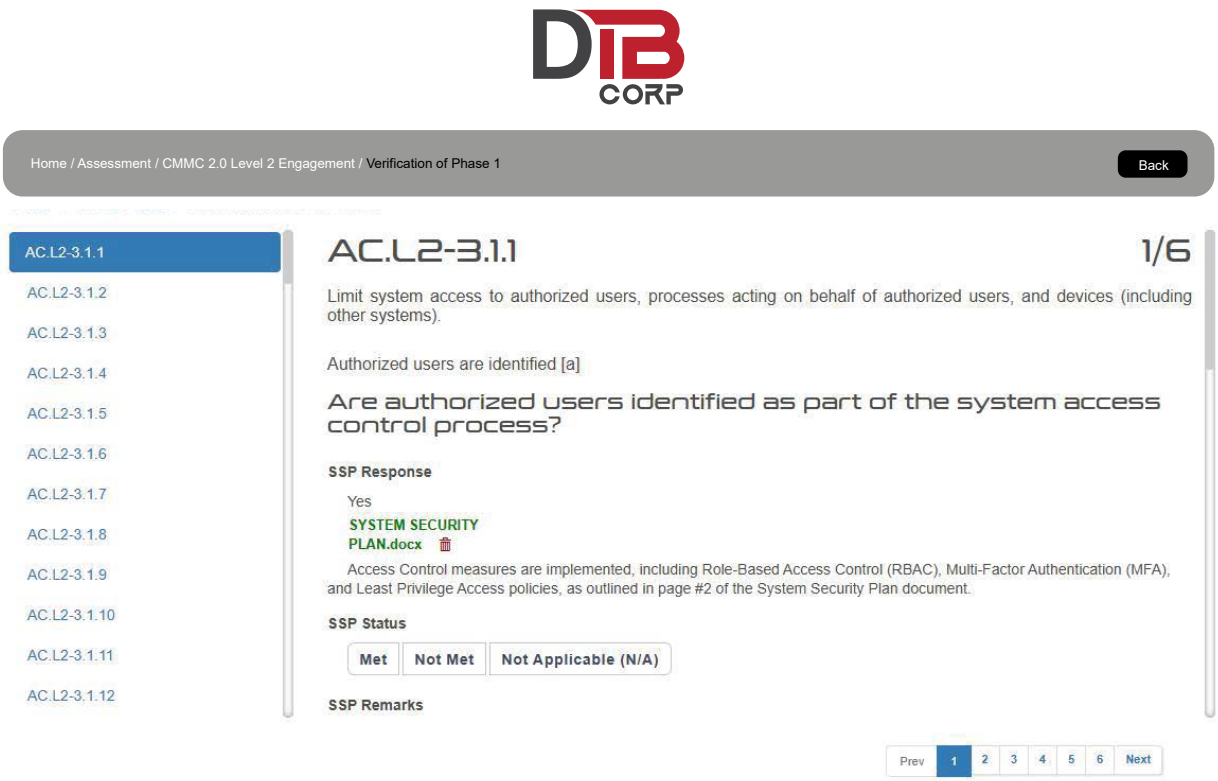
Phase 1 Planning

Home / Assessment / CMMC 2.0 Level 2 Engagement / Phase 1: Planning Back

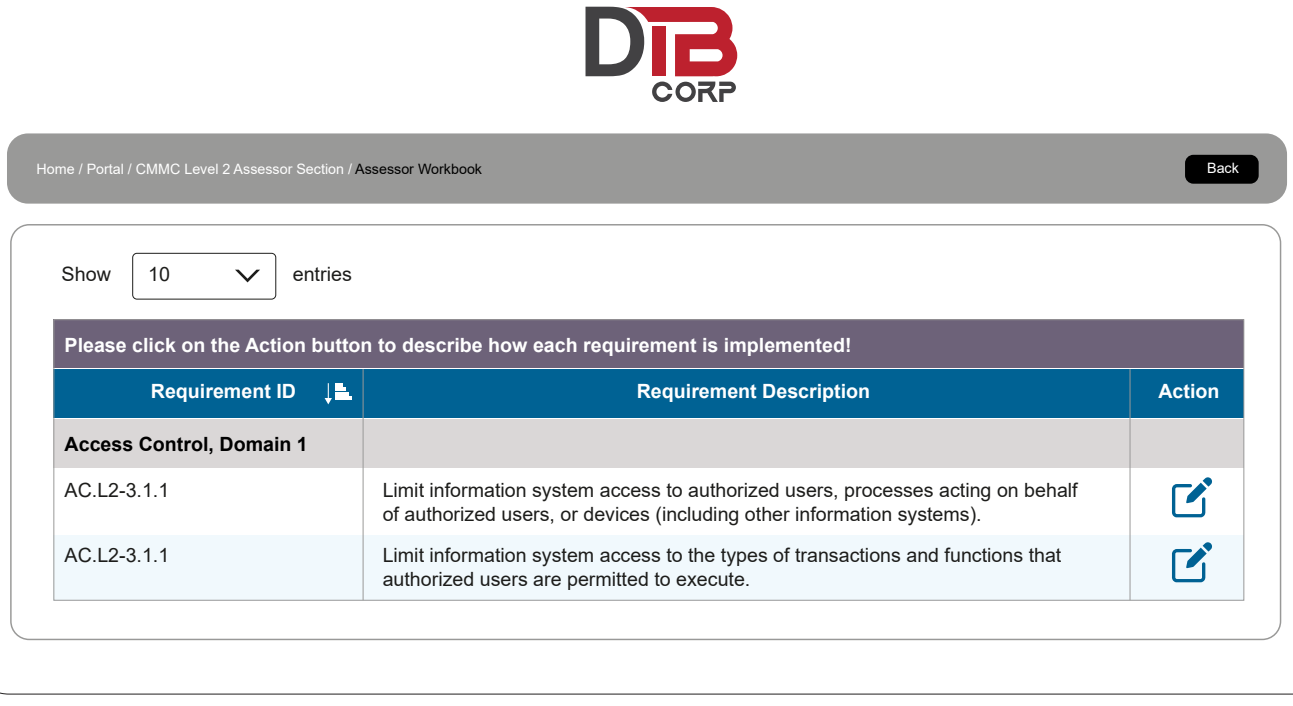
Intake Form 100%
Client Information 96.8%
Roles 31.3%
SSP Scope Document
General Questionnarie 29%

© ecfirst. All Rights Reserved, 2026

Phase 2 Questionnaire



Phase 3 Verification



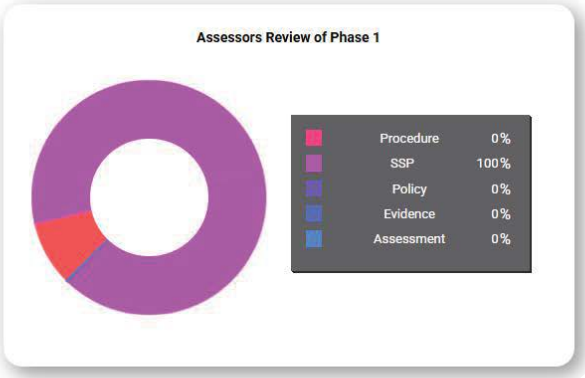
© ecfirst. All Rights Reserved, 2026

Dashboard

DTB CORP

Home / Assessment / CMMC 2.0 Level 2 Engagement / CMMC Level 2 Dashbaord





Final Report

© ecfirst. All Rights Reserved, 2026

HIPAA
Toolkit Package

ecfirst

Policy Template

Procedure Template

Plan Template

- HIPAA Privacy
- HIPAA Security
- HITECH Breach
- HIPAA Security Rule
- HIPAA Business Associate

Checklists

- Encryption
- Multi-Functional Devices
- Security Audit Readiness
- Vulnerability Assessment
- Application Security
- Secure Text Messaging

BAA Templates

- Business Associate → Business Associate
- Covered Entity → Business Associate

- HIPAA → ISO 27001
- HIPAA → NIST Cybersecurity Framework

Mappings

- HIPAA → NIST SP 800-171r2
- HIPAA → NIST SP 800-53r5
- HIPAA → PCI DSS

Forms

- Breach Log
- Change Management
- Media Chain of Custody
- HIPAA Privacy
- HIPAA Security
- Authorization for Release of PHI

- HIPAA and 42 CFR Part 2
- HIPAA Fines
- HIPAA for Covered Entities

Infographics

- HIPAA for Business Associate
- HIPAA Safe Harbor

Quick Reference Cards (QRC)

- HIPAA
- HIPAA Terminology
- HIPAA Privacy Rule
- HIPAA Security Rule
- HIPAA Final Rule
- HITECH Act

© ecfirst. All Rights Reserved, 2026

NIST
Toolkit Package

ecfirst

NIST SP 800-53r5 Toolkit

- Policy Template
- Infographics
  - NIST SP 800-53r5
- Procedure Template
- Quick Reference Card (QRC)
  - NIST SP 800-53r5
- Mappings
  - NIST SP 800-53r5 → HIPAA
  - NIST SP 800-53r5 → CMMC
  - NIST SP 800-53r5 → ISO 27001

NIST SP 800-171r2 Toolkit

- Policy Template
- Procedure Template
- Mappings
  - NIST SP 800-171r2 → CMMC
  - NIST SP 800-171r2 → HIPAA

NIST Cybersecurity Framework Toolkit

- Policy Template
- Quick Reference Card (QRC)
  - NIST Cybersecurity Framework
- Procedure Template
- Checklists
  - Cybersecurity Controls
  - Cybersecurity
  - NIST Cybersecurity
- Mappings
  - NIST Cybersecurity Framework → CMMC
  - NIST Cybersecurity Framework → HIPAA
  - NIST Cybersecurity Framework → ISO 27001

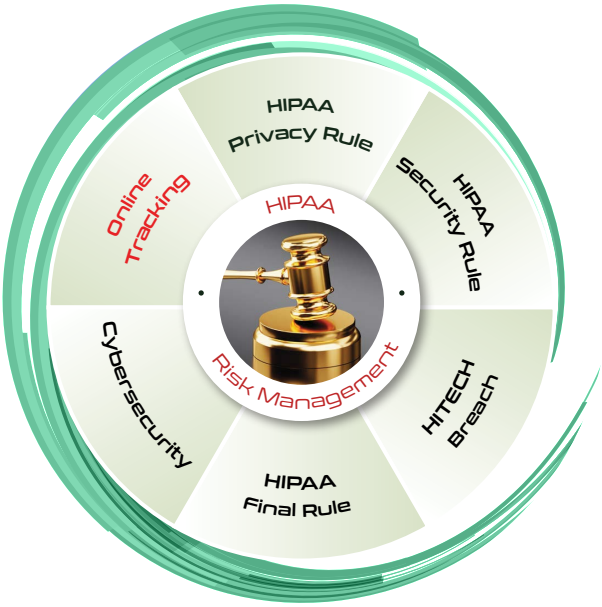
© ecfirst. All Rights Reserved, 2026

HIPAA Playbook

HIPAA™ Academy | ecfirst

Quick Links

- Home
- HIPAA Mandates
  - HIPAA Privacy Rule
  - HIPAA Security Rule
  - HIPAA Security NPRM
  - HITECH Breach
  - HIPAA FAQ
- Cybersecurity
- OCR Resolution Agreements
- Ransomware Guidance
- References
- Posters
- Templates
- Training
- Other Regulations





HIPAA Privacy Rule



HIPAA Security Rule



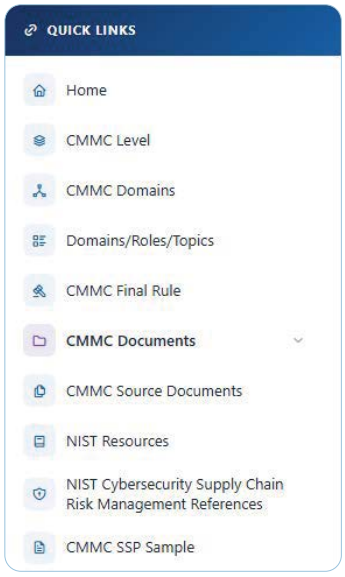
HIPAA Security NPRM

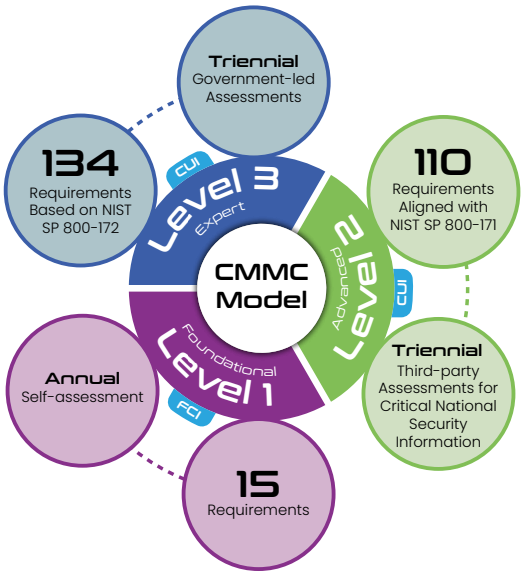


HITECH Breach



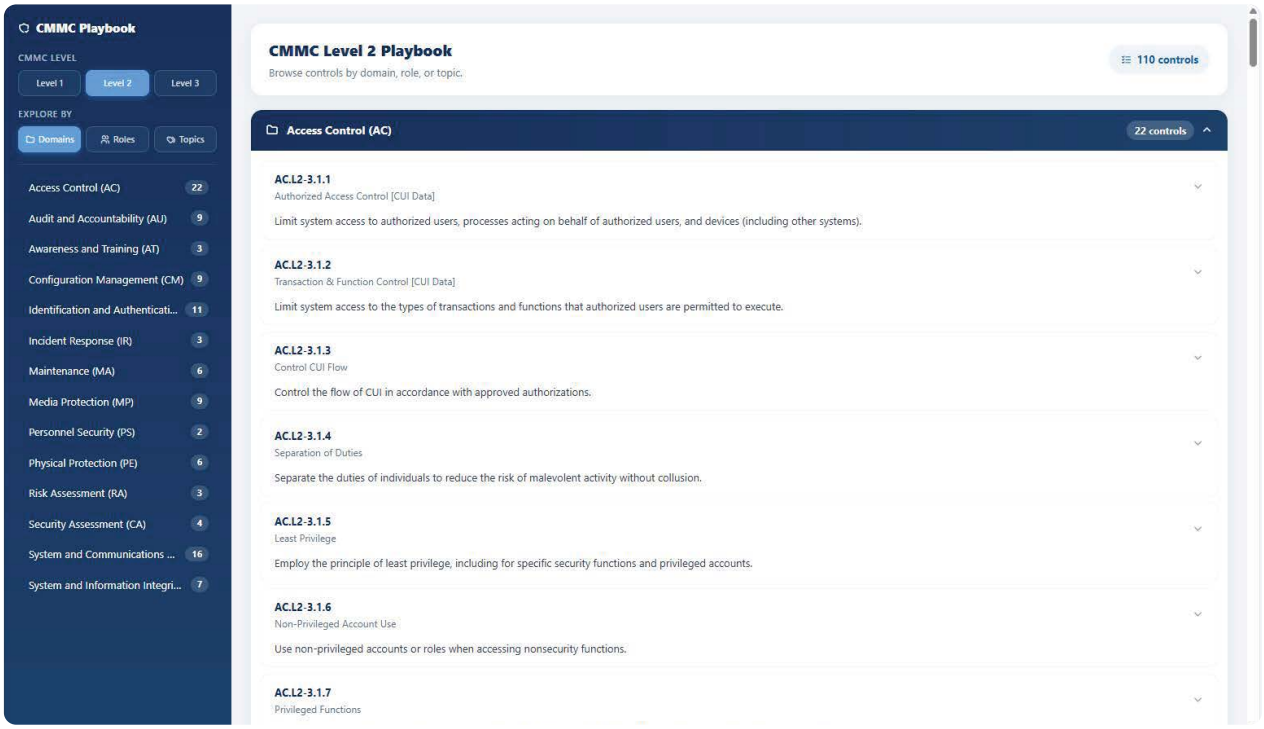
© ecfirst. All Rights Reserved, 2026







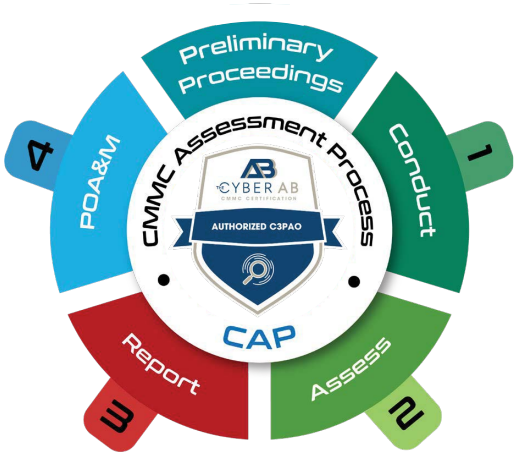
Domains



© ecfirst. All Rights Reserved, 2026

Quick Links

Home
ecfirst CAP Doctrine
CMMC Assessment Readiness
CMMC Training
Assessment Phases
Preliminary Proceedings
Phase 1: Conduct the Pre-Assessmment
Phase 2: Assess Conformity
Phase 3: Report Assessment Results
Phase 4: POA&M
CMMC Source Documents
Assessment Templates





ecfirst CAP Doctrine



CMMC Assessment Readiness

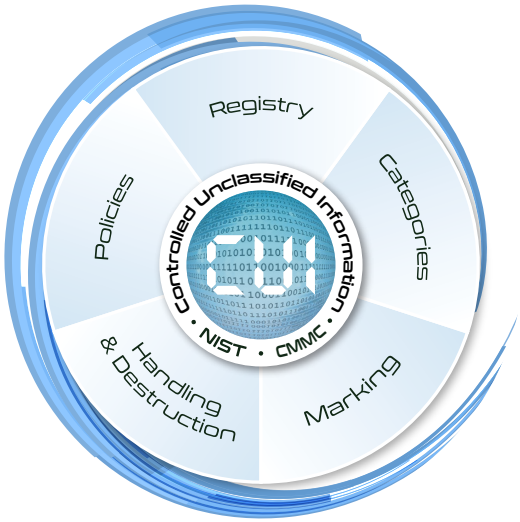


© ecfirst. All Rights Reserved, 2026

CUI Playbook

Quick Links

- Home
- CUI DoD
  - CUI DoD
  - About CUI
  - CUI Categories
  - DoD CUI Registry
  - CUI Marking
  - CUI DoD Policies
  - FAQ
- CUI NARA
  - CUI NARA
  - Introduction
  - CUI Registry
  - CUI Categories
  - CUI Marking
  - CUI Policy
  - CUI Glossary
  - CUI Resources
  - CUI FAQ





CUI | Department of Defense













About CUI









CUI | National Archives Records Administration (NARA)





















Training Resources

CCP | CCA

© ecfirst. All Rights Reserved, 2026

AI Governance Playbook

ecfirst

Quick Links

- Home
- AI Guidance
- NIST AI RMF
- Explore the Playbook





AI Guidance



NIST AI RMF



Explore the Playbook

Function	Title	AI Actors	Topics
Govern	GOVERN 1.1	Governance and Oversight	Legal and Regulatory Governance AI Actor Training
Govern	GOVERN 1.2	Governance and Oversight	Trustworthy Characteristics Governance Validity and Reliability Safety Secure and Resilient Accountability and Transparency Explainability and Interpretability Privacy Fairness and Bias
Govern	GOVERN 1.3	Governance and Oversight	Risk Tolerance Governance
Govern	GOVERN 1.4	Governance and Oversight	Risk Management Governance Documentation
Govern	GOVERN 1.5	Governance and Oversight Operation and Monitoring	Monitoring Governance Continual Improvement
Govern	GOVERN 1.6	Governance and Oversight	Risk Management Governance Data Documentation
Govern	GOVERN 1.7	AI Deployment Operation and Monitoring	Decommission Governance
Govern	GOVERN 2.1	Governance and Oversight	Governance Risk Culture
Govern	GOVERN 2.2	Governance and Oversight	Governance AI Actor Training
Govern	GOVERN 2.3	Governance and Oversight	Governance Risk Tolerance

Previous 1 2 3 4 5 ... 8 Next



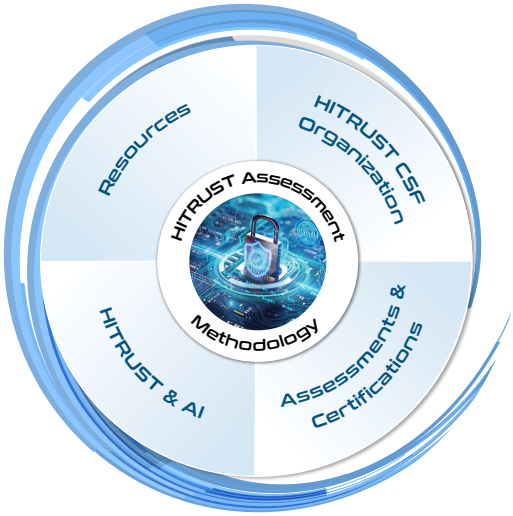
© ecfirst. All Rights Reserved, 2026

HITRUST Playbook

HITRUST Authorized External Assessor | ecfirst

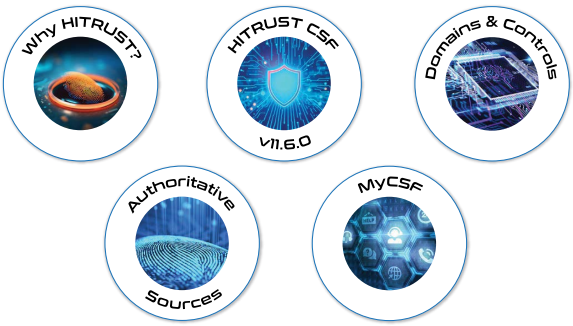
Quick Links

- Home
- HITRUST CSF Organization
  - Why HITRUST?
  - HITRUST CSF V11.6.0
  - Domains & Controls
  - Authoritative Sources
  - MyCSF
- Assessment & Certification
- HITRUST & AI
- HITRUST Resources
- Why ecfirst for HITRUST?





HITRUST CSF Organization



HITRUST Resources



Assessment & Certifications



HITRUST & AI



© ecfirst. All Rights Reserved, 2026

System Security Plan

Playbook | Template | Portal

SSP.ai System Security Plan | ecfirst

- The SSP describes how the controls and solutions meet the security requirements.
- The SSP explains how your organization handles sensitive information and defines how that data is stored, transmitted, and protected.
- The SSP criteria guide network and resource configuration to align with company goals.
- To keep the SSP current, implement a policy for annual review and updates.



SSP Playbook



Quick Links

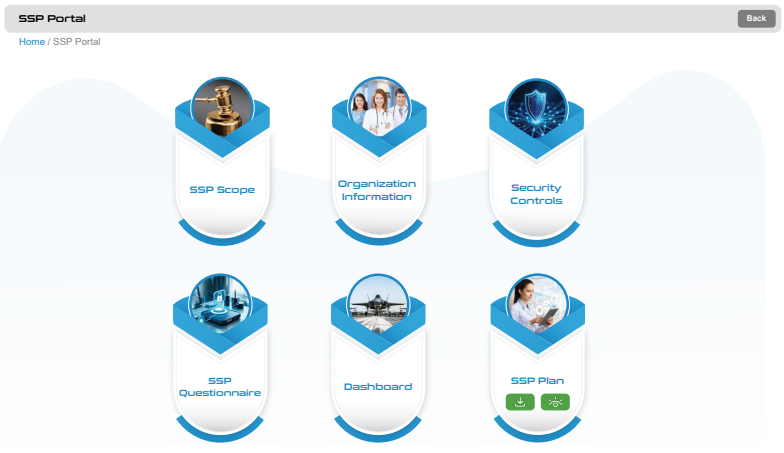
- Introduction
- SSP Components
  - System Identification
  - System Environment
  - System Requirements
- SSP Scope
- Examining SSP Requirements
  - Sample SSP
- NIST SP 800-171 SSP
  - How to Implement and Document
  - Components of an SSP
  - Benefits of SSP
- SSP Templates
- SSP References
- Training

SSP Templates





SSP.ai





Subscription

© ecfirst. All Rights Reserved, 2026

SSP Playbook

Quick Links

- Introduction
- SSP Components
  - System Identification
  - System Environment
  - System Requirements
- SSP Scope
- Examining CMMC SSP Requirements
  - Sample SSP
- NIST SP 800-171 SSP
  - How to Implement and Document
  - Components of an SSP
  - Benefits of SSP
- SSP Templates
- SSP References
- Training





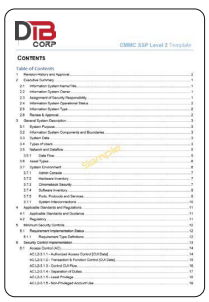
SSP Overview



SSP Templates



Inside the SSP



Training Resources

CCP™ | CCA™

© ecfirst. All Rights Reserved, 2026

SSP Template

SSP Level 1





SSP Level 2







© ecfirst. All Rights Reserved, 2026

SSP Portal

Home

SSP Portal Back

Select Framework

Please select the framework to proceed further

SSP Report



Preparation

SSP Portal Back

Home / SSP Portal



© ecfirst. All Rights Reserved, 2026

AI Training References

ecfirst

> Delivers the latest insights, including AI NIST RMF 100-1.

> Excellent AI content and resources.

> Excellent training & highly effective.

> Fantastic training with actionable items and resources.

> Honest, novel insights on AI disruption.

> Highly effective training with a strong overview of organizational needs and AI risk management lifecycle.

> Well-organized content.

© ecfirst. All Rights Reserved, 2026

"Comprehensive HIPAA course manual and content resources."

"In-depth HIPAA program that covers Privacy, Security, Breach and more."

Informative

Exceptional instructor

Well-crafted HIPAA program

Eye opening compliance resources

References

Extensive library of practice quizzes

Coverage of OCR HIPAA fines

Well-organized training

Comprehensive

"Provided important information for managing HIPAA Compliance."

"Well organized presentation with a strong scope of knowledge."

"Insightful HIPAA Program and positive learning experience."

"Resources for HIPAA compliance/breach material was eye opening."

© ecfirst. All Rights Reserved. 2026

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.

© ecfirst. All Rights Reserved, 2026

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

"The training provided clarity on complex cloud compliance issues."

References

I loved the training

Prepared me for exam

Privileged to participate

Excellent introduction to NIST

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."

© ecfirst. All Rights Reserved, 2026

IRON medical systems℠

"As the largest IaaS provider to the radiation oncology sector, IMS has always prioritized privacy and protection. Our first HITRUST experience left us unprepared, but ecfirst completely changed that. Their transparency, advocacy, and expertise have been invaluable—helping us renew certification, strengthen processes, and become a better company. We look forward to continuing our partnership with ecfirst as we build on HITRUST as the foundation of our risk management framework."

P3 Health Partners
People. Passion. Purpose.

"Working with ecfirst has been invaluable to P3. Their expertise and structured approach made our HITRUST certification seamless, strengthening our security posture and IT resilience. Highly recommend."

GALEN DATA

"Thanks again for your hard work, advice and support throughout the HITRUST engagement. I want to reiterate that I truly appreciate the level of service the ecfirst Team provides. **I would not want to go through HITRUST with anyone else**."

© ecfirst. All Rights Reserved, 2026

HIPAA Consulting References

ecfirst

AULTMAN

"I've worked with ecfirst for 5 years under a multiyear contract, and they've consistently delivered timely work, prompt responses, clear updates, and overall excellent support—Aultman is very satisfied with their services."

BrightOutcome

"ecfirst has been our trusted partner for over a decade, helping us with HIPAA/HITECH policies, procedures, risk assessments, and expert guidance. We are now partnering with their team to extend our policies to include NIST, FERPA, and FISMA. They are prompt, reliable, and consistently deliver on time — a 10 out of 10 in my experience. I'm extremely satisfied with ecfirst, which is why we've sustained a decade-long partnership."

BRG
Berkeley Research Group

"BRG leveraging their expertise for annual risk management and HIPAA compliance assessments, HITRUST certification, and emergency incident response support. Their responsiveness is exceptional, and they consistently meet or exceed project timelines. With the highest level of satisfaction, we consider ecfirst at the very top of our trusted business partner list."

bentek
BENEFITS TECHNOLOGY

"ecfirst team is highly responsive and consistently delivers as outlined, with clear expectations and thorough communication before, during, and after each engagement. Their audits and reports are always thorough, effective, and timely, and I rely on them as the foundation for follow-up SOC2 audits. I greatly trust ecfirst's expertise."

© ecfirst. All Rights Reserved. 2026

CMMC Consulting References

ecfirst

MX2 TECHNOLOGY
Executive IT Leadership

"The MX2 mantra that we are on the runway to client CMMC success has been rocket fueled with the devotion of the ecfirst CMMC Team. Married with their surgical methodology, their CMMC Unreadiness + their SSP Secret SaiCE references, and their commitment to the CMMC ecosystem, has resulted in deep value to MX2.

When MX2 set out on the path to achieve CMMC Level 2 certification, it was very important to our leadership team to select the right C3PAO to partner with.

Five key reasons why MX2 Technology chose ecfirst as our C3PAO partner. Trust, Methodology, Client Commitment, Humility in Execution & Leadership."

solv it

"Despite it being our first audit, the ecfirst Team was devoted throughout the assessment. Their expertise across the Body of Evidence for 110 requirements and 320 objectives was invaluable. We successfully navigated the audit and learned a great deal—looking forward to working with ecfirst again."

CYFLARE
The threat stops here.

"This was a 16-month journey of preparation, assessments, and teamwork - **I couldn't be prouder of what this means for our company and our customers.**

ecfirst - our official C3PAO - made the process **enjoyable and painless.**

Thank you, Team ecfirst!"

HEARTLAND BUSINESS SYSTEMS

"The CMMC training was comprehensive, engaging, and backed by invaluable resources and real-world expertise. Impressed by their quality and dedication, I hired ecfirst for consulting, which has significantly strengthened our RPO services. Partnering with ecfirst was one of our best decisions, and I highly recommend them for CMMC training, consulting, and C3PAO certification support."

© ecfirst. All Rights Reserved. 2026

ARIENTO
IT | CYBERSECURITY | COMPLIANCE

"We truly appreciate the professionalism, competency, and thoroughness of the ecfirst team. You have assembled a seasoned, highly experienced group that ensures C3PAO CMMC engagements are expertly managed and flawlessly executed. We look forward to future opportunities to collaborate within the CMMC ecosystem."

FAIRWINDS
TECHNOLOGIES

"Working with the ecfirst team has been an **outstanding experience.** From start to finish, Casey McLoughlin, Dr. Dwayne Hodges, and Ali Pabrai demonstrated exceptional professionalism, responsiveness, and **deep expertise** in guiding Fairwinds through the CMMC Level 2 assessment process.

ecfirst communicated clearly and promptly, which made each step in the process feel seamless. Whether it was coordinating schedules, clarifying requirements, or resolving last-minute issues, the team at ecfirst handled everything with efficiency and a **positive attitude.** Their proactive approach ensured that our assessment stayed on track and that all deliverables were reviewed accurately and on time.

What stood out most was Dr. Hodges' personal commitment to collaboration. He consistently went above and beyond—providing timely updates, sharing critical feedback, and ensuring our team had the support needed to succeed. This level of **dedication** not only made the process productive but also instilled confidence that we were in capable hands.

Thanks to ecfirst's efforts, the entire engagement was smooth, organized, and **highly effective.** I would strongly recommend ecfirst to any organization seeking a trusted partner for compliance and cybersecurity initiatives."

© ecfirst. All Rights Reserved, 2026

"I am happy to let you know **I passed** the CMMC **CCP exam** on my **first attempt.** The CCP prep process was **easier** than I expected - thanks to the **fantastic training class** and **study materials** from the **ecfirst CCP Academy!** I appreciated **my ecfirst** experience."

Gladly recommend

Excellent flow of the training

Really enjoyed doing quizzes as a group

Thorough and extensive information

Increased my CMMC knowledge exponentially

References

CCP course synthesized the universe of CMMC

A different perspective to the CMMC process

Easy to navigate the CCP Academy Portal

Amazing infographics and content

Tremendous class

"Fantastic course. I appreciated the real-world examples and scenarios."

"Clear, concise, and professional."

"Focused materials and explanations were extremely helpful."

"Great training and resources provided. The portal and quizzes are invaluable for exam prep."

"Excellent instructor—knowledgeable, approachable, and great at explaining complex material."

© ecfirst. All Rights Reserved. 2026

"The **ecfirst CCA Program** was extensive with excellent assessment resources.

Practical, real-world CMMC assessment Scenarios presented, including insight on a credible SSP."

Exceptional dual instructors

Depth of knowledge

Liked the group exercises

Rich material in the CCA Academy Portal

In-depth coverage of CMMC scenarios

References

Loved the CCA quizzes and resources

Thank you for the bulk download

Industry background was invaluable

Real artifacts was fantastic

Terrific course

"Very professional and exceptionally detailed. Empowered and excited."

"Real-world experiences in discussions was awesome."

"Focused materials and explanations were extremely helpful."

"Valuable, motivating, and well-taught. Worth every penny."

"Reality focused, not theoretical – the group scenarios brought everything together."

© ecfirst. All Rights Reserved. 2026

ecfirst



Get Started

295 NE Venture Drive
Waukee, Iowa 50263
United States of America

Info@ecfirst.com

www.ecfirst.com | www.ecfirst.biz