Program CATALOG

ecfirst

HITRUST Authorized External Assessor | HIPAA™ Academy | CYBER AB Authorized C3PAO | CYBER AB Registered Practitioner Organization RPO | aiCRP AI Cyber Risk Professional | TRACER℠ ASSET RISK MANAGEMENT

Message from the Chief Executive

Welcome to ecfirst!

At ecfirst, We at ecfirst 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

CAICO LEAD CCA | CAICO PI | CAICO CMMC CERTIFIED PROFESSIONAL CCP | CISSP | HITRUST CCSFP

ecfirst Facts

1000's of **Satisfied** Customers

Services **Delivered** on 5 Continents

50 U.S. States **Clients** in All

20+ **Years** of Service

Ready to Serve
The CMMC Ecosystem

Iowa's 1st

America's 52nd

U.S. Department of Defense

THE CYBER AB
CMMC CERTIFICATION
AUTHORIZED C3PAO

Flexible with HIPAA compliance program

ecfirst chosen for their deep commitment to HIPAA

Excited to partner with ecfirst on cyber, HIPAA compliance

HIPAA™ Academy References

Strongly recommend ecfirst for covered entities, associates

Leader in helping hospitals meet privacy mandates

Trusted partner for long-term success

Partner trusted for U.S. mandates

Guided us every step

Always delivered without any delays

The HITRUST experience was truly invaluable

Appropriate SMEs answered all our questions thoroughly

HITRUST® Authorized External Assessor References

Instrumental in our maturity on security and compliance

Always has a ear to lend to listen and guide

They are an extremely devoted SME team

Valued partner in our HITRUST journey

Tremendous Support

Leadership

Ali Pabrai

Chief Executive & Co-founder

Allen Nguyen

President & Co-founder

Debbie Burke

VP, Operations & Finance

Mike Turpin

VP, Global Assessments

Ben Miller

Director, Cyber Defense

Dave Ekstrom

Team Lead, HITRUST

Will Allen

Team Lead, Assessments

Lorna Waggoner

Director, Training & Certification

Audra Curtis

Team Lead, Certification Programs

Casey McLoughlin

Team Lead, Client Operations

Table of Contents

AI

Certification Training

HITRUST

HIPAA

NIST

Cyber Defense

CMMC

Compliance

Online Store

Client References

aiCRP

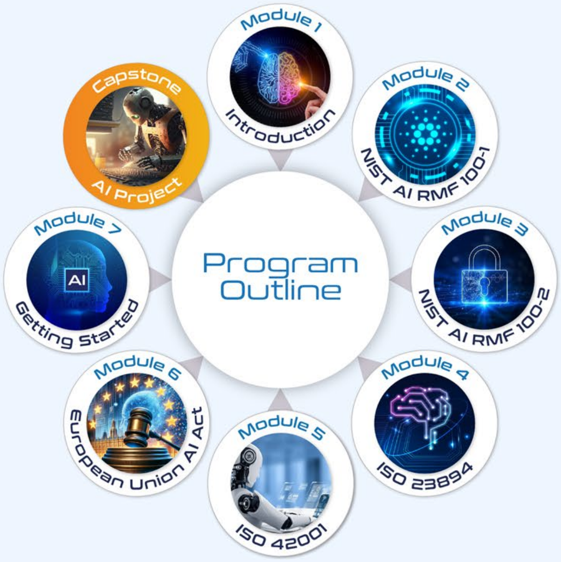
AI Cyber Risk Professional

Online | Self-Paced

ecfirst

The Industry's First AI Cyber Risk Management Training Program

HIMSS APPROVED EDUCATION PARTNER | CEU 8 Hours | AI-Powered Assistant BaiLEY



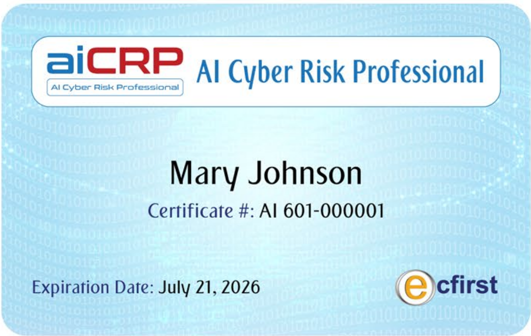
Unlock the World's First AI Playbook

AI CYBER RISK Management Playbook

AI Governance Playbook

What's in it for you?

- Examine the NIST AI Risk Management Framework (RMF)
- Review valued AI resources for risk management including ISO 23894 and ISO 42001
- 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



aiCRP AI Cyber Risk Professional | AI Cyber Risk Professional

Mary Johnson

Certificate #: AI 601-000001

Expiration Date: July 21, 2026

ecfirst

Digital Badge

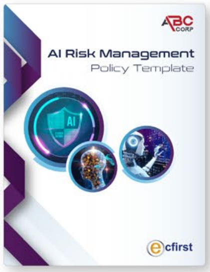
ecfirst also offers a Digital Badge with your certification. There is no fee for this service and acceptance is totally up to you.

aiCRP AI Cyber Risk Professional

AI Risk Management Assessment

AI raksha defense | ecfirst

1


AI Risk Management
Policy Template

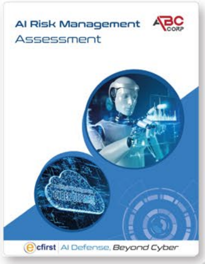
ecfirst

2

AI Risk Management
Plan

ecfirst

3


AI Risk Management
Assessment

ecfirst | AI Defense, Beyond Cyber

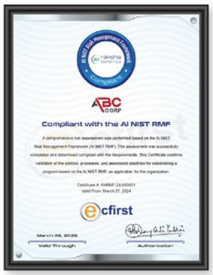
NIST AI 100-1 • ISO 23894 • ISO 42001

AI Risk Assessment

AI raksha defense

ABC CORP

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


AI NIST Risk Management Framework

Compliant

ABC CORP

Compliant with the AI NIST RMF

A comprehensive risk assessment was performed based on the AI NIST Risk Management Framework (AI NIST RMF). The assessment was successfully completed and determined compliant with the Requirements. This Certificate confirms validation of the policies, processes, and associated practices for establishing a program based on the AI NIST RMF, as applicable, for the organization.

Certificate #: ANRMF-24-000001
Valid From: March 27, 2024

ecfirst

March 26, 2025
Valid Through

Authorization

Certificate

Sources

INTERNATIONAL STANDARD

ISO/IEC 23894

First edition
2023-02

Information technology — Artificial intelligence — Guidance on risk management

Technologies de l'information — Intelligence artificielle — Recommandations relatives au management du risque

Reference number
ISO/IEC 23894:2023(E)

© ISO/IEC 2023

ISO 23894

NIST AI 100-1

Artificial Intelligence Risk Management Framework (AI RMF 1.0)

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST AI 100-1

INTERNATIONAL STANDARD

ISO/IEC 42001

First edition
2023-12

Information technology — Artificial intelligence — Management system

Technologies de l'information — Intelligence artificielle — Système de management

Reference number
ISO/IEC 42001:2023(E)

© ISO/IEC 2023

ISO 42001

AI
Certification Training
HITRUST
HIPAA
NIST
Cyber Defense
CMMC
Compliance
Online Store
Client Reference

AI | HIPAA | Cyber Defense

Certification Training Programs

HIMSS APPROVED EDUCATION PARTNER | ecfirst

CHP Certified HIPAA Professional HIPAA Academy

CEU 16 Hours

Healthcare Industry's First & Leading HIPAA Credential

- 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

CEU 16 Hours

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

- 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

CSCS™ CERTIFIED SECURITY COMPLIANCE SPECIALIST

CCSA℠ Certified Cyber Security Architect

CEU 8 Hours

An Executive Cybersecurity Program

- 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

CEU 8 Hours

The Industry's First AI Cyber Risk Management Training Program

- Examine the NIST AI Risk Management Framework (RMF)
- Review valued AI resources for risk management including ISO 23894 and ISO 42001
- 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

aiCRP AI Cyber Risk Professional

CHP Certified HIPAA Professional

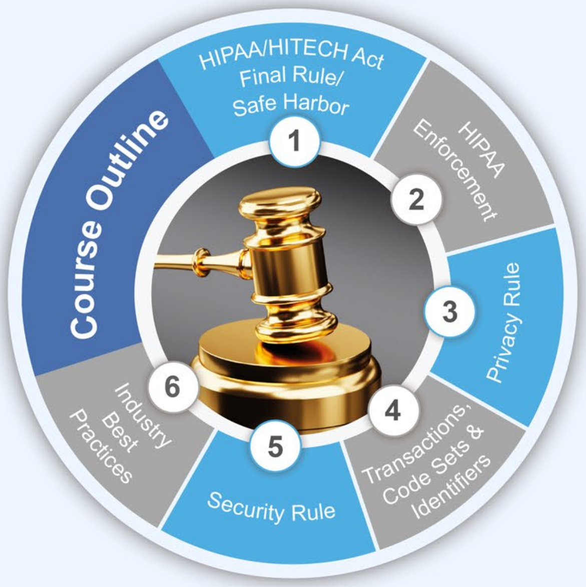
HIPAA Academy

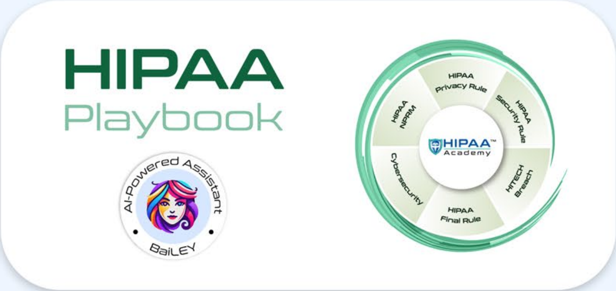
Virtual | Online | Public

HIPAA™ Academy | ecfirst

Healthcare Industry's First & Leading HIPAA Credential

HIMSS Approved Education Partner | CEU 16 Hours

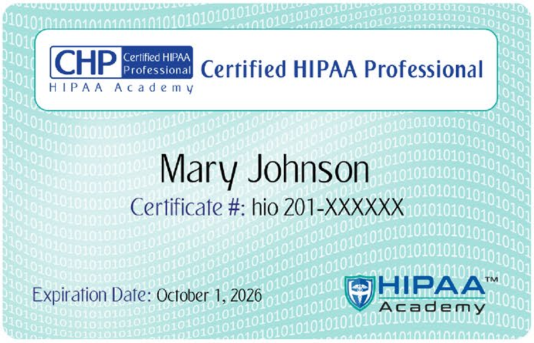

Course Outline
1 HIPAA/HITECH Act Final Rule/ Safe Harbor
2 HIPAA Enforcement
3 Privacy Rule
4 Transactions, Code Sets & Identifiers
5 Security Rule
6 Industry Best Practices



> **Precise**, **informative**, and **well-structured** HIPAA content. Would love to recommend ecfirst.

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



CHP Certified HIPAA Professional HIPAA Academy **Certified HIPAA Professional**

Mary Johnson

Certificate #: hio 201-XXXXXX

Expiration Date: October 1, 2026

HIPAA™ Academy

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 AI Cyber Risk Professional

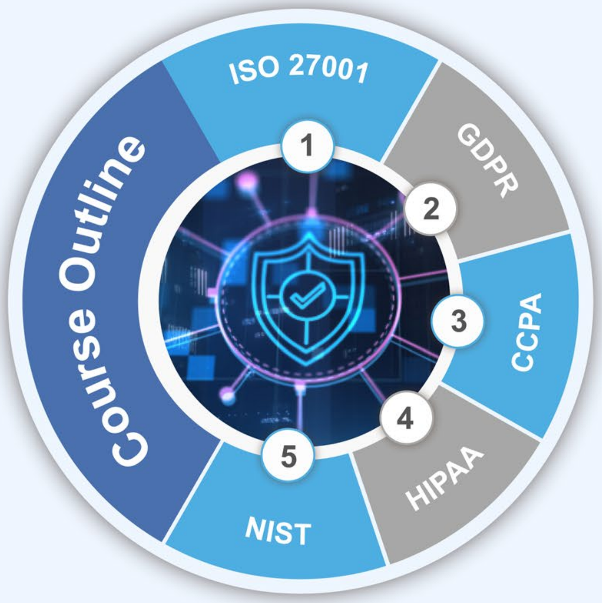
AI
Certification Training
HITRUST
HIPAA
NIST
Cyber Defense
CMMC
Compliance
Online Store
Client Reference

CSCS™
CERTIFIED SECURITY COMPLIANCE SPECIALIST
Online | Self-Paced

ecfirst

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

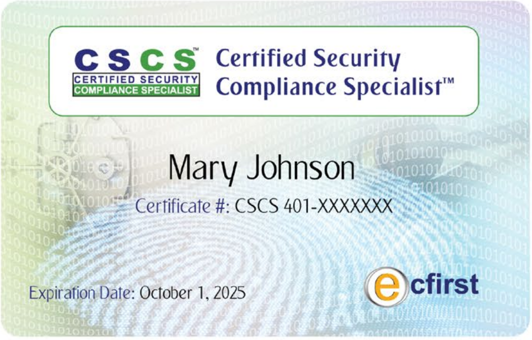
HIMSS APPROVED EDUCATION PARTNER | CEU 16 Hours



> “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


CSCS Certified Security Compliance Specialist™

Mary Johnson

Certificate #: CSCS 401-XXXXXXX

Expiration Date: October 1, 2025

ecfirst

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℠

Certified Cyber Security Architect

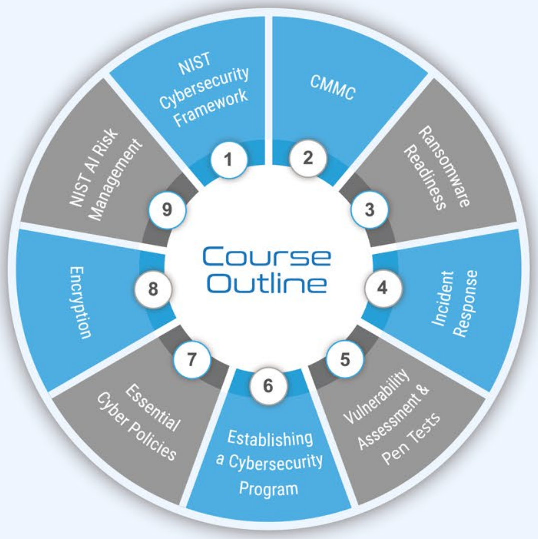
Online | Self-Paced

ecfirst

An Executive Cybersecurity Program

HIMSS APPROVED EDUCATION PARTNER

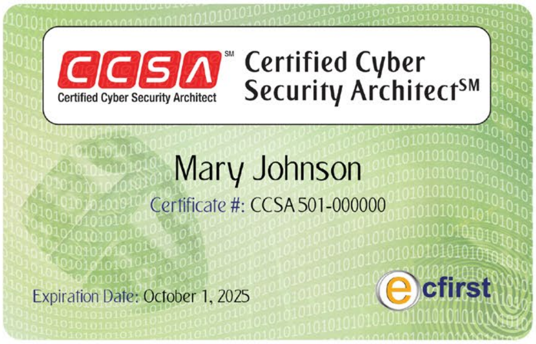
CEU 8 Hours



> “**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



CCSA℠ Certified Cyber Security Architect

Certified Cyber Security Architect℠

Mary Johnson

Certificate #: CCSA 501-000000

Expiration Date: October 1, 2025

ecfirst

Digital Badge

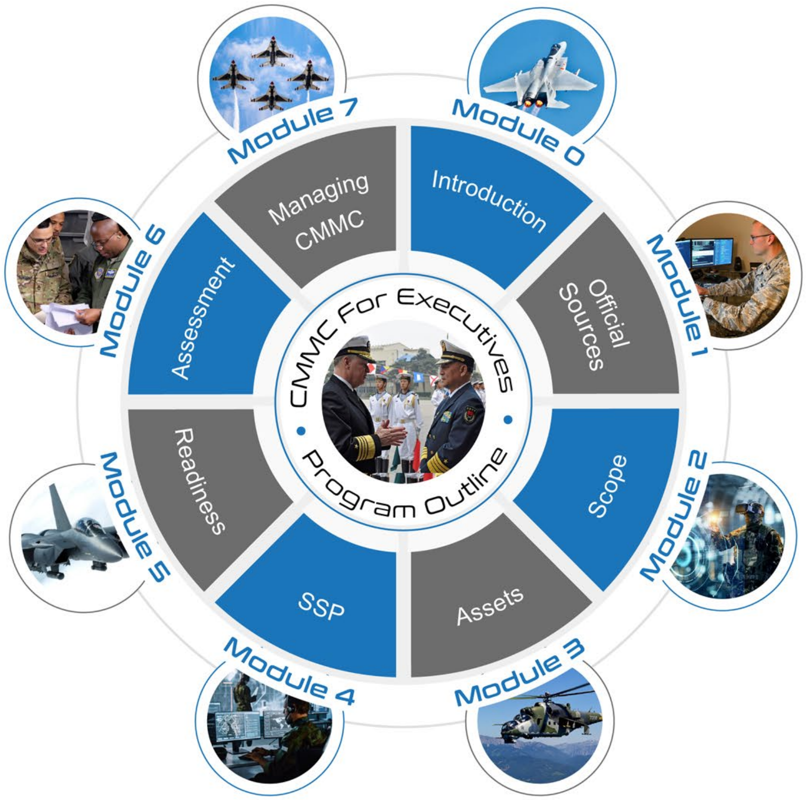
ecfirst also offers a Digital Badge with your certification. There is no fee for this service and acceptance is totally up to you.

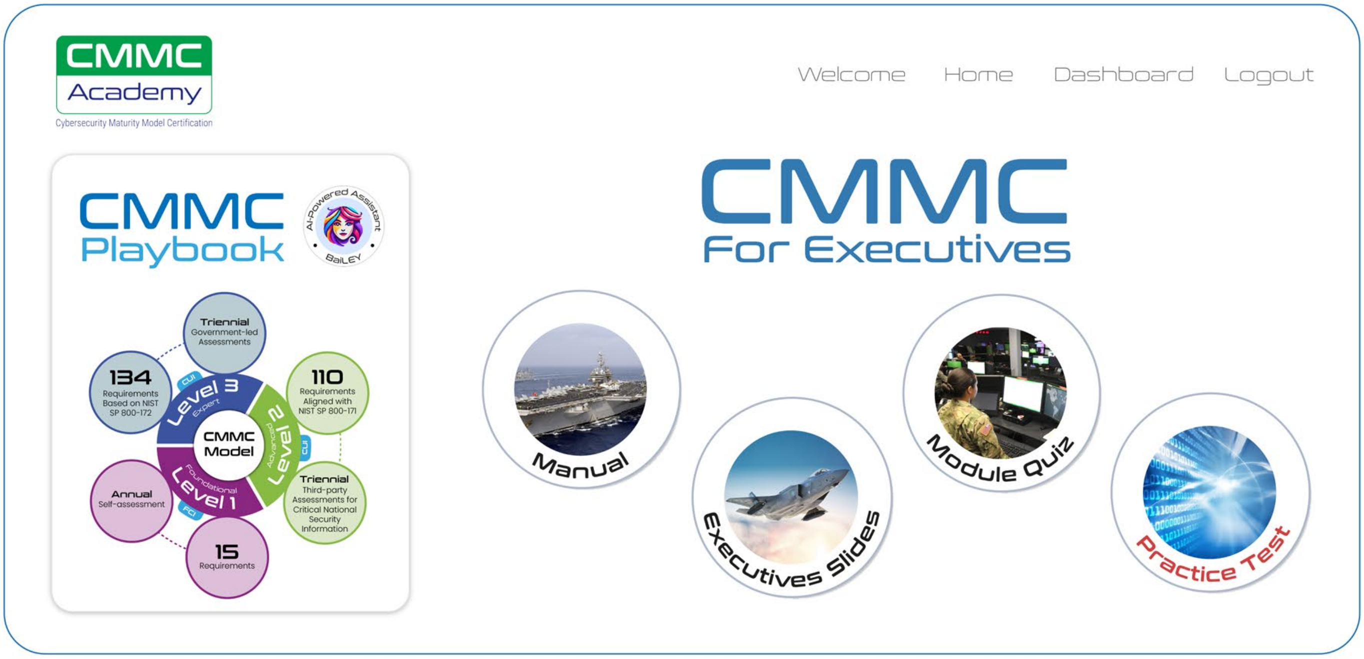
CMMC For Executives

Online | Self-Paced

ecfirst

An Executive CMMC Program | CEU 8 Hours



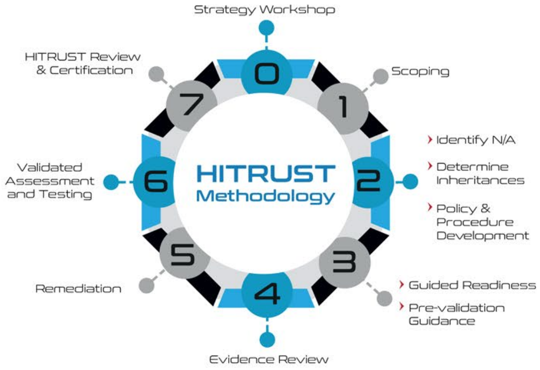


HITRUST
Why ecfirst?

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

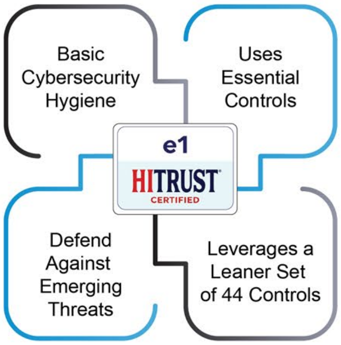
Flat Price

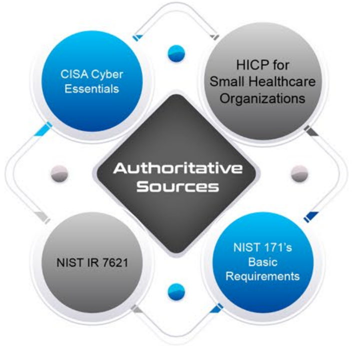
HITRUST e1 Certification

HITRUST Authorized External Assessor | ecfirst

e1 Essentials

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


Basic Cybersecurity Hygiene
Uses Essential Controls
e1
HITRUST CERTIFIED
Defend Against Emerging Threats
Leverages a Leaner Set of 44 Controls


CISA Cyber Essentials
HICP for Small Healthcare Organizations
Authoritative Sources
NIST IR 7621
NIST 171's Basic Requirements

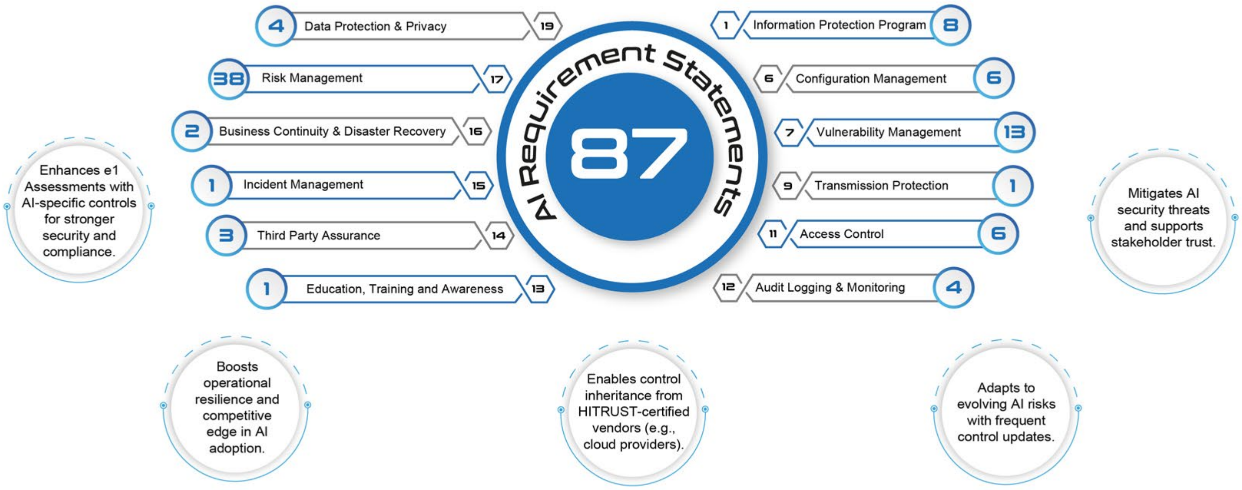
HITRUST e1 and HIPAA

- 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


4 Data Protection & Privacy 19
38 Risk Management 17
2 Business Continuity & Disaster Recovery 16
1 Incident Management 15
3 Third Party Assurance 14
1 Education, Training and Awareness 13
AI Requirement Statements
87
1 Information Protection Program 8
6 Configuration Management 6
7 Vulnerability Management 13
9 Transmission Protection 1
11 Access Control 6
12 Audit Logging & Monitoring 4
Enhances e1 Assessments with AI-specific controls for stronger security and compliance.
Mitigates AI security threats and supports stakeholder trust.
Boosts operational resilience and competitive edge in AI adoption.
Enables control inheritance from HITRUST-certified vendors (e.g., cloud providers).
Adapts to evolving AI risks with frequent control updates.

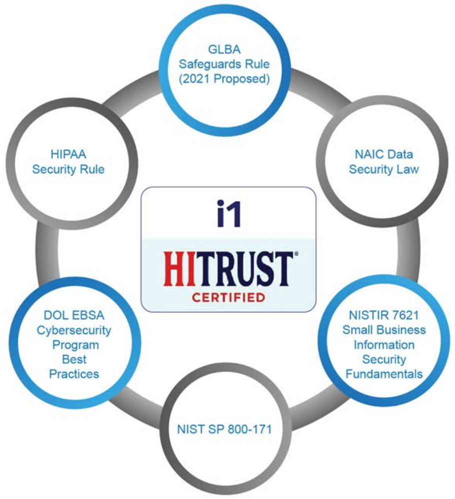
HITRUST i1 Certification

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
HITRUST®
CERTIFIED
GLBA Safeguards Rule (2021 Proposed)
NAIC Data Security Law
NISTIR 7621 Small Business Information Security Fundamentals
NIST SP 800-171
DOL EBSA Cybersecurity Program Best Practices
HIPAA Security Rule

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
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.

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

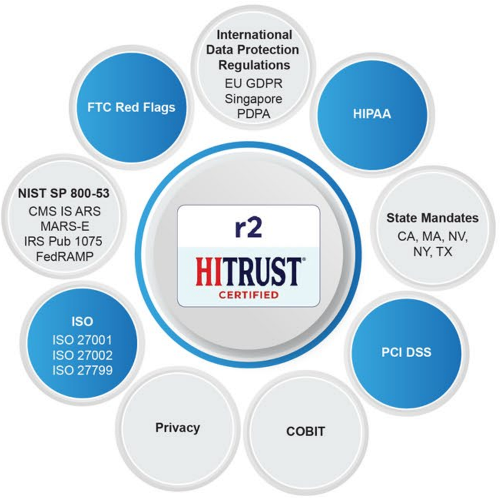
HITRUST r2 Certification

HITRUST Authorized External Assessor | ecfirst

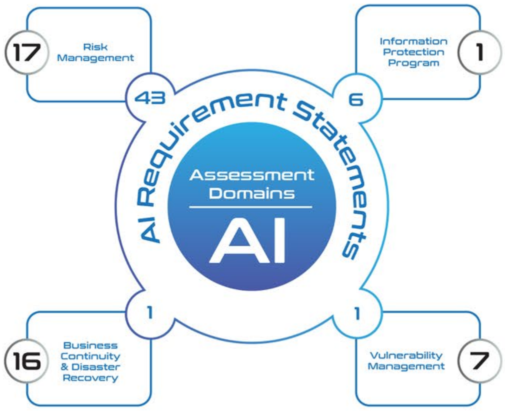
r2 Key Highlights

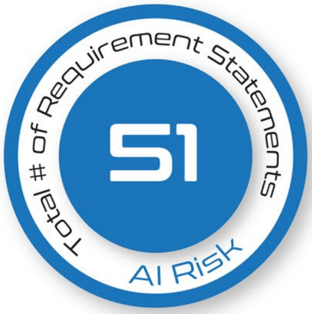
Comprehensive Controls	Up to 250 aligned with major standards
Customizable	Select controls based on risk and compliance needs
HIPAA & NIST CSF Reporting	Automated evidence collection and compliance reports
Proven Assurance	Transparent results for stakeholder confidence
Control Inheritance	Reuse prior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

HITRUST r2 Certification

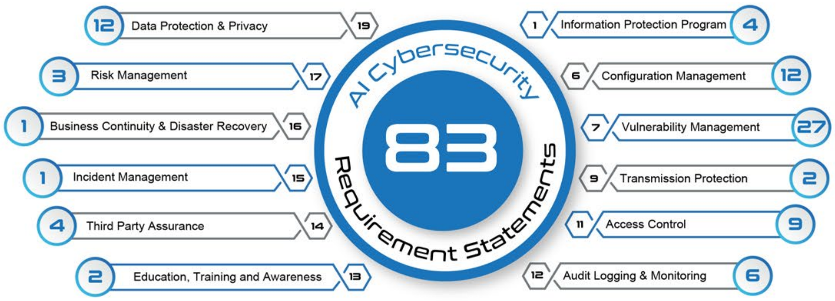


AI Cybersecurity Requirements


17
Risk Management
1
Information Protection Program
16
Business Continuity & Disaster Recovery
7
Vulnerability Management
43
6
1
1
AI Requirement Statements
Assessment Domains
AI



AI Cybersecurity Requirements

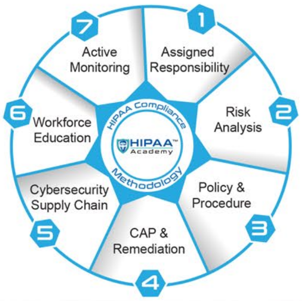


HITRUST's AI Assurance program provides certification and an insight report, integrating AI frameworks into MyCSF to streamline assessments and enhance security.

HIPAA

Why ecfirst?

HIPAA™ Academy | ecfirst



HIPAA *Signature* Methodology

Industry Leading HIPAA Certification Training

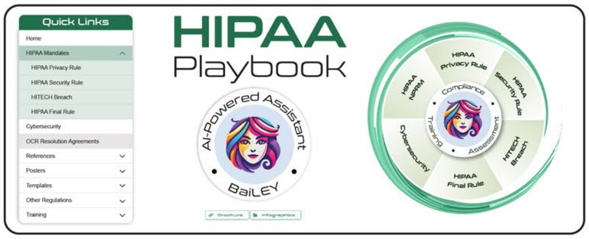
Updated with NPRM

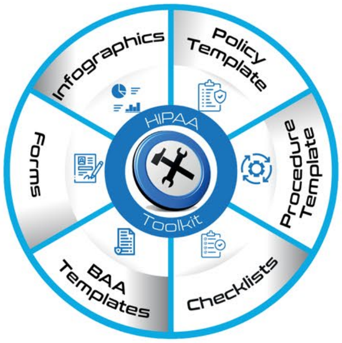
CHP Certified HIPAA Professional
HIPAA Academy

HITRUST®
Authorized External Assessor

Delivering HITRUST Certification Since 2016

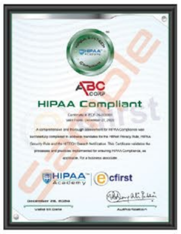
AI Powered HIPAA Playbook





HIPAA Toolkit
www.ecfirst.biz

HIPAA NPRM Assessment



ABC CORP

HIPAA Compliant

Certificate # ECF-24-00000
Valid From: December 21, 2022

A comprehensive and thorough assessment for HIPAA Compliance was successfully completed to address mandates for the HIPAA Privacy Rule, HIPAA Security Rule and the HITECH Breach Notification. This Certificate validates the processes and practices implemented for ensuring HIPAA Compliance, as applicable, for a business associate.

HIPAA™ Academy | ecfirst

December 26, 2024
Valid till Date

Authorization

HIPAA Compliance Attestation

Risk Assessment

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

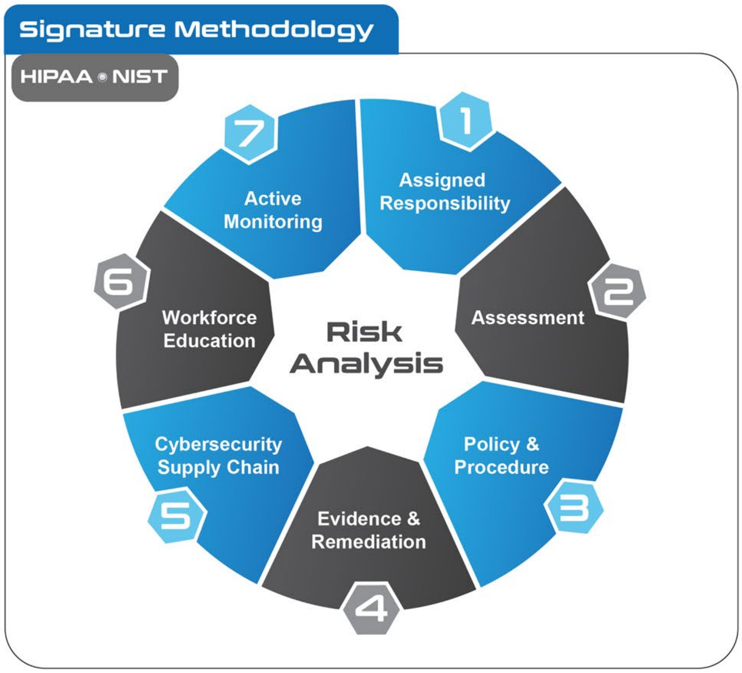
ecfirst

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

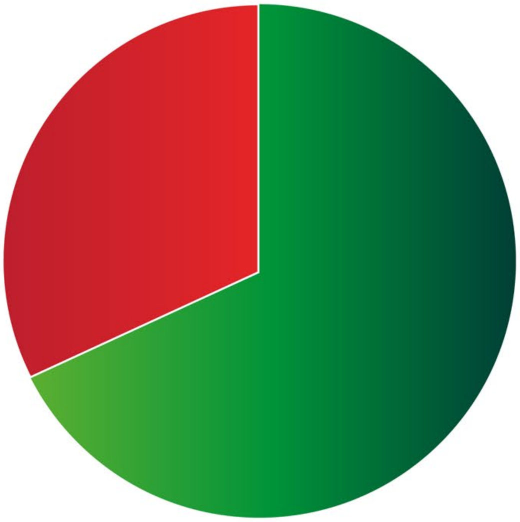
HIPAA Mandates

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

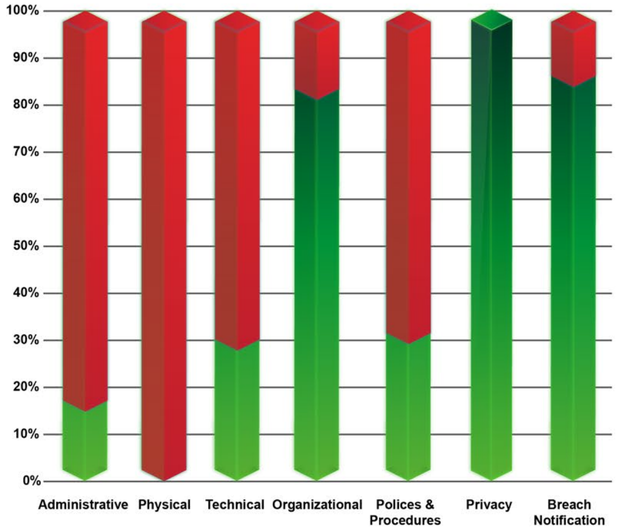
Signature Methodology



Compliance Status



Implementation Specifications



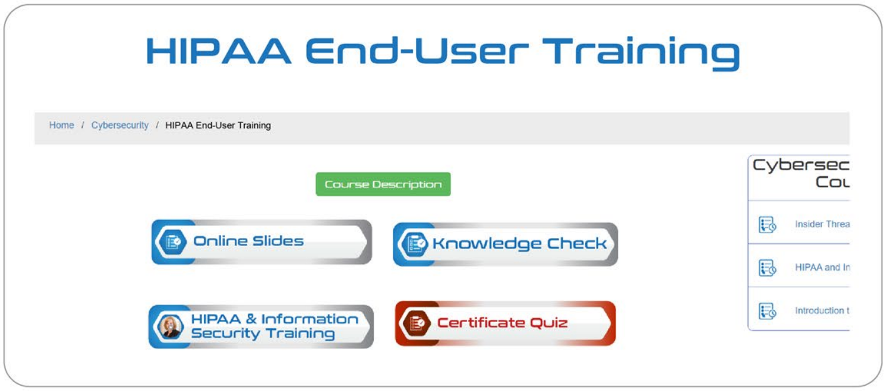
🟩 Met 🟥 Not Met

AI
Certification Training
HITRUST
HIPAA
NIST
Cyber Defense
CMMC
Compliance
Online Store
Client Reference

HIPAA End-User Package

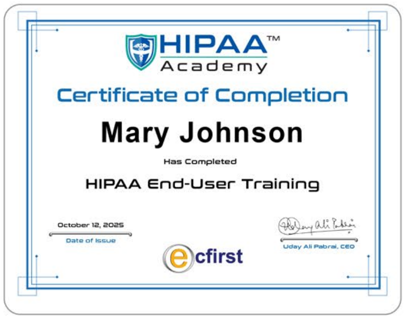
- End-to-end training content covering HIPAA Privacy, HIPAA Security, HITECH Breach, the HIPAA Final Rule, and more
- Practice quiz to emphasize important concepts
- HIPAA End-User Certificate Exam
- Several sample documents for reference including HIPAA quick reference cards, flash cards, and more

HIPAA™ Academy Portal



HIPAA End-User Training

Home / Cybersecurity / HIPAA End-User Training



HIPAA™ Academy

Certificate of Completion

Mary Johnson

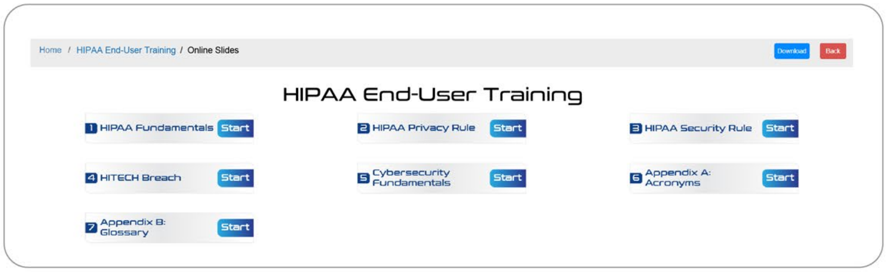
Has Completed

HIPAA End-User Training

October 12, 2025
Date of Issue

Uday Ali Pabrai, CEO

ecfirst



Home / HIPAA End-User Training / Online Slides

HIPAA End-User Training

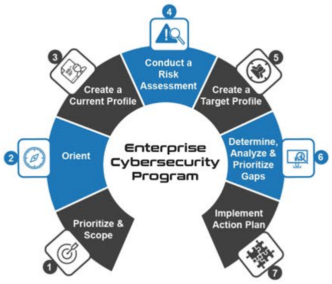
Download
Back
1 HIPAA Fundamentals Start
2 HIPAA Privacy Rule Start
3 HIPAA Security Rule Start
4 HITECH Breach Start
5 Cybersecurity Fundamentals Start
6 Appendix A: Acronyms Start
7 Appendix B: Glossary Start

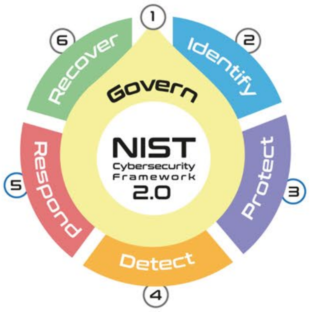
NIST

Why ecfirst?

ecfirst

NIST *Signature* Methodology





NIST 2.0 Assessment

Industry Leading Cybersecurity Certification Training

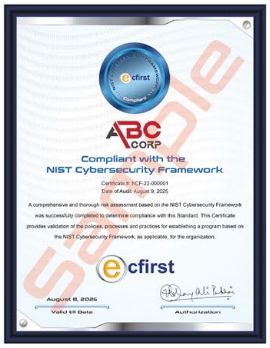
CCSA℠
Certified Cyber Security Architect

NIST Cybersecurity Framework
Risk Assessment Report

ecfirst

NIST Risk Assessment Report

NIST Compliance Attestation



ecfirst
NIST Cybersecurity Framework Compliant

ABC CORP

Compliant with the
NIST Cybersecurity Framework

Certificate #: NCF-22-000001
Date of Audit: August 9, 2025

A comprehensive and thorough risk assessment based on the NIST Cybersecurity Framework was successfully completed to determine compliance with this Standard. This Certificate provides validation of the policies, processes and practices for establishing a program based on the NIST Cybersecurity Framework, as applicable, for the organization.

ecfirst

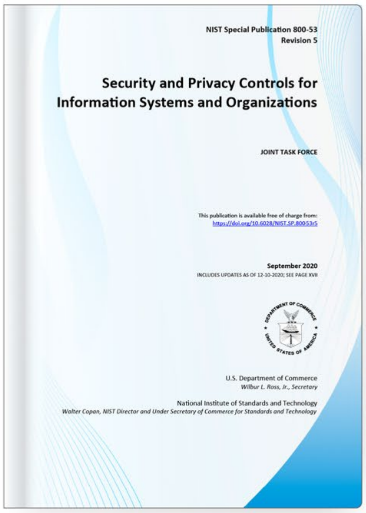
August 8, 2026
Valid till Date

Authorization

AI
Certification Training
HITRUST
HIPAA
NIST
Cyber Defense
CMMC
Compliance
Online Store
Client Reference

NIST SP 800-53 r5
Risk Assessment

ecfirst



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

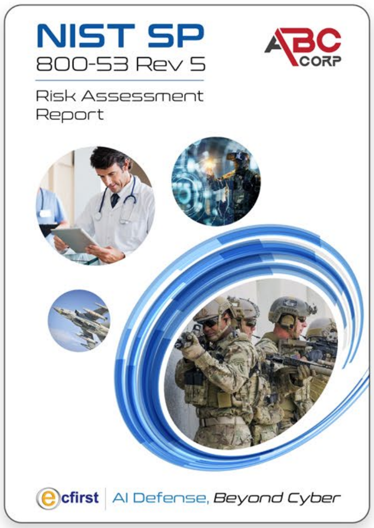
JOINT TASK FORCE

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

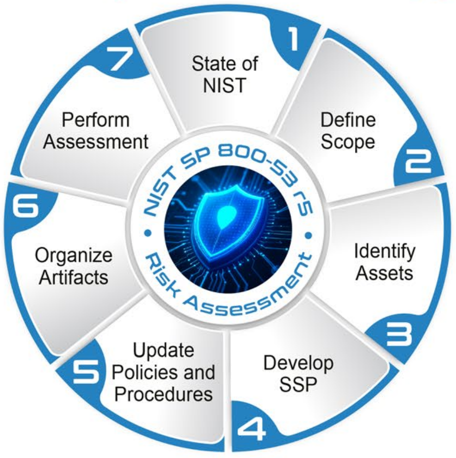


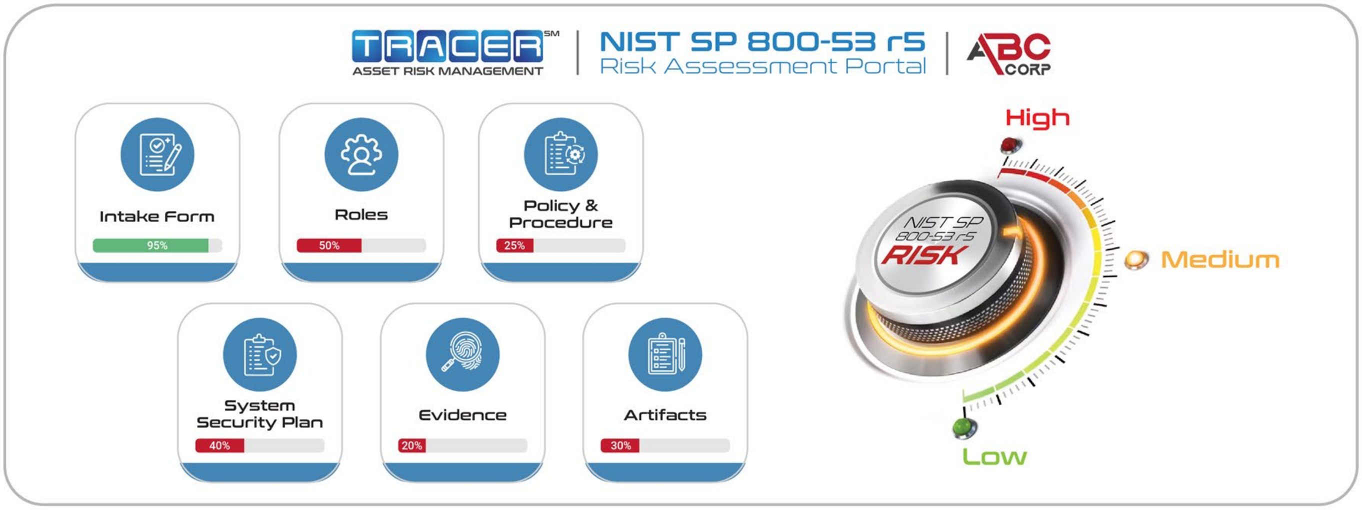
NIST SP
800-53 Rev 5
Risk Assessment Report

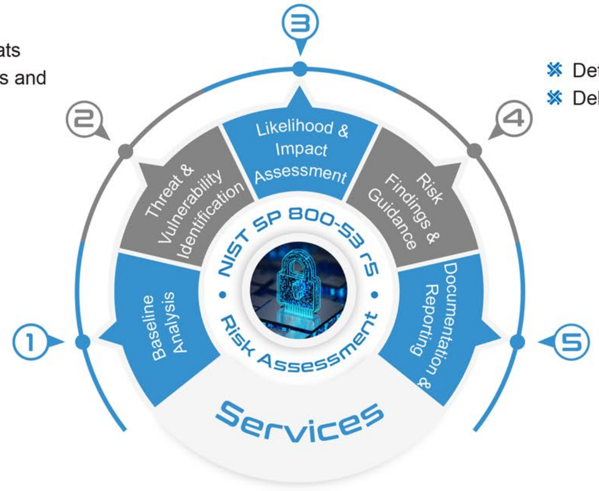
ABC CORP

ecfirst | AI Defense, *Beyond Cyber*

NIST *Signature* Methodology






1
2
3
4
5
Baseline Analysis
Threat & Vulnerability Identification
Likelihood & Impact Assessment
Risk Findings & Guidance
Documentation & Reporting
NIST SP 800-53 r5
Risk Assessment
Services

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

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

③ Evaluate risk severity and align with organizational risk tolerance

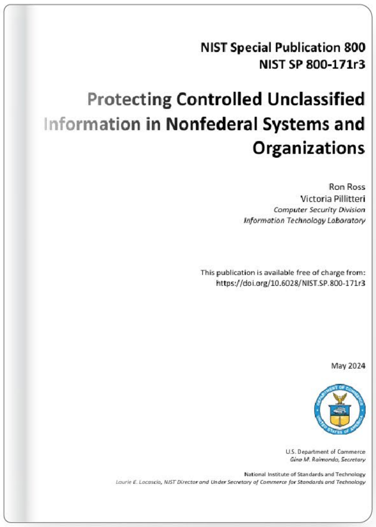
④
- Determine risk levels (low, moderate, high)
- Deliver a prioritized mitigation plan

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

AI
Certification Training
HITRUST
HIPAA
NIST
Cyber Defense
CMMC
Compliance
Online Store
Client Reference

NIST SP 800-171 r3
Assessment

ecfirst


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

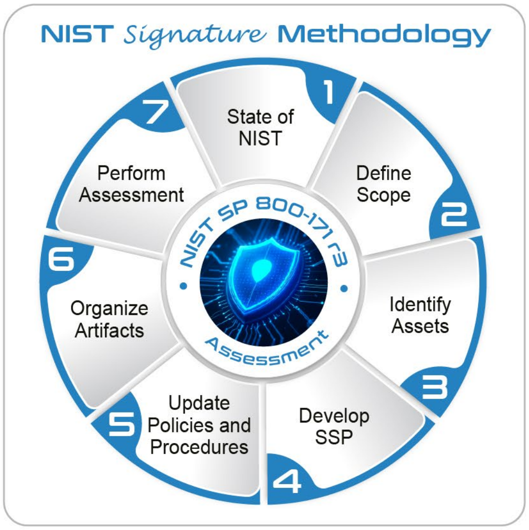
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST SP 800-171
Assessment Report

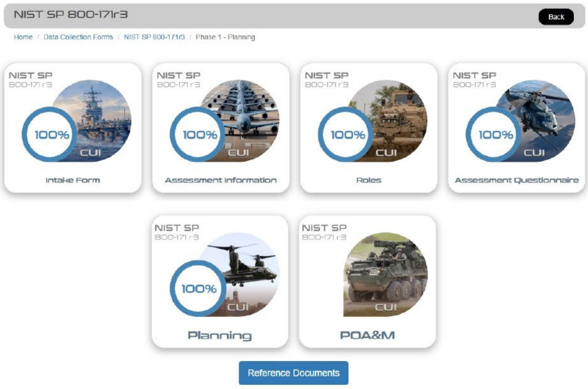
ABC CORP

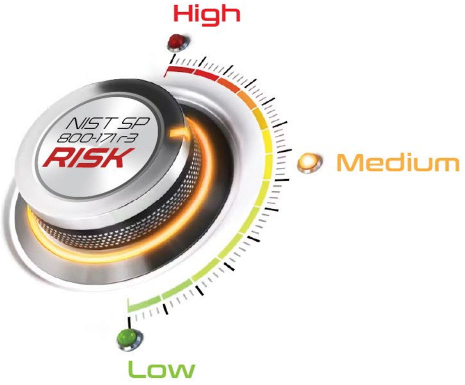
August 13, 2025

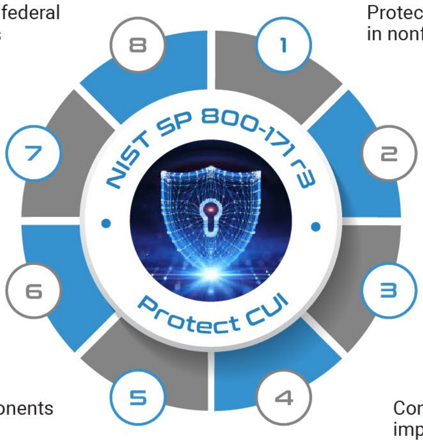
ecfirst | AI Defense, *Beyond Cyber*


NIST *Signature* Methodology

TRACER℠ ASSET RISK MANAGEMENT | NIST SP 800-171 r3 Assessment Portal | ABC CORP

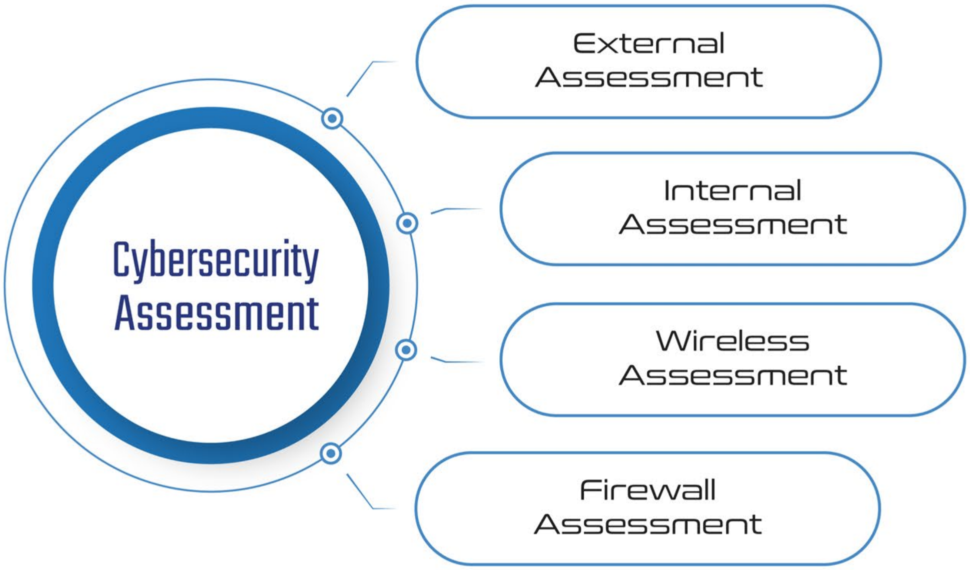

NIST SP 800-171r3





1. Protects CUI confidentiality in nonfederal systems
2. Applies when CUI is present & no specific safeguarding regulation exists
3. Consistent protections: Federal and nonfederal systems treated the same
4. Confidentiality impact ≥ Moderate
5. Applies only to components handling CUI
6. ODPs provide flexibility to tailor security requirements
7. Organized into 17 security families (expanded from 14)
8. Requirements used in federal contracts/agreements

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

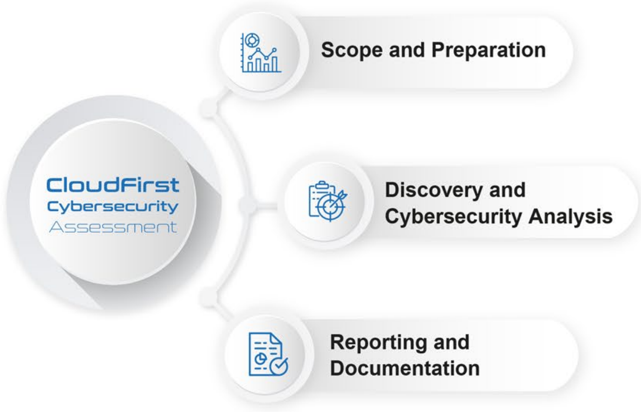
Firewall Assessment

- OS vulnerability analysis
- Security configuration & rule review

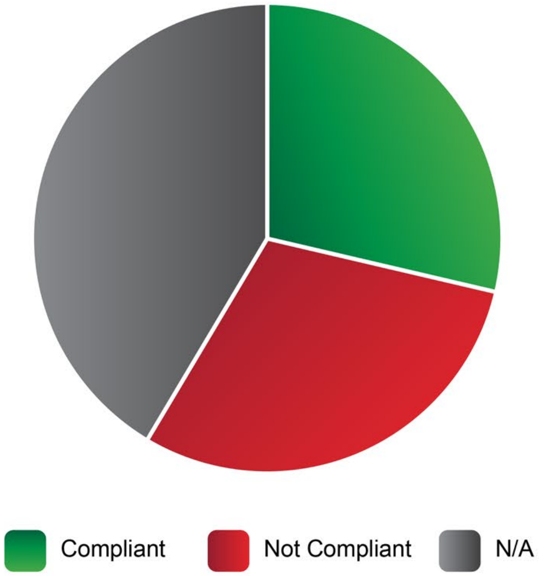
CYBERSECURITY ASSESSMENT SCOPE	TITANIUM	PLATINUM	GOLD	SILVER	BRONZE
External Assessment	✓ Customized	✓	✓	✓	✓
Internal Assessment	✓ Customized	✓	✓	✗	✗
Firewall Assessment	✓ Customized	✓	✓	✓	✗
Wireless Assessment	✓ Customized	✓	✗	✗	✗
Detailed Analysis	✓	✓	✓	✓	✗
Corrective Action Plan (CAP)	✓	✓	✓	✗	✗
Detailed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

CloudFirst Assessment

CloudFirst Assessment

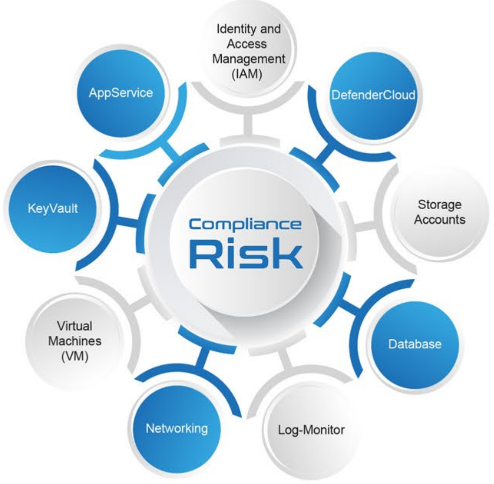

CloudFirst Cybersecurity Assessment
Scope and Preparation
Discovery and Cybersecurity Analysis
Reporting and Documentation

Compliance Status Example



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 Risk Status



CloudFirst Scope

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

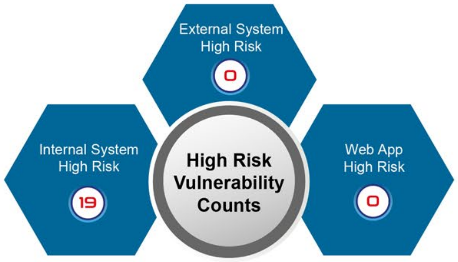
External Assessment

- Up to 32 IP addresses

Internal Assessment

- An Active Directory (AD) domain is tested

Significant Findings

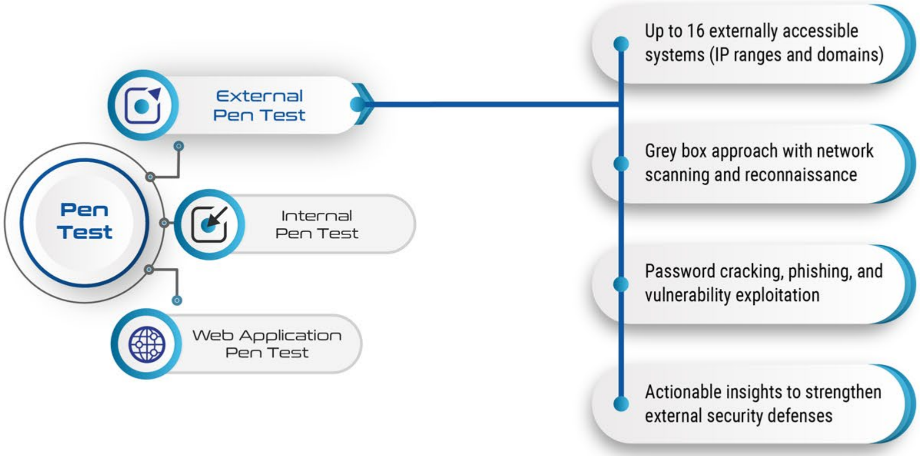

External System High Risk
0
Internal System High Risk
19
High Risk Vulnerability Counts
Web App High Risk
0

AI
Certification Training
HITRUST
HIPAA
NIST
Cyber Defense
CMMC
Compliance
Online Store
Client Reference

Penetration(Pen) Testing

ecfirst

External Pen Test



Pen Test

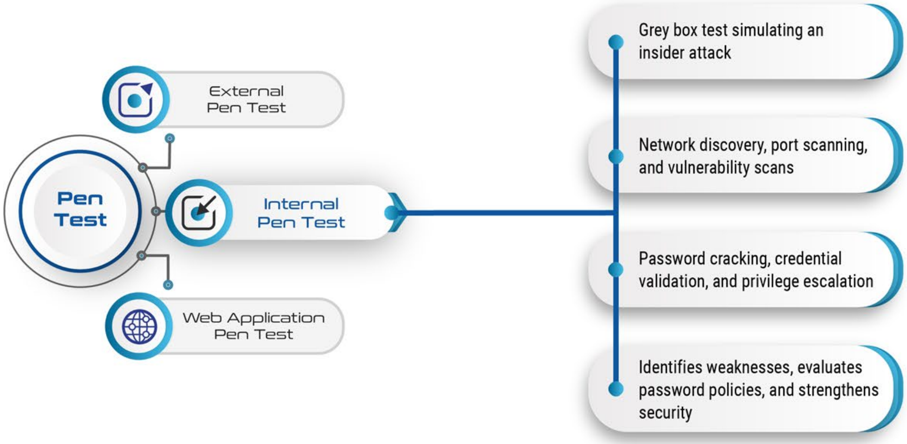
External Pen Test

Internal Pen Test

Web Application Pen Test

- Up to 16 externally accessible systems (IP ranges and domains)
- Grey box approach with network scanning and reconnaissance
- Password cracking, phishing, and vulnerability exploitation
- Actionable insights to strengthen external security defenses

Internal Pen Test



Pen Test

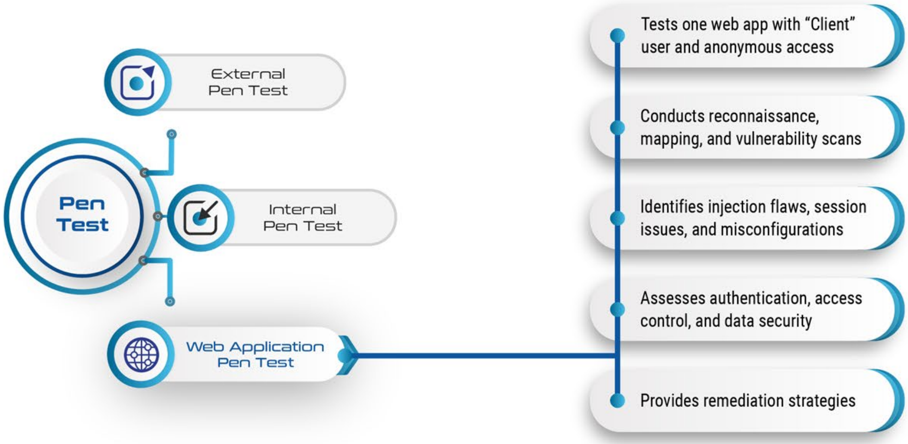
External Pen Test

Internal Pen Test

Web Application Pen Test

- Grey box test simulating an insider attack
- Network discovery, port scanning, and vulnerability scans
- Password cracking, credential validation, and privilege escalation
- Identifies weaknesses, evaluates password policies, and strengthens security

Web Application Pen Test



Pen Test

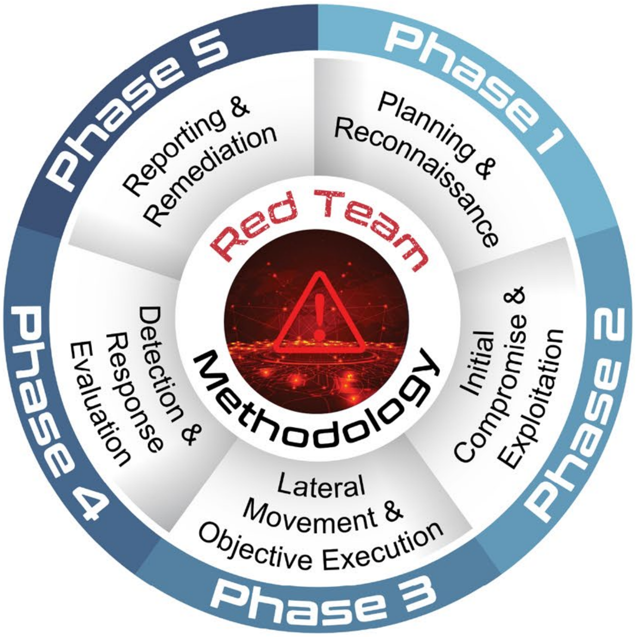
External Pen Test

Internal Pen Test

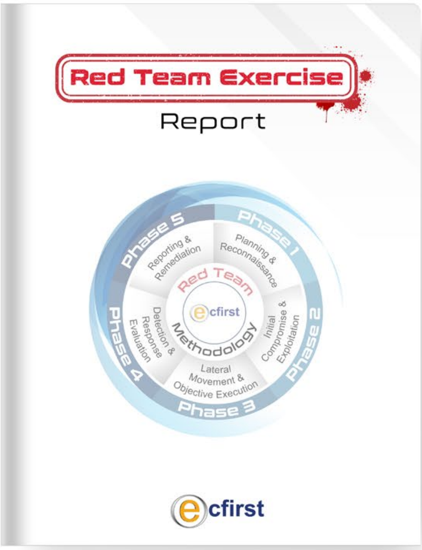
Web Application Pen Test

- Tests one web app with "Client" user and anonymous access
- Conducts reconnaissance, mapping, and vulnerability scans
- Identifies injection flaws, session issues, and misconfigurations
- Assesses authentication, access control, and data security
- Provides remediation strategies

Red Team Exercise

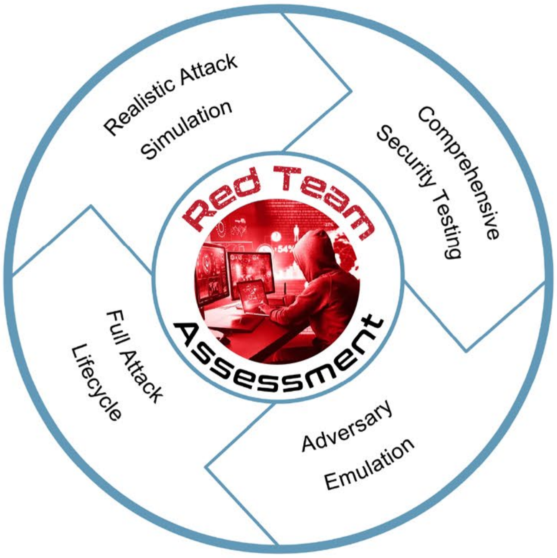


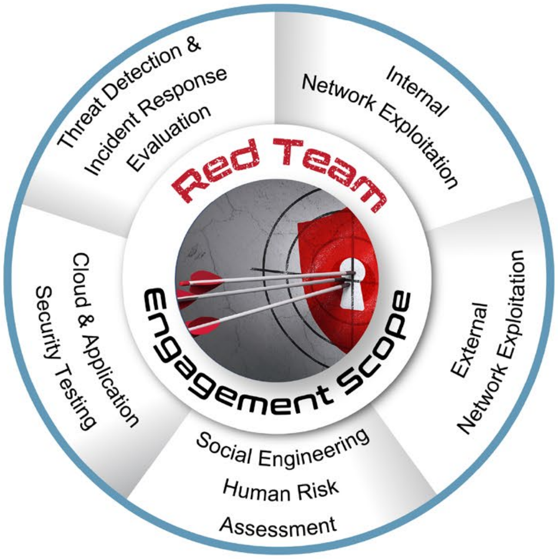
Phase 1
Planning & Reconnaissance
Phase 2
Initial Compromise & Exploitation
Phase 3
Lateral Movement & Objective Execution
Phase 4
Detection & Response Evaluation
Phase 5
Reporting & Remediation
Red Team
Methodology



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.

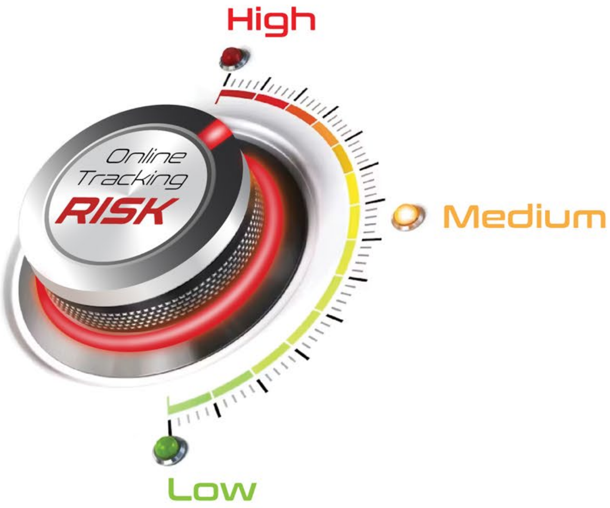




Internal Network Exploitation
External Network Exploitation
Social Engineering Human Risk Assessment
Cloud & Application Security Testing
Threat Detection & Incident Response Evaluation
Red Team
Engagement Scope

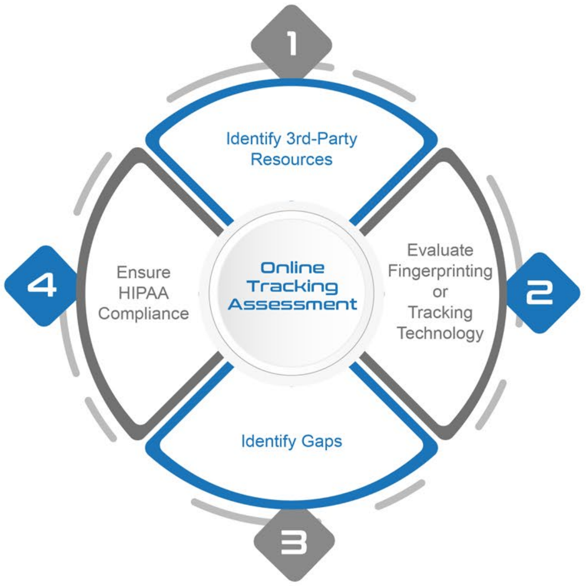
Online Tracking Assessment

ecfirst



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.”


Online
Tracking
Assessment
1
Identify 3rd-Party Resources
2
Evaluate Fingerprinting or Tracking Technology
3
Identify Gaps
4
Ensure HIPAA Compliance

Online Tracking
$9.25 M Settlement
HIPAA Compliance • July 25, 2025

Online Tracking
$875,000 Settlement
HIPAA Compliance • July 16, 2025

Online Tracking
$3 M Settlement
HIPAA Compliance • July 10, 2025

Online Tracking
$1.8 M Settlement
HIPAA Compliance • Dec 6, 2024

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

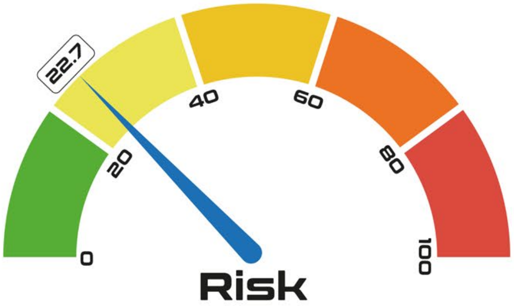
Campaign Start Date	Number of Phishing Victims
Dec 6, 2021	11

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

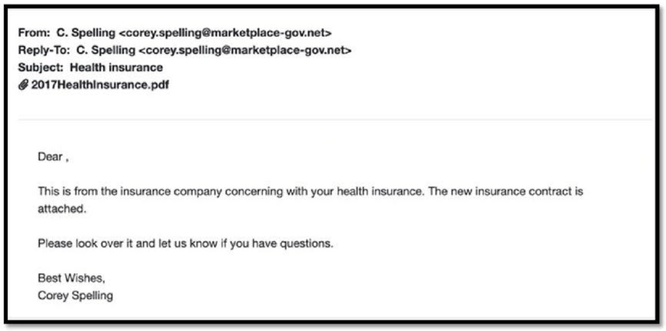
- Based on the number of users that fell victim to the phishing performed, ecfirst estimates the risk of a successful Social Engineering attack against to be a Medium risk.



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

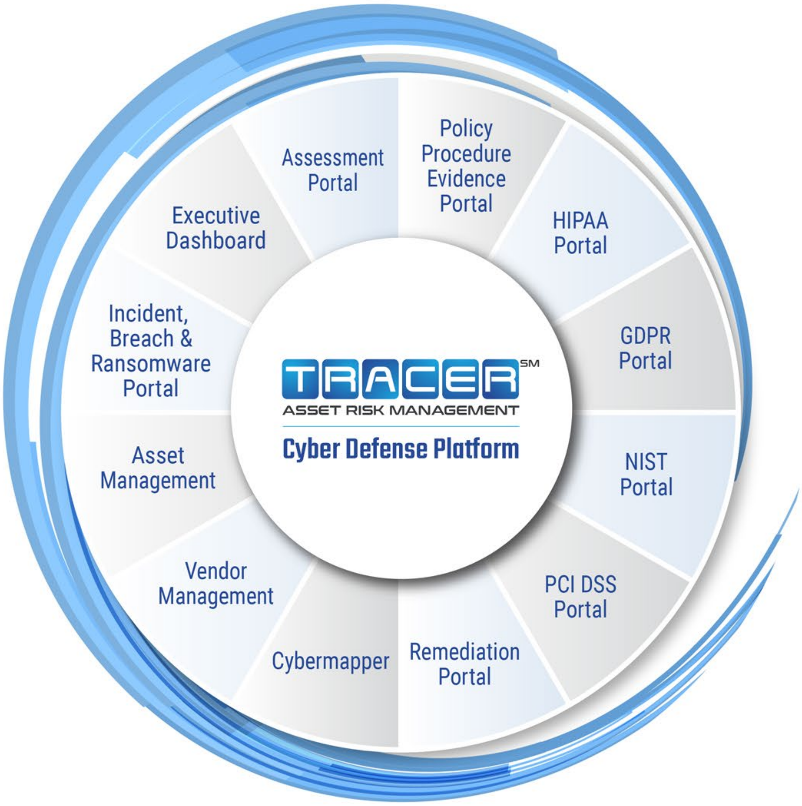
Dear ,

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

AI
Certification Training
HITRUST
HIPAA
NIST
Cyber Defense
CMMC
Compliance
Online Store
Client Reference



Compliance Portals

HIPAA

HIPAA Risk Assessment

Home / Data Collection Forms / HIPAA Risk Assessment

GDPR

Global Data Protection Regulation (GDPR)

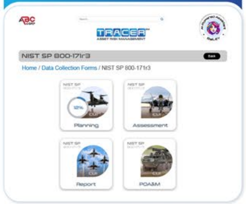
Home / Data Collection Forms / GDPR

NIST SP 800-171r2

NIST SP 800-171r2

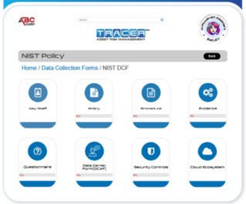
Home / Data Collection Forms / NIST SP 800-171r2

NIST SP 800-171r3


NIST SP 800-171r3

Home / Data Collection Forms / NIST SP 800-171r3

NIST Cybersecurity


NIST Policy

Home / Data Collection Forms / NIST DCF

PCI DSS

PCI DSS

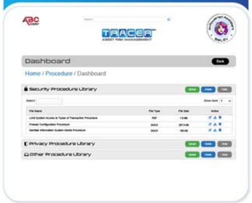
Home / Data Collection Forms / PCI DSS

Policy

Dashboard

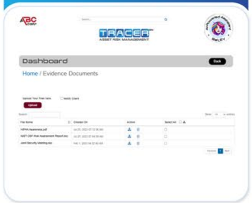
Home / Policy / Dashboard

Procedure


Dashboard

Home / Procedure / Dashboard

Evidence


Dashboard

Home / Evidence Documents

CMMC
Why ecfirst?

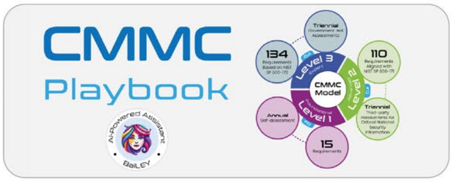
ecfirst

Credentialed Staff

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

CCA
Lead | Higher Level Certifications

AI Powered CMMC Playbook


CMMC
Playbook
AI-Powered Assistant
BaiLEY
Triennial
Government-led Assessments
134
Requirements Based on NIST SP 800-172
Level 3
Expert
CMMC Model
Level 2
Advanced
110
Requirements Aligned with NIST SP 800-171
Triennial
Third-party Assessments for Critical National Security Information
Level 1
Foundational
Annual
Self-assessment
15
Requirements

Surgically Defined CMMC Assessment Process

CYBER AB
CMMC CERTIFICATION
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 ecfirst CCP Academy! I appreciated my ecfirst experience.”

CAICO
CMMC CERTIFIED PROFESSIONAL
CCP

CAICO
CMMC CERTIFIED ASSESSOR
CCA

CCA Reference

> “The ecfirst 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
CMMC CERTIFICATION
REGISTERED PRACTITIONER ORGANIZATION
RPO

CAICO
APP

DoD CMMC Certification Training Content
Approved and Authorized

CAICO
ATP

DoD CMMC Certification Training Provider
Approved and Authorized

CMMC CCP

Public | Virtual | On-Site

CAICO CMMC CERTIFIED PROFESSIONAL CCP | ecfirst

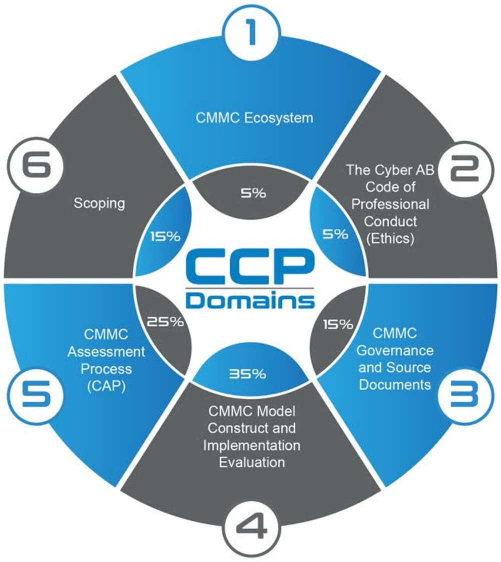
Summary

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.

Why ecfirst for CCP Training?

- Our auditors are our trainers
- ecfirst is all in for CMMC (RPO, APP, ATP & C3PAO)
- ecfirst's Academy Portal gives students access to all training materials, resource documents, study guides, and quizzes to solidify learning in one location
- 25 years of privacy and security compliance training experience
- 24 years of compliance audit/assessment experience (HIPAA, PCI DSS, HITRUST, GDPR, NIST SP 800-171, multiple state regulations)
- One of the first organizations to take the training to market

CMMC Certified Professional (CCP)


1
CMMC Ecosystem
5%
2
The Cyber AB Code of Professional Conduct (Ethics)
5%
3
CMMC Governance and Source Documents
15%
4
CMMC Model Construct and Implementation Evaluation
35%
5
CMMC Assessment Process (CAP)
25%
6
Scoping
15%
CCP Domains

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

Exam Prerequisites

- College degree in a cyber or information technical field or 2+ years of related experience or education, or 2+ years of equivalent experience (including military) in a cyber, information technology, or assessment field
- Suggested CompTIA A+ or equivalent knowledge/experience
- Complete CCP Class offered by a Approved Training Provider (ATP)
- Pass DoD CUI Awareness Training no earlier than three (3) months prior to the exam
  - https://securityhub.usalearning.gov/index.html

CCP Exam Specifications

- Number of Questions: 170
- Types of Questions: Multiple Choice
- Length: 3.5 Hours
- Passing Score: 500 Points
- This is not an open book exam

Domain Exam Weight

#	Domain	Exam Weight	CCP Program	Hours 36
1	CCP Pre Program Prep			Hours 2
2	CMMC Ecosystem **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			

CMMC CCA

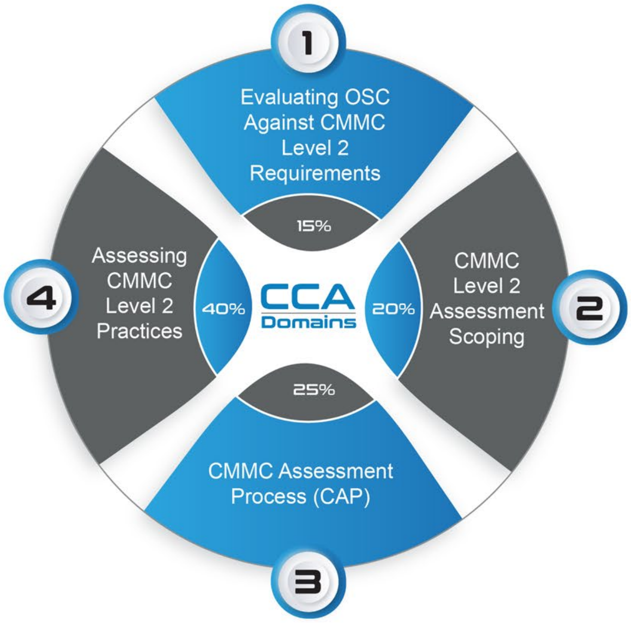
Public | Virtual | On-Site

CAICO CMMC CERTIFIED ASSESSOR CCA | ecfirst

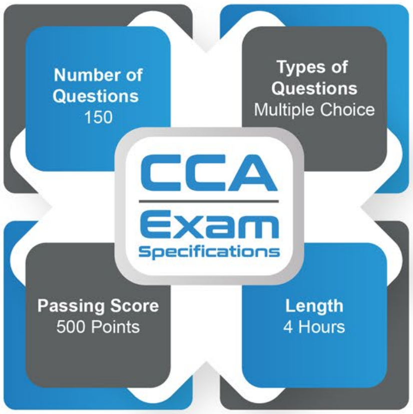
Summary

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)


1
Evaluating OSC Against CMMC Level 2 Requirements
15%
2
CMMC Level 2 Assessment Scoping
20%
3
CMMC Assessment Process (CAP)
25%
4
Assessing CMMC Level 2 Practices
40%
CCA Domains

CCA Exam Specifications



Number of Questions	150
Types of Questions	Multiple Choice
Passing Score	500 Points
Length	4 Hours

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		**Domain 0, 1, 2** Tuesday, Day 1 8:30 am - 4:30 pm Group Exercises: 8 | 40 Minutes Offline Prep: 2 Hours	Hours 10
	Evaluating OSC Against CMMC Level 2 Requirements Blueprint Domain 1	15%		
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

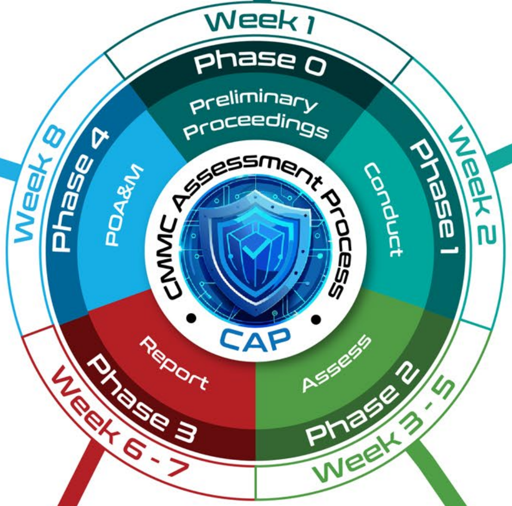
Intended Audience

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

Why ecfirst for CCA Training?

- Our auditors are our trainers
- ecfirst is all in for CMMC (RPO, APP, ATP & C3PAO)
- ecfirst's Academy Portal gives students access to all training materials, resource documents, study guides, and quizzes to solidify learning in one location
- 25 years of privacy and security compliance training experience
- 25 years of compliance audit/assessment experience (HIPAA, PCI DSS, HITRUST, GDPR, NIST SP 800-171, multiple state regulations)
- One of the first organizations to take the training to market

CMMC Assessment



Week 1

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

Week 2

- 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

Weeks 3 - 5

- 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

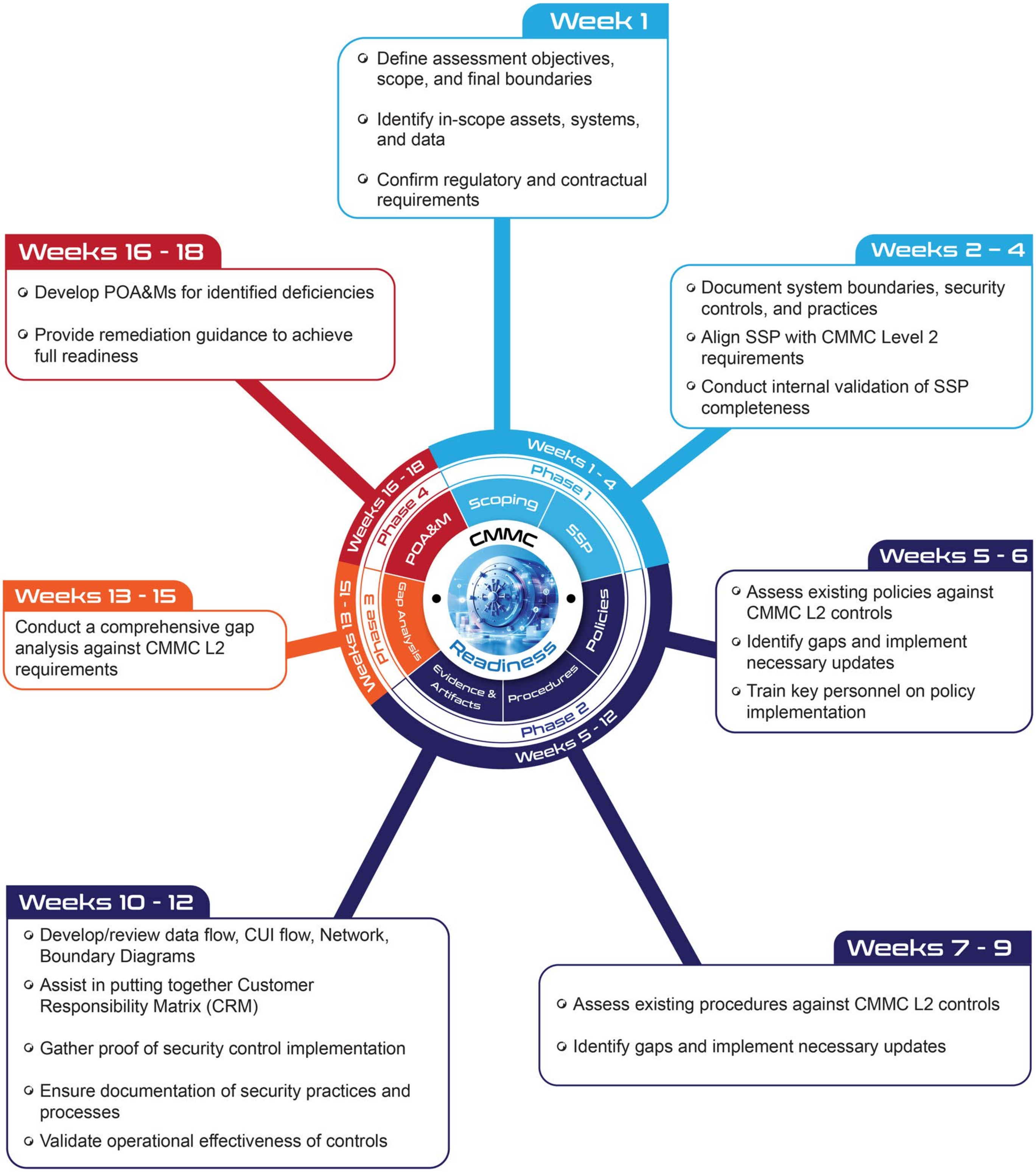
Weeks 6 - 7

- 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)

Week 8

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

CMMC Readiness
Mock Assessment



Week 1

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

Weeks 2 – 4

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

Weeks 5 - 6

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

Weeks 7 - 9

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

Weeks 10 - 12

- 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

Weeks 13 - 15

Conduct a comprehensive gap analysis against CMMC L2 requirements

Weeks 16 - 18

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

AI
Certification Training
HITRUST
HIPAA
NIST
Cyber Defense
CMMC
Compliance
Online Store
Client Reference

Ransomware Readiness BIA | DRP

NISTIR 8374

Ransomware Risk Management:
A Cybersecurity Framework Profile

William C. Barker
Dakota Consulting
Silver Spring, MD

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

William Fisher
Applied Cybersecurity Division
Information Technology Laboratory

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

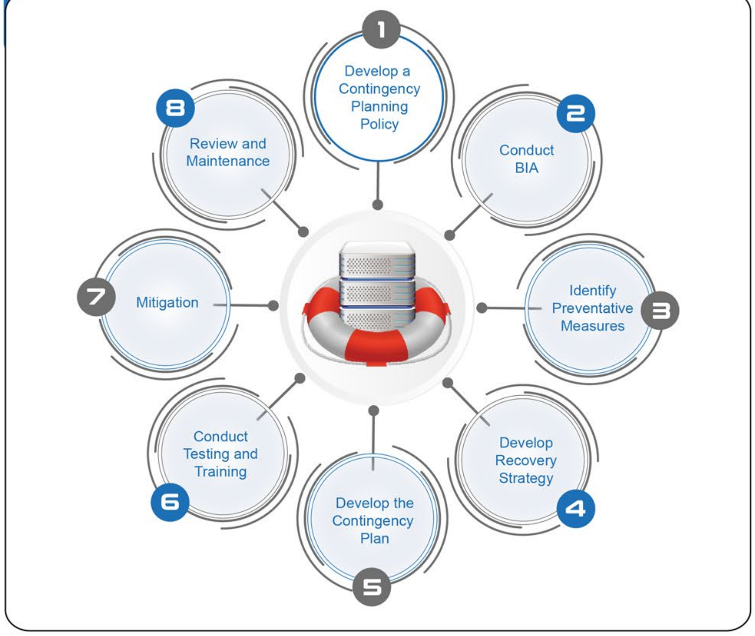
This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8374

February 2022

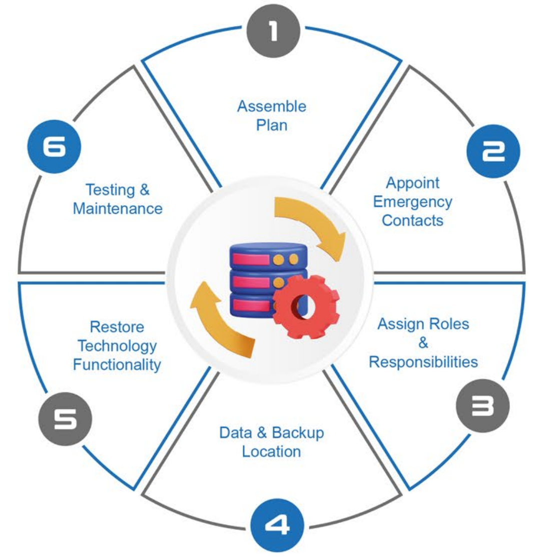
U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

Business Impact Analysis (BIA)


1
Develop a Contingency Planning Policy
2
Conduct BIA
3
Identify Preventative Measures
4
Develop Recovery Strategy
5
Develop the Contingency Plan
6
Conduct Testing and Training
7
Mitigation
8
Review and Maintenance

IT Disaster Recovery Plan

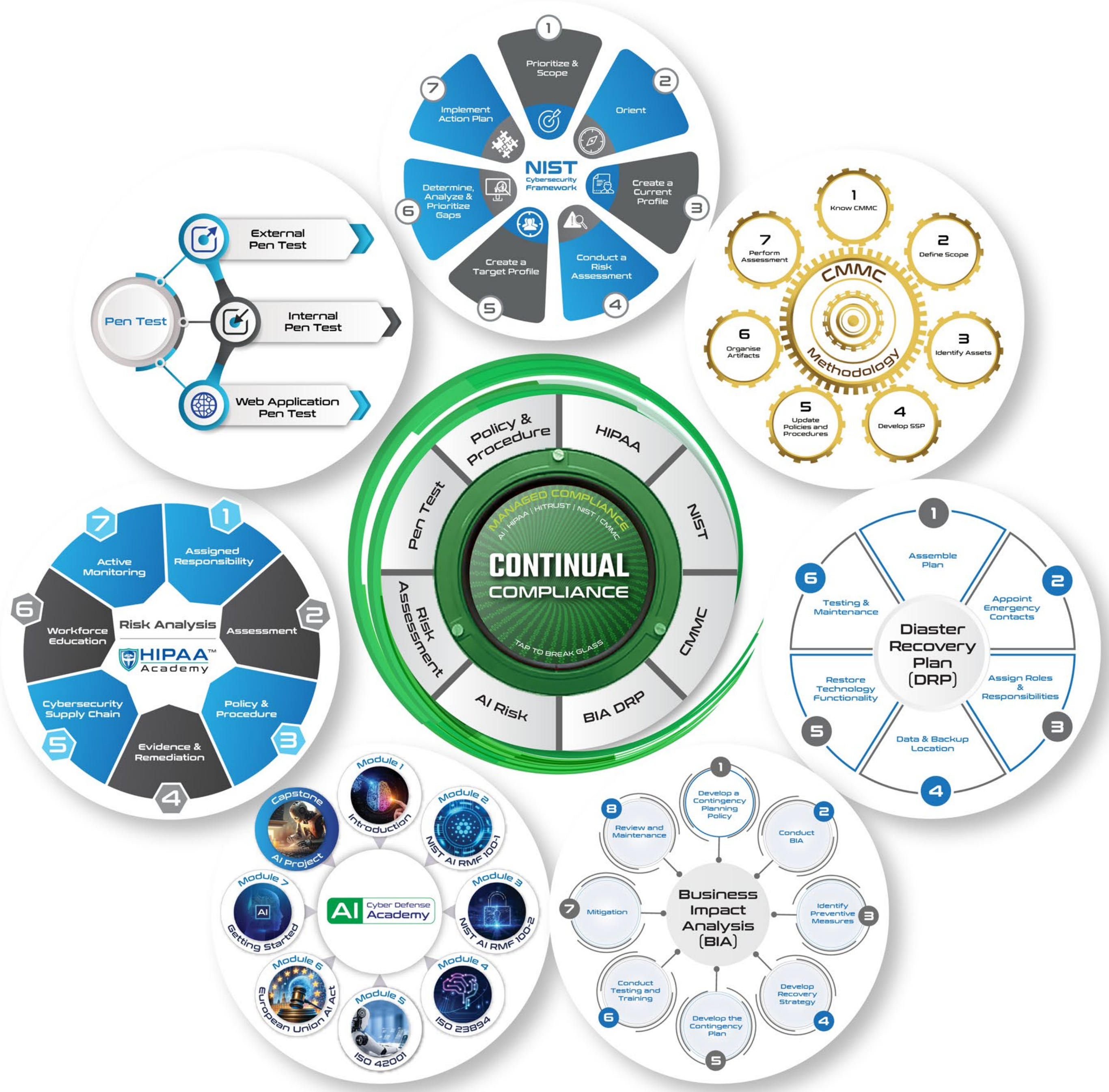

1
Assemble Plan
2
Appoint Emergency Contacts
3
Assign Roles & Responsibilities
4
Data & Backup Location
5
Restore Technology Functionality
6
Testing & Maintenance

Ransomware Resilience

- Educate Employees
- Mitigate System Vulnerabilities
- Detect and Stop Ransomware Attacks
- Prevent Ransomware Spread
- Facilitate Recovery from Ransomware

MANAGED COMPLIANCE
Fixed Price | Flexible | Scalable

ecfirst



HIPAA HITRUST NIST CMMC

ON DEMAND CONSULTING

ecfirst

Consulting (ODC)

Fixed-rate

Expert Advisors

No Long-term Commitment

Short Term Consulting

Pen Test

Cybersecurity Assessment

Virtual ISO

InfoSec Staffing

Policy Development

Remediation Services

Procedure Development

Business Impact Analysis

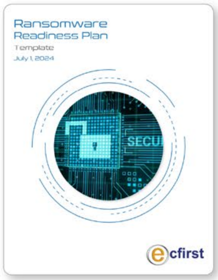
Compliance Solutions

IT Disaster Recovery Plan

Social Engineering

Business Continuity

Cybersecurity Plans


Ransomware Readiness Plan
Template
July 1, 2024
ecfirst

Enterprise
Cybersecurity Plan
Template
July 1, 2024
ecfirst

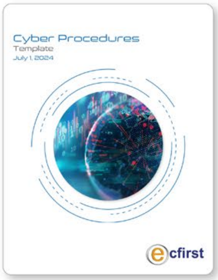
Contingency Plan
Template
July 1, 2024
ecfirst

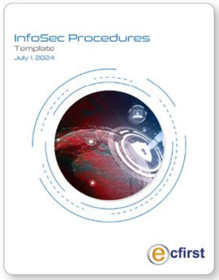
Cybersecurity Incident Management Plan
Template
July 1, 2024
ecfirst

IT Disaster Recovery Plan
Template
July 1, 2024
ecfirst

Policies and Procedures

Security Policy
Template
July 1, 2024
ecfirst


Cyber Procedures
Template
July 1, 2024
ecfirst


InfoSec Procedures
Template
July 1, 2024
ecfirst

Privacy Policy
Template
July 1, 2024
ecfirst

AI
Certification Training
HITRUST
HIPAA
NIST
Cyber Defense
CMMC
Compliance
Online Store
Client Reference

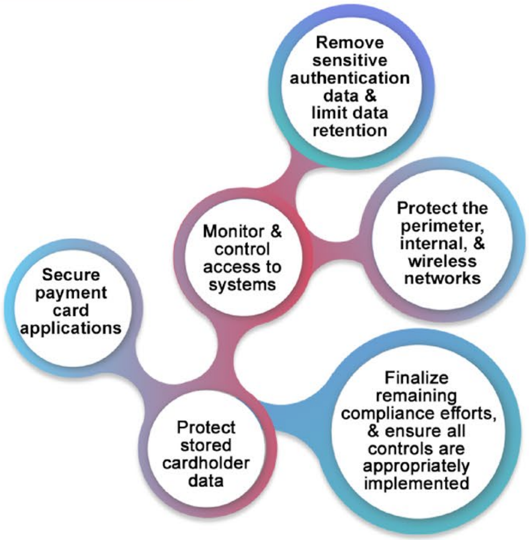
PCI DSS

Pre-Assessment

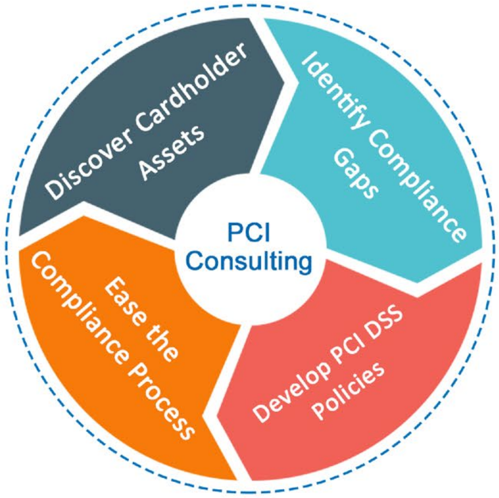
PCI DSS Readiness Assessment

- 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

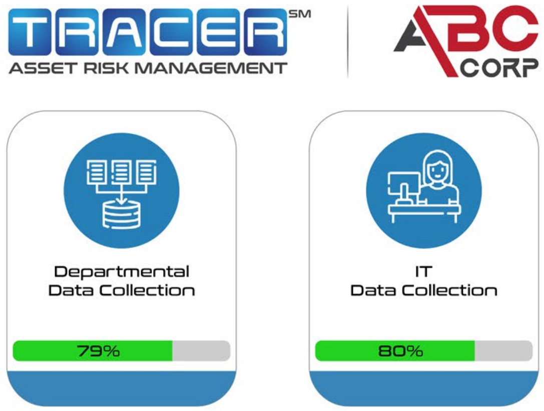
PCI Dss Goals


Remove sensitive authentication data & limit data retention
Protect the perimeter, internal, & wireless networks
Monitor & control access to systems
Secure payment card applications
Protect stored cardholder data
Finalize remaining compliance efforts, & ensure all controls are appropriately implemented

PCI Consulting



PCI DSS Portal



AI
Certification Training
HITRUST
HIPAA
NIST
Cyber Defense
CMMC
Compliance
Online Store
Client Reference

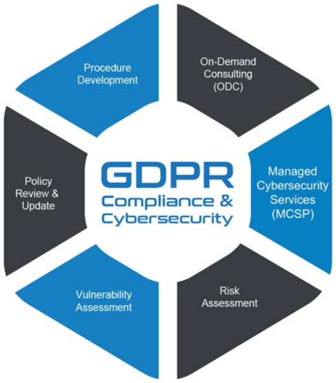
GDPR Compliance
Pre-Assessment

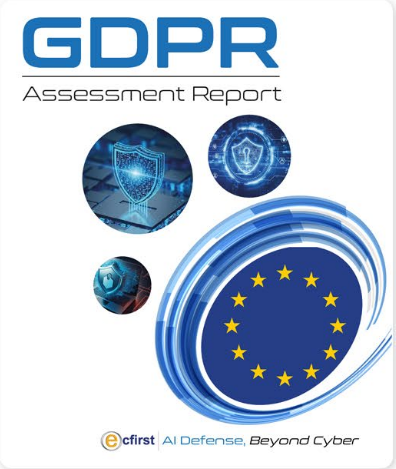
ecfirst

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

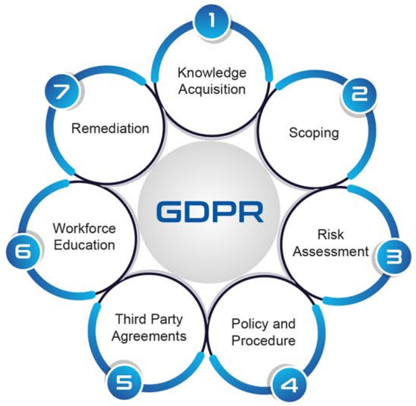

GDPR Compliance & Cybersecurity
Procedure Development
On-Demand Consulting (ODC)
Managed Cybersecurity Services (MCSP)
Risk Assessment
Vulnerability Assessment
Policy Review & Update


GDPR
Assessment Report
ecfirst | AI Defense, Beyond Cyber

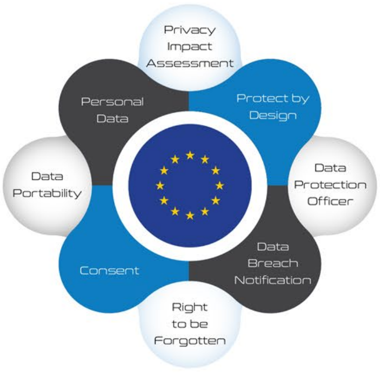
GDPR: Who, What, Why?

- 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

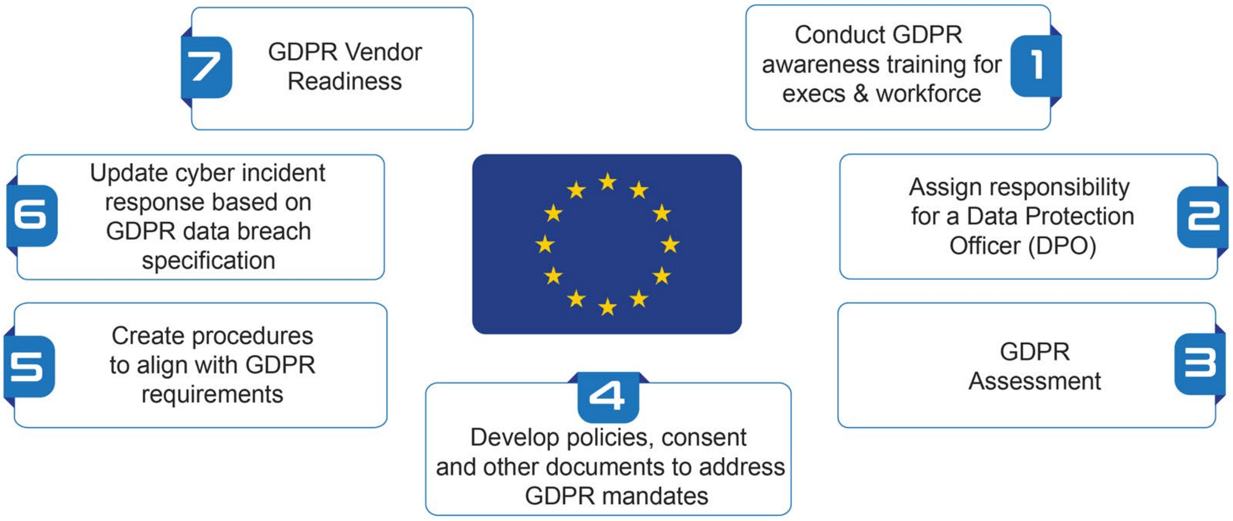
GDPR *Signature* Methodology



Purpose & Scope



Establish a Credible GDPR Program


1 Conduct GDPR awareness training for execs & workforce

2 Assign responsibility for a Data Protection Officer (DPO)

3 GDPR Assessment

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

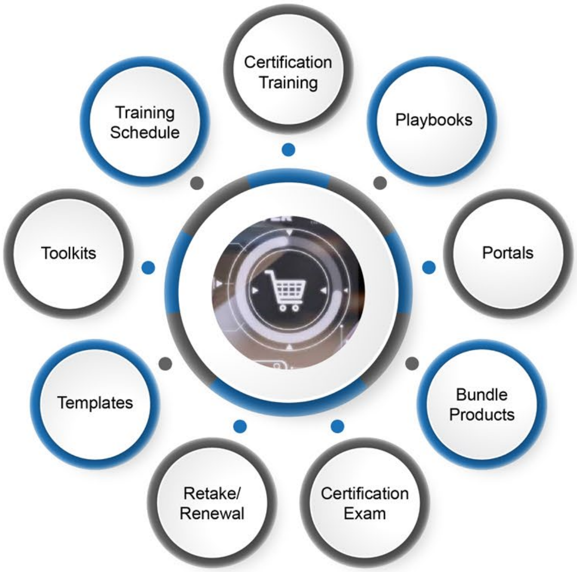
5 Create procedures to align with GDPR requirements

6 Update cyber incident response based on GDPR data breach specification

7 GDPR Vendor Readiness

Online Store

ecfirst online



Certification Training

Playbooks

Portals

Bundle Products

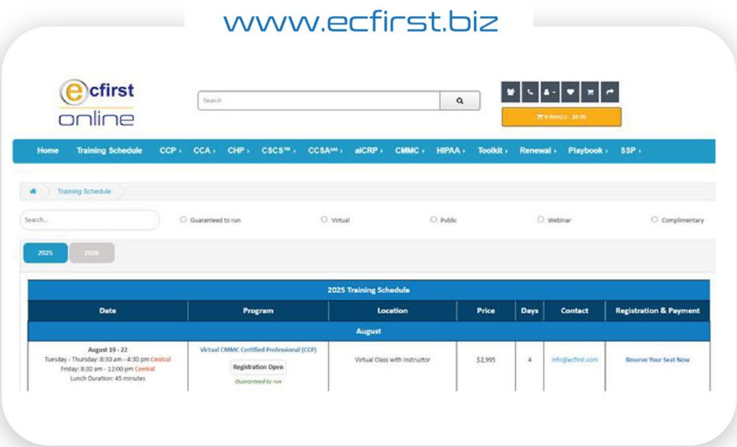
Certification Exam

Retake/ Renewal

Templates

Toolkits

Training Schedule



www.ecfirst.biz

ecfirst online

Search

○ Guaranteed to run ○ Virtual ○ Public ○ Webinar ○ Complimentary

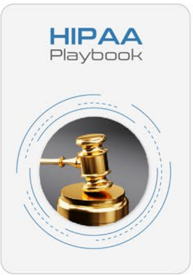
2025 2026

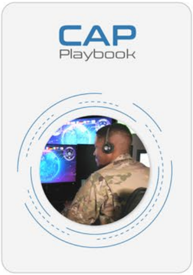
2025 Training Schedule

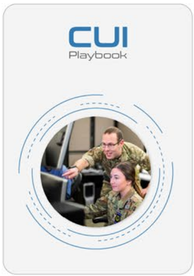
Date	Program	Location	Price	Days	Contact	Registration & Payment
August						
August 19 - 22 Tuesday - Thursday: 8:30 am - 4:30 pm Central Friday: 8:30 am - 12:00 pm Central Lunch Duration: 45 minutes	Virtual CMMC Certified Professional (CCP) Registration Open Guaranteed to run	Virtual Class with Instructor	$2,995	4	info@ecfirst.com	Reserve Your Seat Now

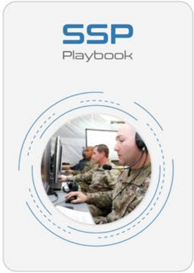
Training

Playbooks









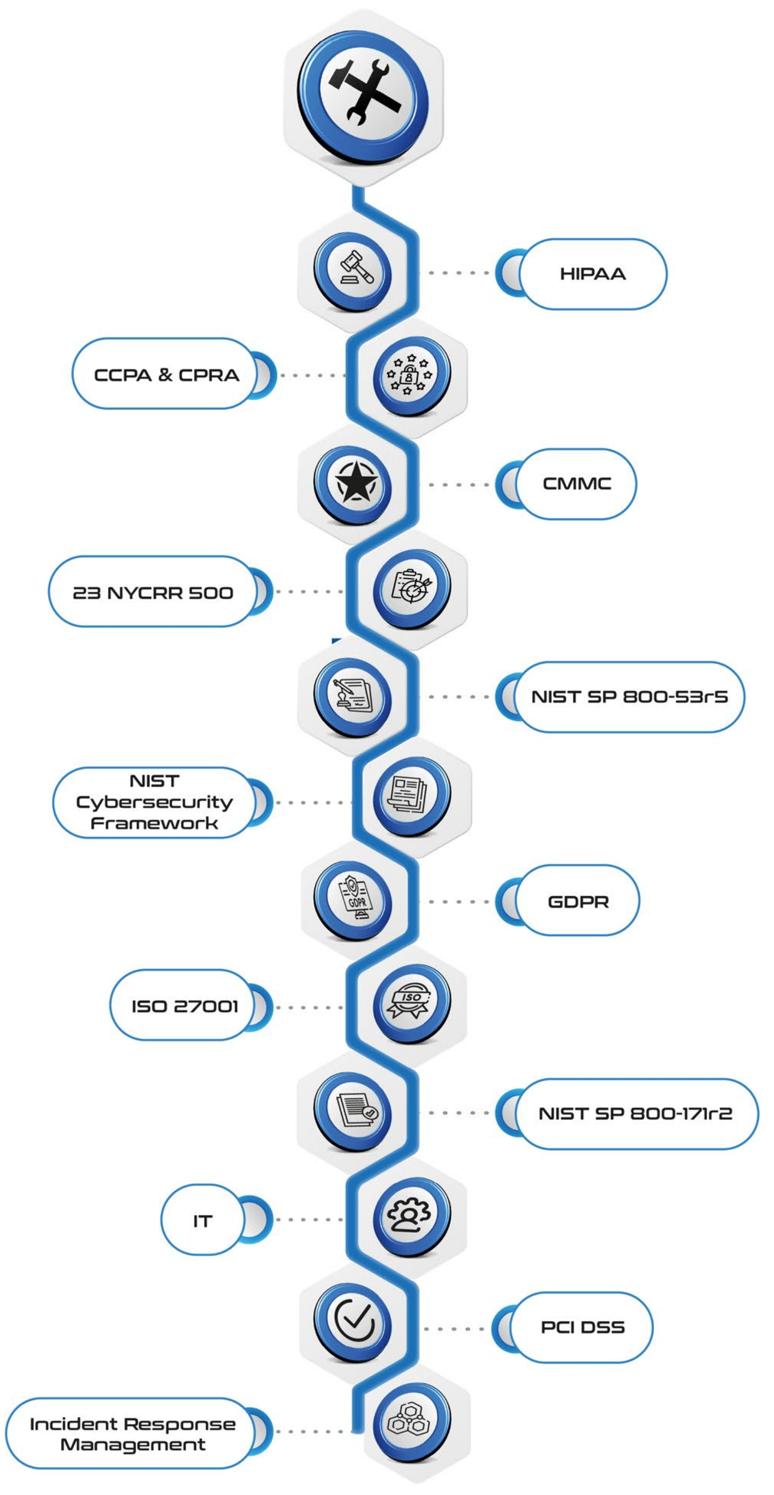
Templates

CMMC HIPAA GDPR NIST SSP

Compliance
and Cyber Toolkit

ecfirst online

Toolkit Packages



HIPAA

CCPA & CPRA

CMMC

23 NYCRR 500

NIST SP 800-53r5

NIST Cybersecurity Framework

GDPR

ISO 27001

NIST SP 800-171r2

IT

PCI DSS

Incident Response Management

Components

Policy

Procedure

Plan

Checklist

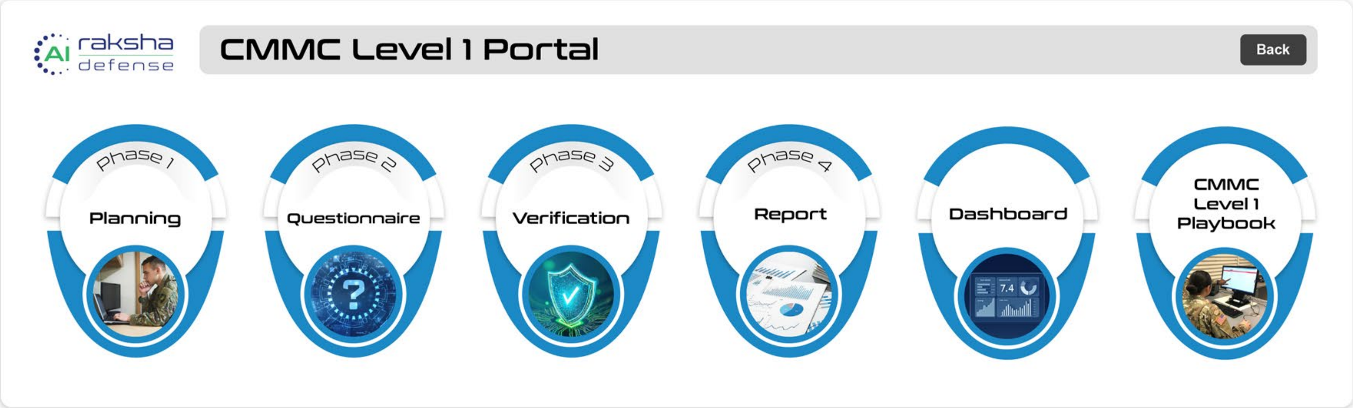
Infographics

Mappings

Quick Reference Cards

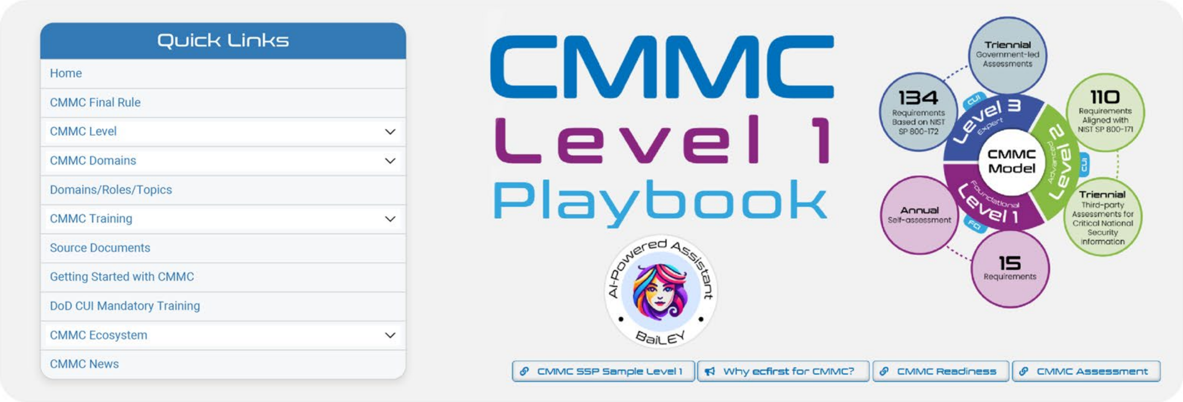
CMMC
Level 1 Toolkit

FAR clause 52.204-21
FCI
6
Domains
15
Requirements
59
Assessment Objectives
Policy Template
Level 1
SSP Template
Level 1
Procedure Template
Level 1
CMMC
Policy Template
CMMC System Security Plan
Level 1
ABC CORP



CMMC Level 1 Portal

- Planning
- Questionnaire
- Verification
- Report
- Dashboard
- CMMC Level 1 Playbook


Triennial Government-led Assessments
134 Requirements Based on NIST SP 800-172
110 Requirements Aligned with NIST SP 800-171
Level 3 Expert
Level 2 Advanced
Level 1 Foundational
CUI
FCI
CMMC Model
Annual Self-assessment
Triennial Third-party Assessments for Critical National Security Information
15 Requirements
AI-Powered Assistant
BaiLEY

Quick Links

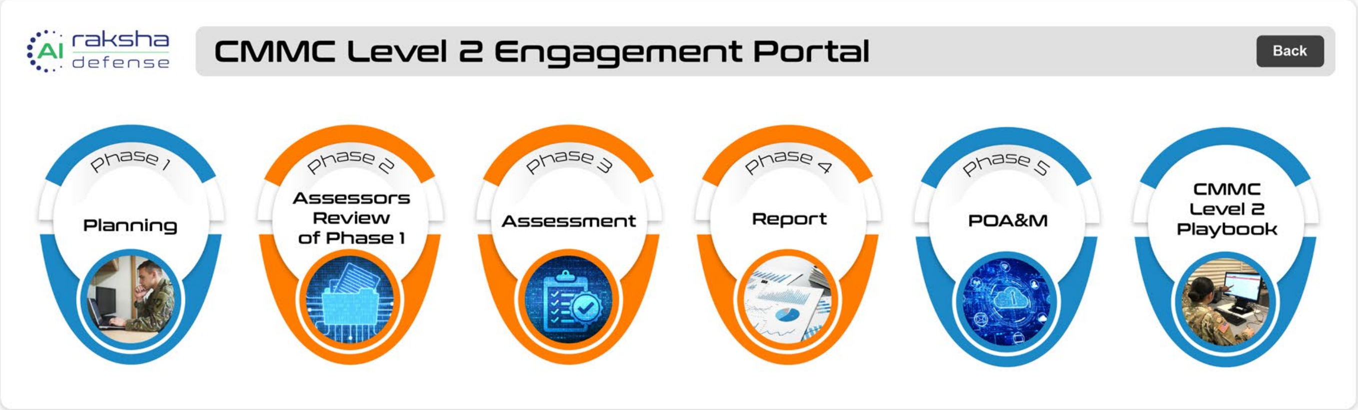
- Home
- CMMC Final Rule
- CMMC Level
- CMMC Domains
- Domains/Roles/Topics
- CMMC Training
- Source Documents
- Getting Started with CMMC
- DoD CUI Mandatory Training
- CMMC Ecosystem
- CMMC News

CMMC Level 1 Playbook

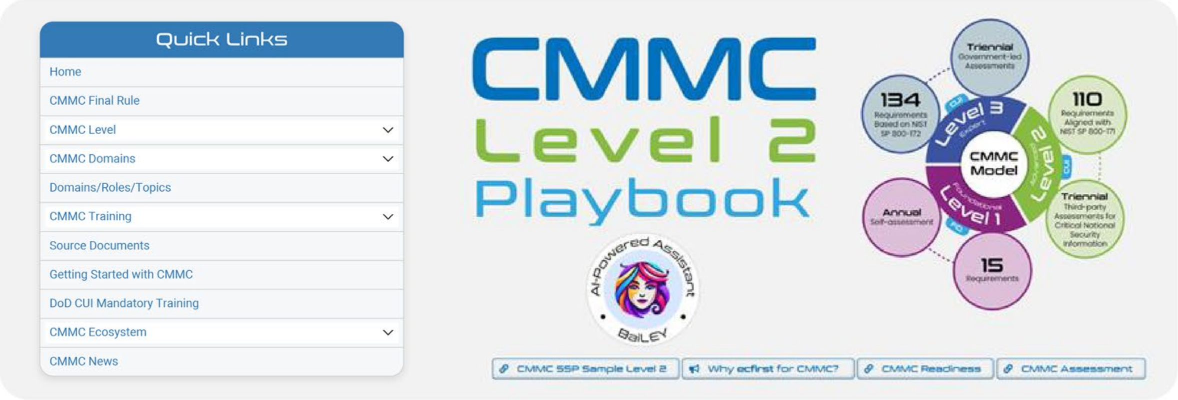
CMMC SSP Sample Level 1 | Why ecfirst for CMMC? | CMMC Readiness | CMMC Assessment

CMMC
Level 2 Toolkit

Policy Template
CMMC
Policy Template
ABC CORP
ecfirst
Level 2
SSP Template
CMMC System Security Plan
Level 2
ABC CORP
ecfirst
Level 2
Procedure Template
CMMC
Cybersecurity Procedure
ABC CORP
ecfirst
Level 2
NIST SP 800-171 r2
CUI
14
Domains
110
Requirements
320
Assessment Objectives



CMMC Level 2 Engagement Portal



Quick Links

- Home
- CMMC Final Rule
- CMMC Level
- CMMC Domains
- Domains/Roles/Topics
- CMMC Training
- Source Documents
- Getting Started with CMMC
- DoD CUI Mandatory Training
- CMMC Ecosystem
- CMMC News

AI
Certification Training
HITRUST
HIPAA
NIST
Cyber Defense
CMMC
Compliance
Online Store
Client Reference

HIPAA
Toolkit Package

ecfirst online

Policy Template

Procedure Template

Plan Template

Checklists

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

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

BAA Templates

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

Mappings

- HIPAA → ISO 27001
- HIPAA → NIST Cybersecurity Framework

- 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

Infographics

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

- 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

AI
Certification Training
HITRUST
HIPAA
NIST
Cyber Defense
CMMC
Compliance
Online Store
Client Reference

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

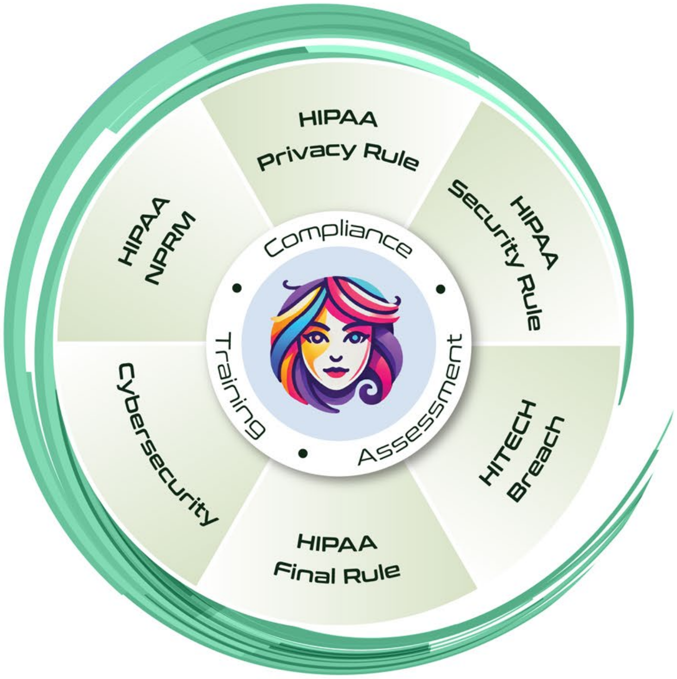
- Cybersecurity Controls
- Cybersecurity
- NIST Cybersecurity

Mappings

- NIST Cybersecurity Framework → CMMC
- NIST Cybersecurity Framework → HIPAA
- NIST Cybersecurity Framework → ISO 27001

HIPAA Playbook

HIPAA™ Academy | ecfirst online



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

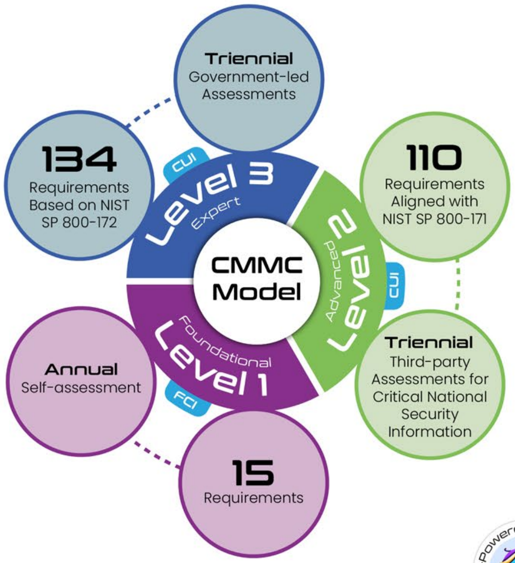
CMMC Playbook

ecfirst online

AI
Certification Training
HITRUST
HIPAA
NIST
Cyber Defense
CMMC
Compliance
Online Store
Client Reference

Quick Links

- Home
- CMMC Final Rule
- CMMC Level
- CMMC Domains
- Domains/Roles/Topics
- CMMC Training
- Source Documents
- Getting Started with CMMC
- DoD CUI Mandatory Training
- CMMC Ecosystem
- CMMC News

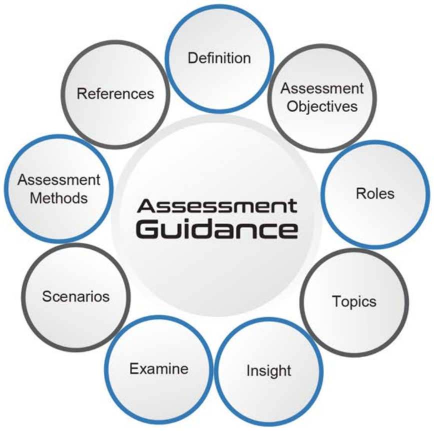

CMMC Model
Level 3 Expert
CUI
Level 2 Advanced
CUI
Level 1 Foundational
FCI
Triennial Government-led Assessments
134 Requirements Based on NIST SP 800-172
110 Requirements Aligned with NIST SP 800-171
Triennial Third-party Assessments for Critical National Security Information
Annual Self-assessment
15 Requirements

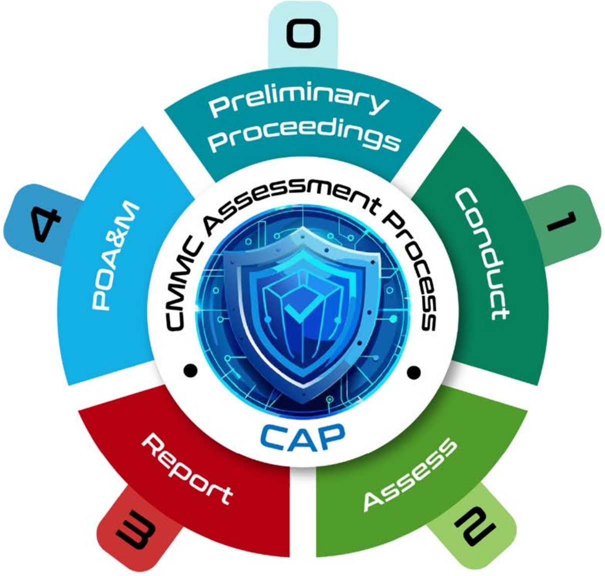
Domains

Level 1 Level 2 Level 3

CMMC Domain 1 Access Control (AC)
CMMC Domain 2 Awareness & Training (AT)
CMMC Domain 3 Audit & Accountability (AU)
CMMC Domain 4 Configuration Management (CM)
CMMC Domain 5 Identification & Authentication (IA)
CMMC Domain 6 Incident Response (IR)
CMMC Domain 7 Maintenance (MA)
CMMC Domain 8 Media Protection (MP)
CMMC Domain 9 Personnel Security (PS)
CMMC Domain 10 Physical Protection (PE)
CMMC Domain 11 Risk Assessment (RA)
CMMC Domain 12 Security Assessment (CA)
CMMC Domain 13 System & Communications Protection (SC)
CMMC Domain 14 System & Information Integrity (SI)

Explore





Quick Links

- Home
- ecfirst CAP Doctrine
- CMMC Assessment Readiness
- CMMC Training
- Assessment Phases
- Phase 0: Primary 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

AI-Powered Assistant
BaiLEY

ecfirst CAP Doctrine

Flowchart

Playbook

Pre-Assessment Review Documents

C3PAO Outbrief Daily Assessment Summary

C3PAO CAP Checklist

Assessment Process

CMMC 2.0 Practices

CMMC 2.0 Requirements

Assessor Domain Grouping

CAP 2.0 Infographic

CMMC Assessment Readiness

CMMC UnReadiness

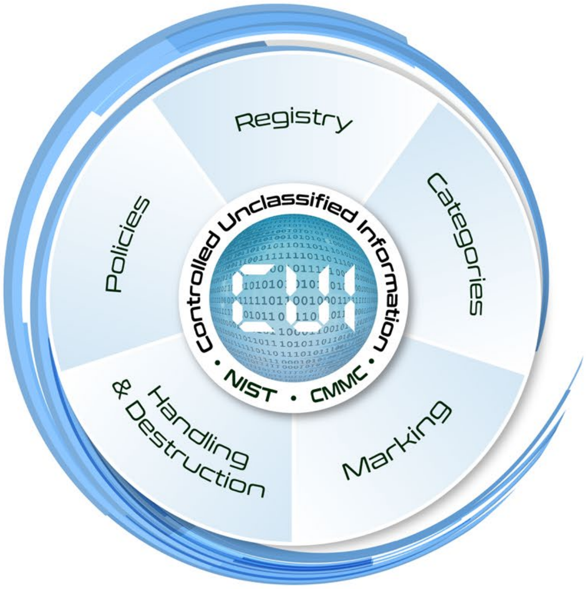
SSP UnReadiness

SSP Sample

CMMC 10-Day Eval Insight

Quick Links

- Home
- DoD CUI References
  - Introduction
  - CUI Category
  - CUI Registry
  - CUI Marking
  - CUI Policy
  - FAQ
- NARA CUI References
  - Introduction
  - CUI Category
  - CUI Registry
  - CUI Marking
  - CUI Handling and Destruction
  - CUI Policy
  - CUI EO 13556
  - 32 CFR Part 2002
  - CUI Glossary
  - CUI Reports
  - CUI Resources
  - FAQ
- Training



DoD CUI References

NARA CUI References

Training Resources

CAICO
CMMC CERTIFIED PROFESSIONAL
CCP

CAICO
CMMC CERTIFIED ASSESSOR
CCA

AI Risk Management Playbook

ecfirst

Quick Links

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

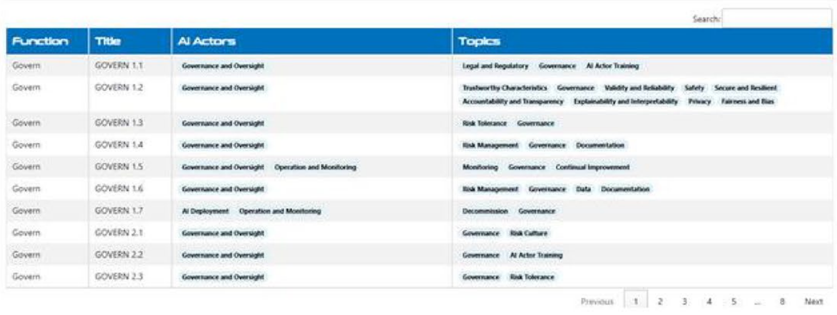
AI CYBER RISK Management Playbook

AI Governance Playbook

AI Guidance

NIST AI RMF

Explore the Playbook



Search:

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

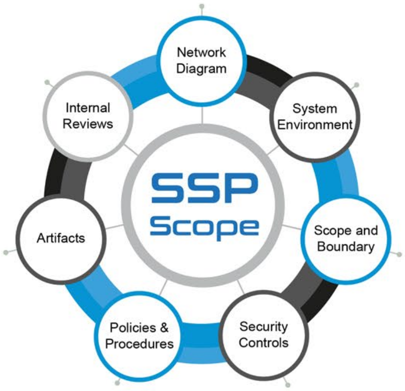
System Security Plan

Playbook | Template | Portal

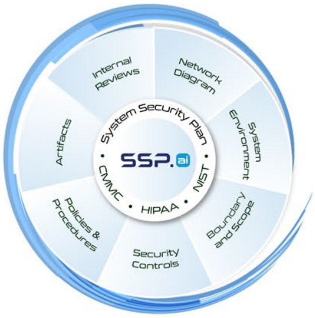
SSP.ai System Security Plan

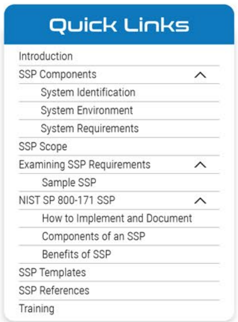
ecfirst online

- 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

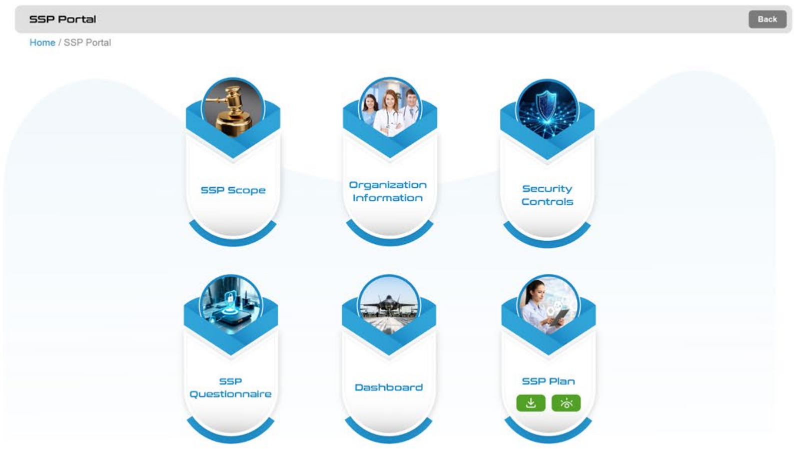
- Introduction
- SSP Components
  - System Identification
  - System Environment
  - System Requirements
- SSP Scope
- Examining SSP Requirements
  - Sample SSP
- NIST SP 800-171 SSP
  - How to Implement and Document
  - Components of an SSP
  - Benefits of SSP
- SSP Templates
- SSP References
- Training

SSP Templates

SSP Level 1 Template

SSP Level 2 Template

SSP.ai



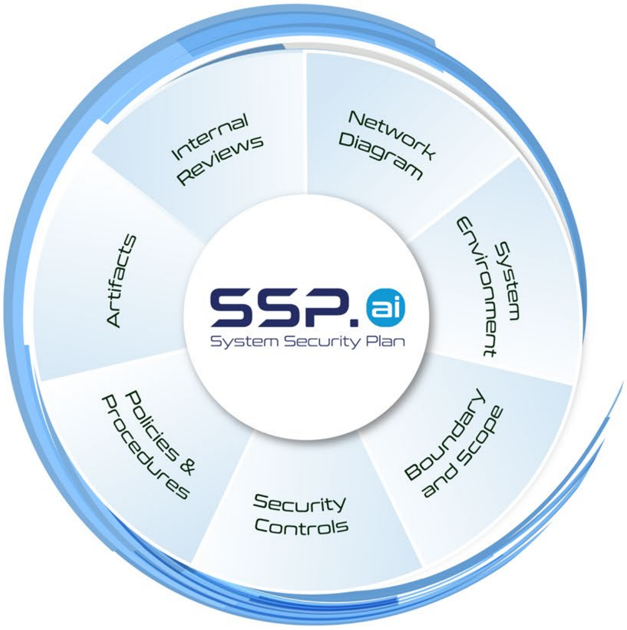
SSP Portal

Back

Home / SSP Portal

Subscription

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

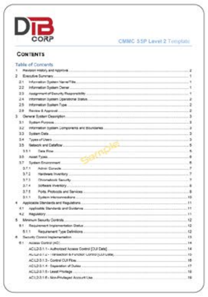
SSP Level 1
Template

ecfirst

SSP Level 2
Template

ecfirst

Inside the SSP


DTB CORP

CMMC SSP Level 2 Template

CONTENTS

Table of Contents

1 Revision History and Approvals ... 2
2 Executive Summary ... 1
2.1 Information System Name/Title ... 1
2.2 Information System Owner ... 1
2.3 Assignment of Security Responsibility ... 1
2.4 Information System Operational Status ... 2
2.5 Information System Type ... 2
2.6 Review & Approval ... 2
3 General System Description ... 3
3.1 System Purpose ... 3
3.2 Information System Components and Boundaries ... 3
3.3 System Data ... 3
3.4 Types of Users ... 3
3.5 Network and Dataflow ... 5
3.5.1 Data Flow ... 6
3.6 Asset Types ... 6
3.7 System Environment ... 6
3.7.1 Admin Console ... 7
3.7.2 Hardware Inventory ... 7
3.7.3 Chromebook Security ... 7
3.7.4 Software Inventory ... 8
3.7.5 Ports, Protocols and Services ... 8
3.1.1 System Interconnections ... 10
4 Applicable Standards and Regulations ... 11
4.1 Applicable Standards and Guidance ... 11
4.2 Regulatory ... 11
5 Minimum Security Controls ... 12
5.1 Requirement Implementation Status ... 12
5.1.1 Requirement Type Definitions ... 12
6 Security Control Implementation ... 13
6.1 Access Control (AC) ... 14
AC.L2-3.1.1 - Authorized Access Control [CUI Data] ... 14
AC.L2-3.1.2 - Transaction & Function Control [CUI Data] ... 15
AC.L2-3.1.3 - Control CUI Flow ... 16
AC.L2-3.1.4 - Separation of Duties ... 17
AC.L2-3.1.5 - Least Privilege ... 18
AC.L2-3.1.6 - Non-Privileged Account Use ... 18

Sample

Training Resources

CAICO
CMMC CERTIFIED PROFESSIONAL
CCP

CAICO
CMMC CERTIFIED ASSESSOR
CCA

AI
Certification Training
HITRUST
HIPAA
NIST
Cyber Defense
CMMC
Compliance
Online Store
Client Reference

SSP Template

SSP Level 1

SSP Level 1
Template

Level 1

15
Requirements

FCI

SSP Level 2

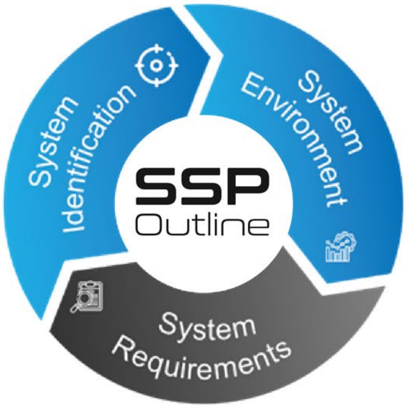
SSP Level 2
Template

Level 2

110
Requirements

CUI

Procedures



Organization's Security Controls

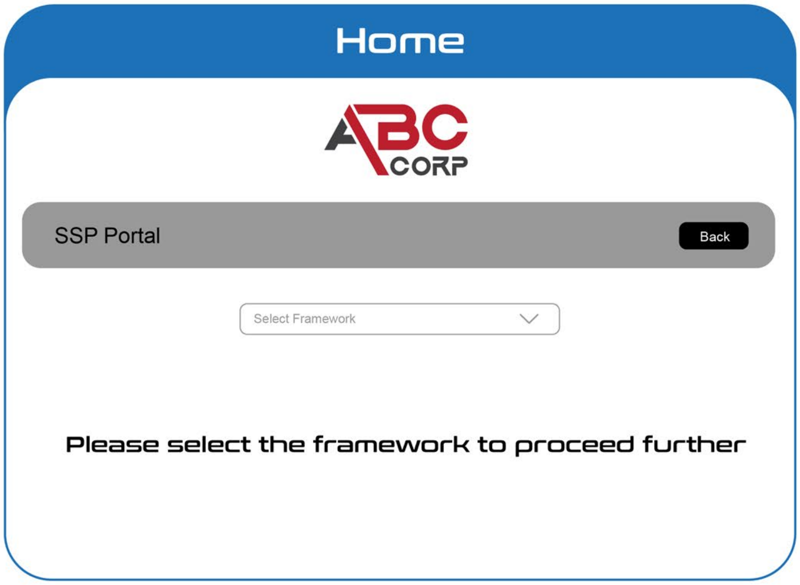
Policies

AI
Certification Training
HITRUST
HIPAA
NIST
Cyber Defense
CMMC
Compliance
Online Store
Client Reference

SSP Portal

SSP.ai System Security Plan | ecfirst online

Home



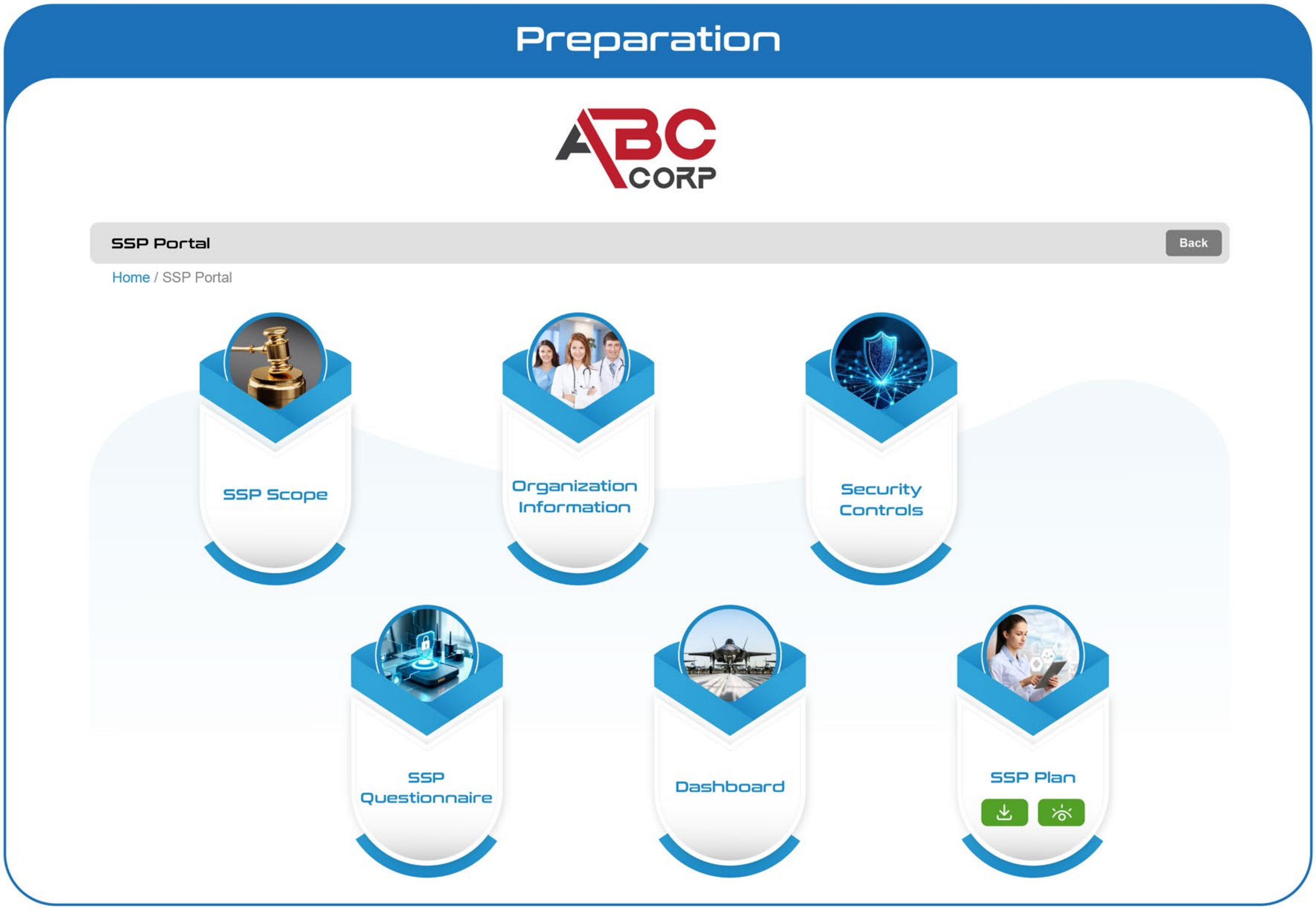
ABC CORP

SSP Portal — Back

Select Framework

Please select the framework to proceed further

Preparation



ABC CORP

SSP Portal — Back

Home / SSP Portal

- SSP Scope
- Organization Information
- Security Controls
- SSP Questionnaire
- Dashboard
- SSP Plan

AI Training
References

“ 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. ”

“Comprehensive HIPAA course manual and content resources.”

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

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

“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.”

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."

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**.”

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."

CMMC Consulting
References

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.”

> “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.”

AI
Certification Training
HITRUST
HIPAA
NIST
Cyber Defense
CMMC
Compliance
Online Store
Client Reference

“ 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

Get Started

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

Info@ecfirst.com

www.ecfirst.com | www.ecfirst.biz