

# Program CATALOG



# Message from the Chief Executive

## Welcome to ecfirst!

At ecfirst, we stand at the intersection of AI risk management, cyber defense, and compliance. 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







**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

<b>AI</b>	aiCRP Certification	5
	AI Risk Management Assessment	6
<b>Certification Training</b>	AI   HIPAA   Cyber Defense	7
	CHP Certification	8
	CSCS™ Certification	9
	CCSA™ Certification	10
	CMMC for Executives	11
<b>HITRUST</b>	Why ecfirst for HITRUST	12
	HITRUST e1 Certification	13
	HITRUST i1 Certification	14
	HITRUST r2 Certification	15
<b>HIPAA</b>	Why ecfirst for HIPAA	16
	Risk Assessment	17
	HIPAA End-User Training	18
<b>NIST</b>	Why ecfirst for NIST	19
	NIST SP 800-53 r5 Risk Assessment	20
	NIST SP 800-171 r3 Assessment	21
<b>Cyber Defense</b>	Cybersecurity Assessment	22
	CloudFirst Assessment	23
	Pen Test	24
	Red Team Exercise	25
	Online Tracking Assessment	26
	Social Engineering	27
<b>CMMC</b>	Why ecfirst for CMMC	28
	CCP Training	29
	CCA Training	30
	CMMC Assessment	31
	CMMC Readiness Mock Assessment	32
	System Security Plan	33
<b>Compliance</b>	Ransomware Readiness BIA   DRP	34
	Managed Compliance	35
	On Demand Consulting	36
	PCI DSS Pre-Assessment	37
	GDPR Compliance Pre-Assessment	38
<b>Online Store</b>	Online Store	39
	Compliance and Cyber Toolkit	40
	Toolkit Package CMMC   HIPAA   NIST	41
	Playbooks HIPAA   CMMC   CAP   CUI   SSP	44
<b>Client References</b>	AI	49
	CHP	50
	CSCS™	51
	CCSA™	52
	HITRUST	53
	HIPAA	54
	CMMC	55
	CCP	56
	CCA	57



The Industry's First AI Cyber Risk Management Training program



Unlock the World's First AI Playbook



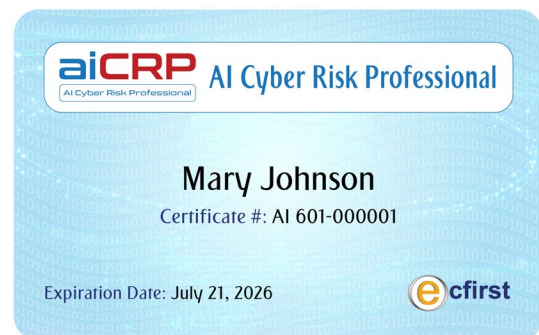
**AI CYBER RISK  
Management  
Playbook**

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 assessments



## 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.



# AI Risk Management Assessment



## AI Risk Assessment



## Sources





### 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 Harbour



### 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



### 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



### 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 assessments





Healthcare Industry's First  
& Leading HIPAA Credential



**HIPAA**  
Playbook



“

**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 Harbour



## 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.



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



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

## What's in it for you?

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

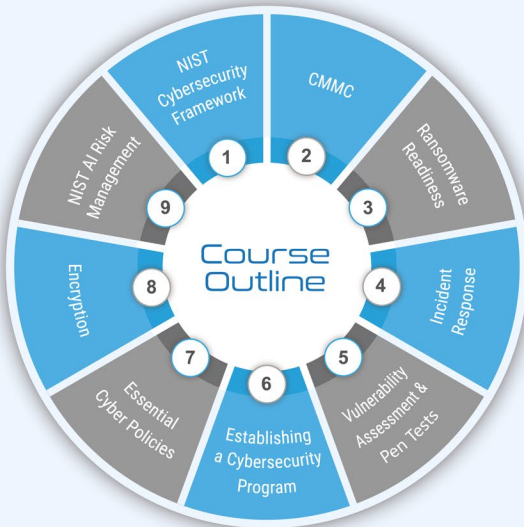


## Digital Badge

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



An Executive Cybersecurity Program



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

## What's in it for you?

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



### Digital Badge

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







Online | Self-Paced



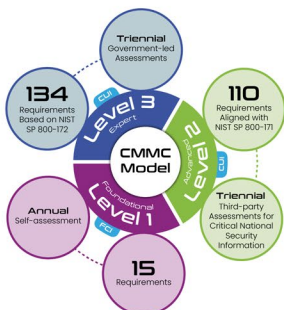
## An Executive CMMC Program



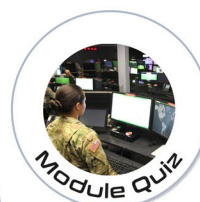
Cybersecurity Maturity Model Certification

[Welcome](#) [Home](#) [Dashboard](#) [Logout](#)

### CMMC Playbook



## CMMC For Executives



# HITRUST

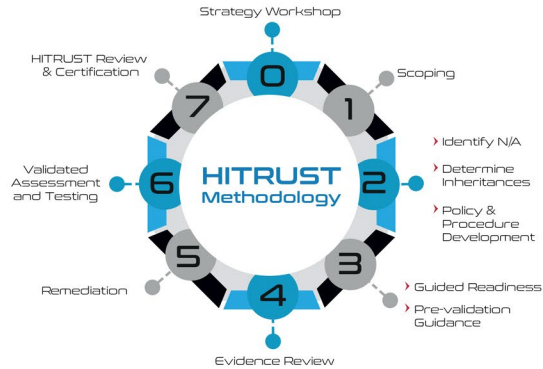
## Why ecfirst?

**HITRUST**  
Authorized External Assessor

**ecfirst**

ecfirst is one of the few HITRUST External Assessment Organizations to achieve HITRUST Certification.

### Signature Methodology



### Devoted to Client Success

### HITRUST Assessor Council

Member, AI Committee

HITRUST Commitment

**COLLABORATE**<sup>24</sup>  
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

Monthly Payment

Multi year Engagement

Flat Price

**e1 · i1 · r2 · AI**



AI

Certification  
Training

HITRUST

HIPAA

NIST

Cyber  
Defense

CM/MC

Compliance

Online  
Store

Client  
Reference

e1 Essentials

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



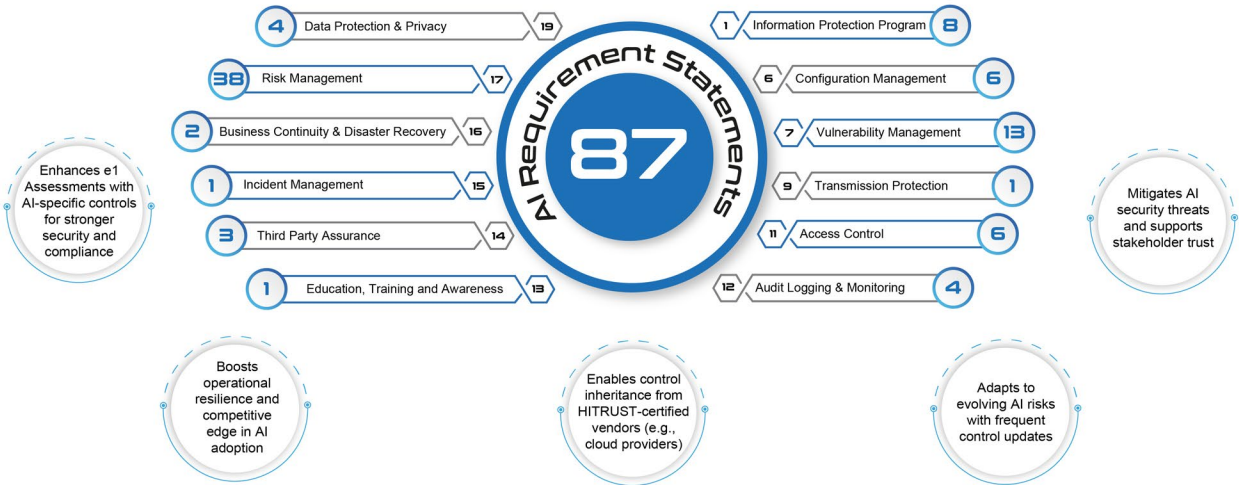
HITRUST e1 and HIPAA

- ✖ 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





### 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			Domain		
1	Information Protection Program	15	10	Password Management	6
2	Endpoint Protection	7	11	Access Control	21
3	Portable Media Security	6	12	Audit Logging & Monitoring	9
4	Mobile Device Security	6	13	Education, Training, and Awareness	6
5	Wireless Security	7	14	Third Party Assurance	8
6	Configuration Management	9	15	Incident Management	7
7	Vulnerability Management	12	16	Business Continuity & Disaster Recovery	10
8	Network Protection	9	17	Risk Management	10
9	Transmission Protection	9	18	Physical & Environmental Security	15
			19	Data Protection & Privacy	10



### 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.



#### Timeline



Eligibility Questionnaire becomes available.

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



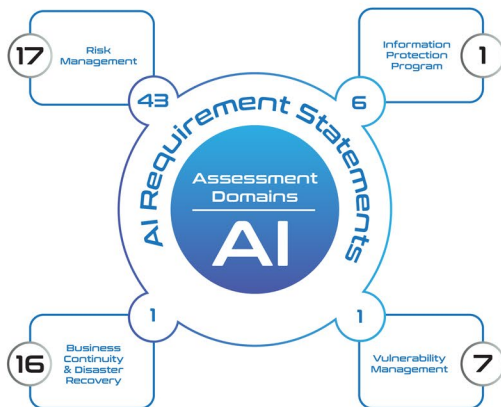
### r2 Key Highlights

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.

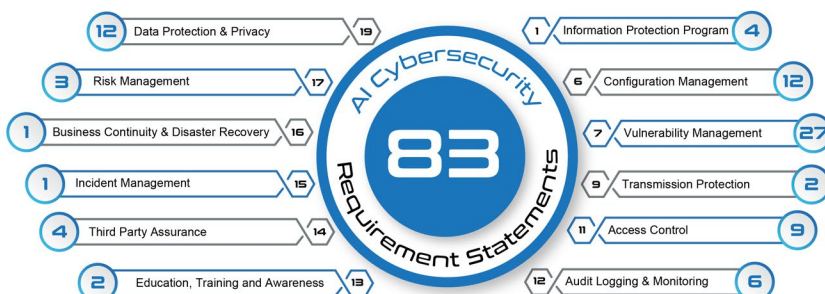
### HITRUST r2 Certification



### AI Cybersecurity Requirements



### 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?



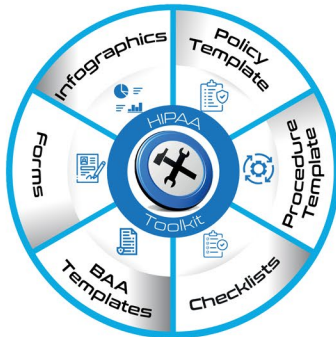
HIPAA Signature Methodology

Industry Leading HIPAA Certification Training  
Updated with NPRM



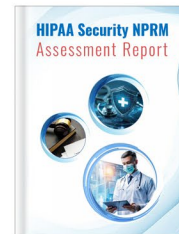
Delivering HITRUST Certification Since 2016

AI Powered HIPAA Playbook



HIPAA Toolkit  
[www.ecfirst.biz](http://www.ecfirst.biz)

HIPAA NPRM Assessment



HIPAA Compliance Attestation

AI

Certification Training

HITRUST

HIPAA

NIST

Cyber Defense

CMIMC

Compliance

Online Store

Client Reference



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

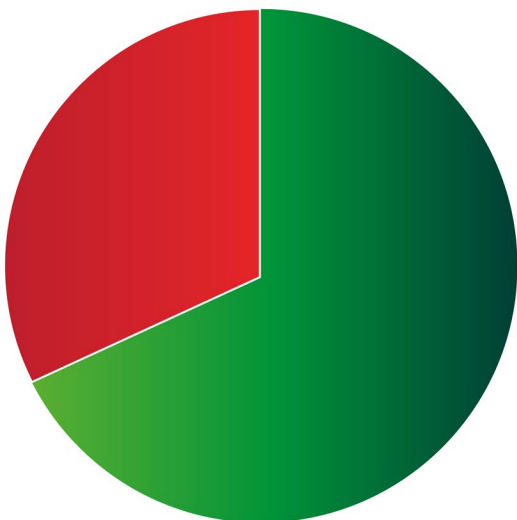
Grade	Security Rule
D	Administrative Safeguards
F	Physical Safeguards
A	Technical Safeguards
B	Organizational Requirements
F	Policies, Procedures, and Documentation
Privacy Rule	
B	Administrative Requirements
A-	Uses and Disclosures
Breach Notification	
C	Reporting

## Signature Methodology

HIPAA + NIST

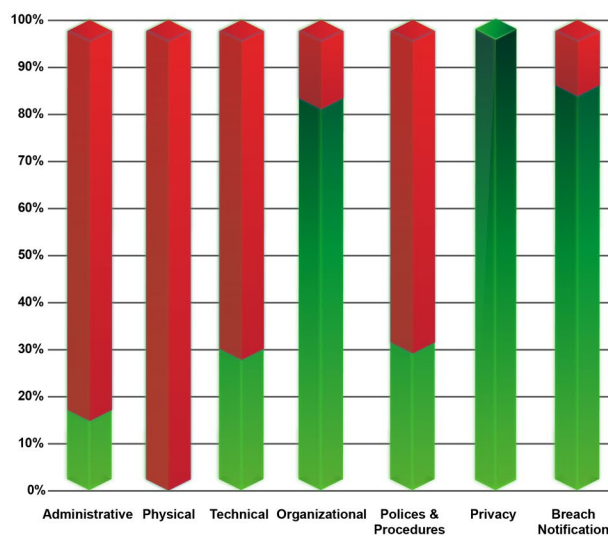


## Compliance Status



Met Not Met

## Implementation Specifications



## 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

Course Description

Online Slides

Knowledge Check

HIPAA & Information Security Training

Certificate Quiz

Cybersec Col

Insider Threa

HIPAA and In

Introduction t



Home / HIPAA End-User Training / Online Slides

Download Back

### HIPAA End-User Training

1 HIPAA Fundamentals [Start](#)

2 HIPAA Privacy Rule [Start](#)

3 HIPAA Security Rule [Start](#)

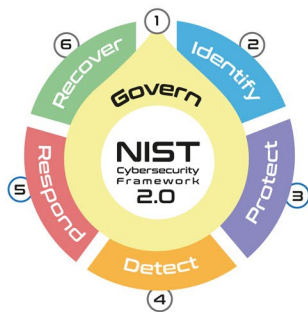
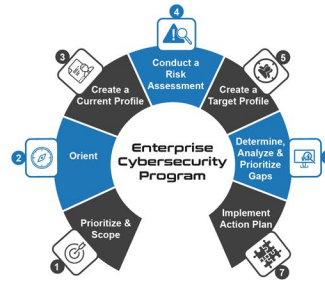
4 HITECH Breach [Start](#)

5 Cybersecurity Fundamentals [Start](#)

6 Appendix A: Acronyms [Start](#)

7 Appendix B: Glossary [Start](#)

## NIST Signature Methodology



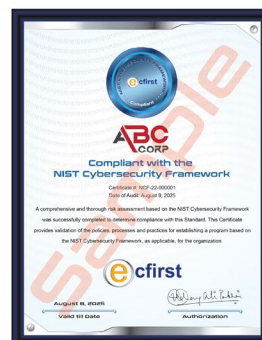
## NIST 2.0 Assessment

## Industry Leading Cybersecurity Certification Training



## NIST Risk Assessment Report

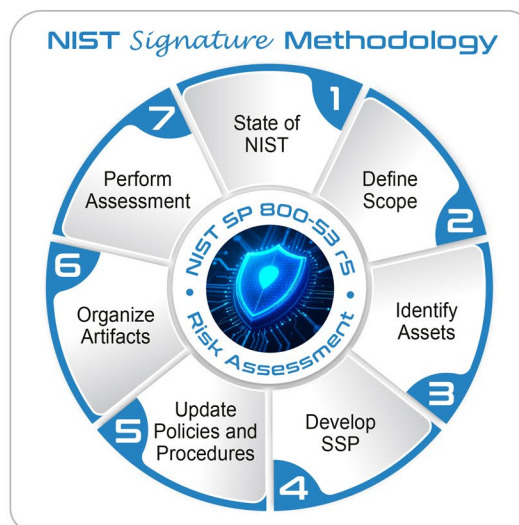
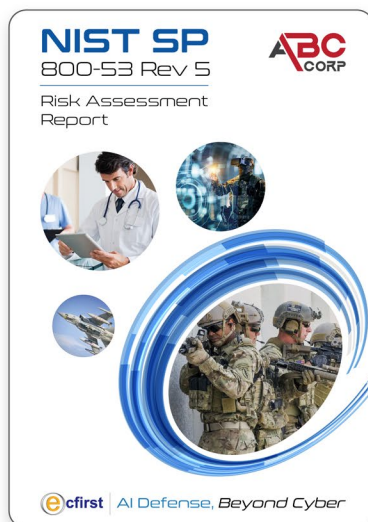
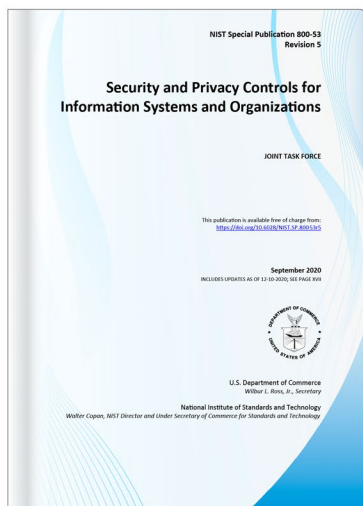
## NIST Compliance Attestation





# NIST SP 800-53 r5

## Risk Assessment



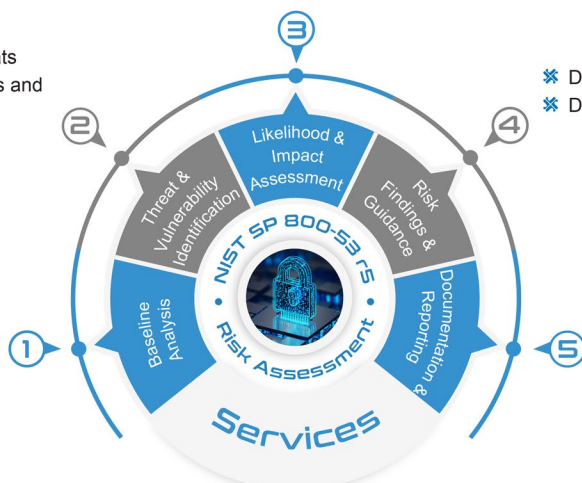
Evaluate risk severity and align with organizational risk tolerance

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

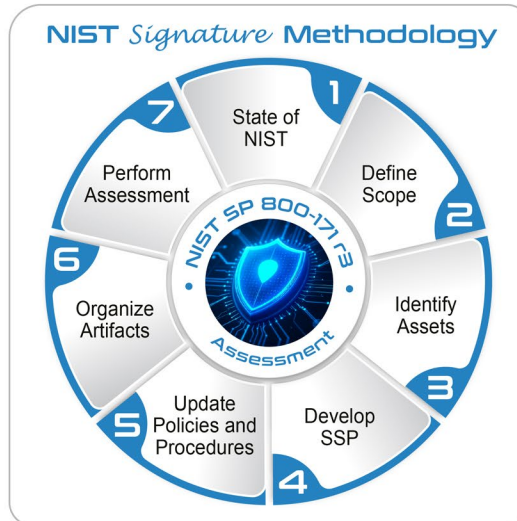
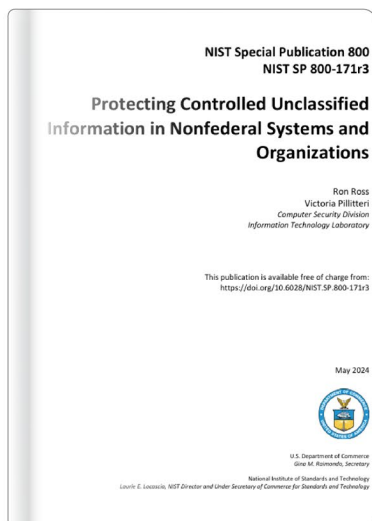
- ✖ Determine risk levels (low, moderate, high)
- ✖ Deliver a prioritized mitigation plan

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

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



# NIST SP 800-171 r3 Assessment



## NIST SP 800-171 r3 Assessment Portal

**NIST SP 800-171r3**

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

Intake Form

Assessment Information

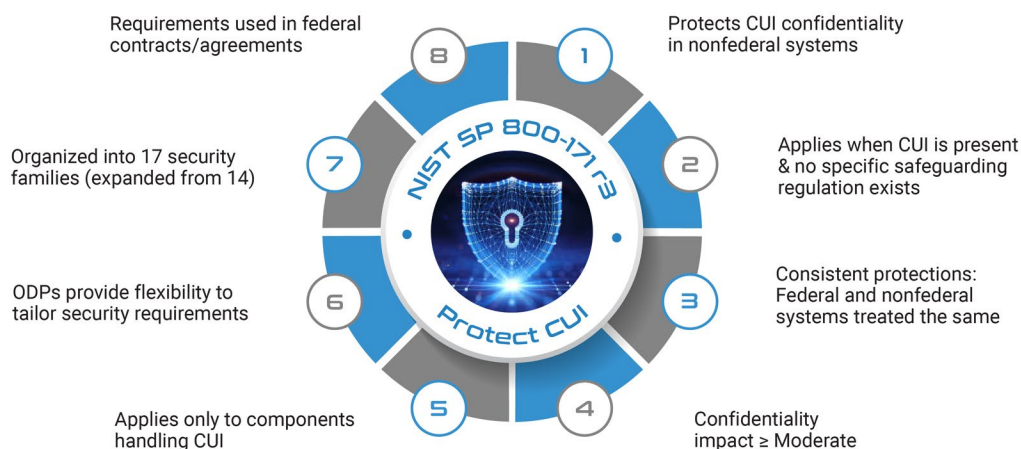
Roles

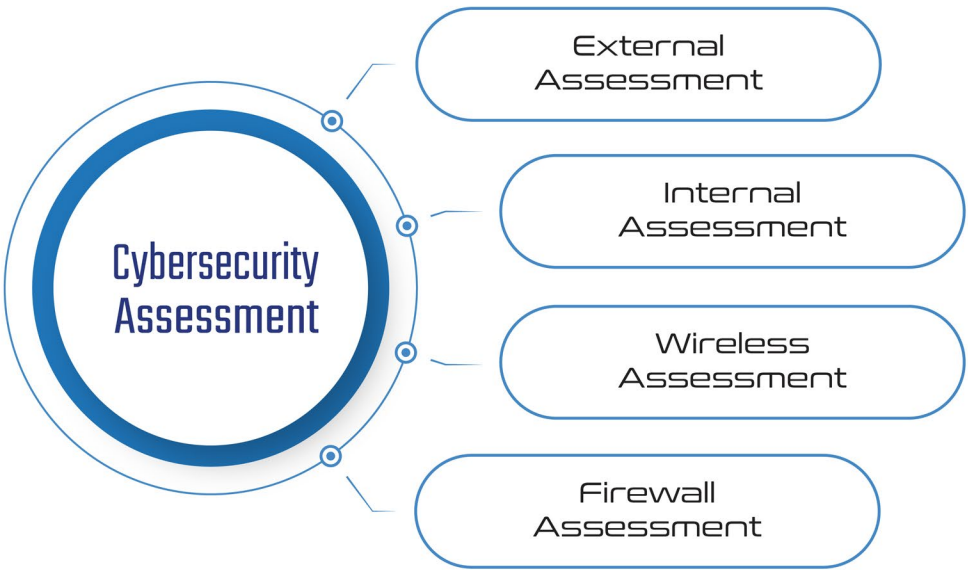
Assessment Questionnaire

Planning

POA&M

[Reference Documents](#)





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

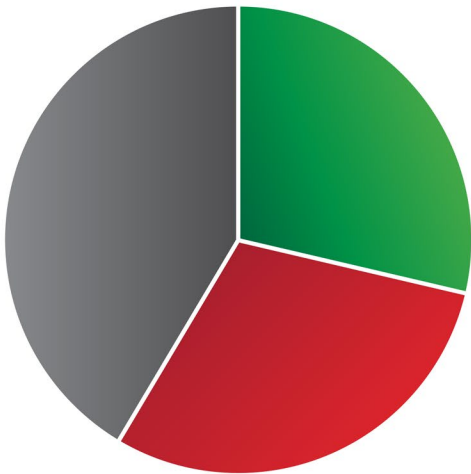
CYBERSECURITY ASSESSMENT SCOPE	TITANIUM	PLATINUM	GOLD	SILVER	BRONZE
External Assessment	✔ Customized	✔	✔	✔	✔
Internal Assessment	✔ Customized	✔	✔	✖	✖
Firewall Assessment	✔ Customized	✔	✔	✔	✖
Wireless Assessment	✔ Customized	✔	✖	✖	✖
Detailed Analysis	✔	✔	✔	✔	✖
Corrective Action Plan (CAP)	✔	✔	✔	✖	✖
Detailed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



CloudFirst Assessment



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 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

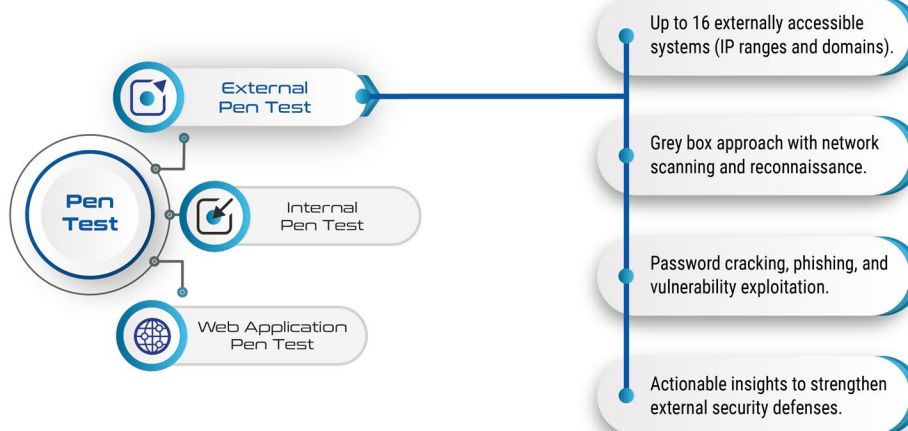
Internal Assessment

- An Active Directory (AD) domain is tested

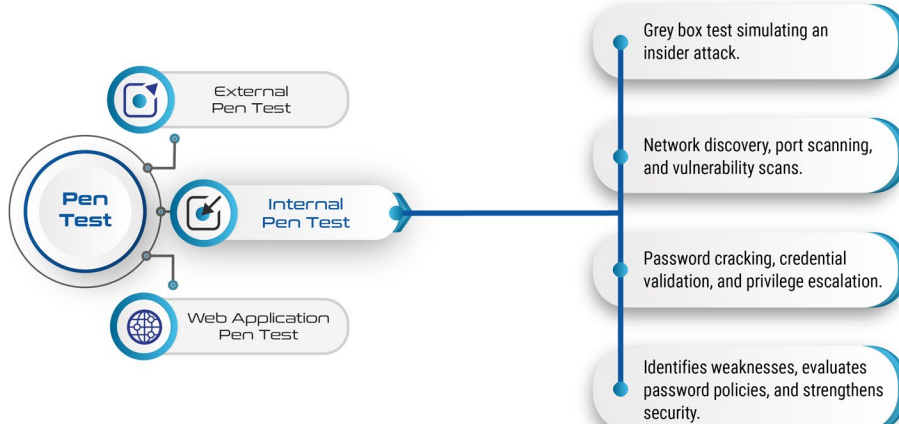
Significant Findings



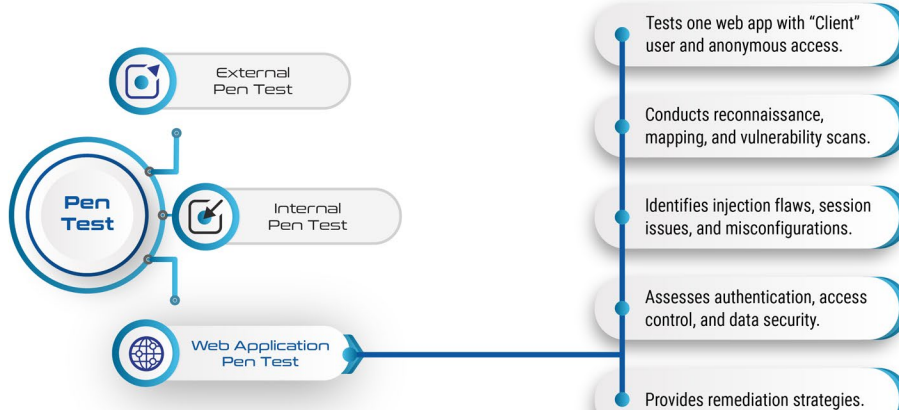
## External Pen Test

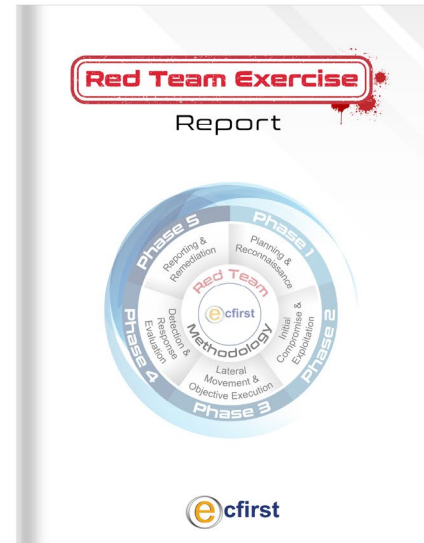
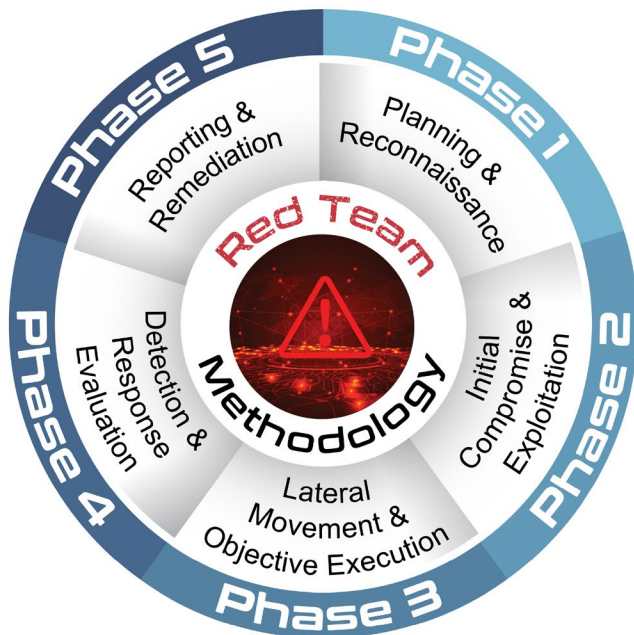


## Internal Pen Test



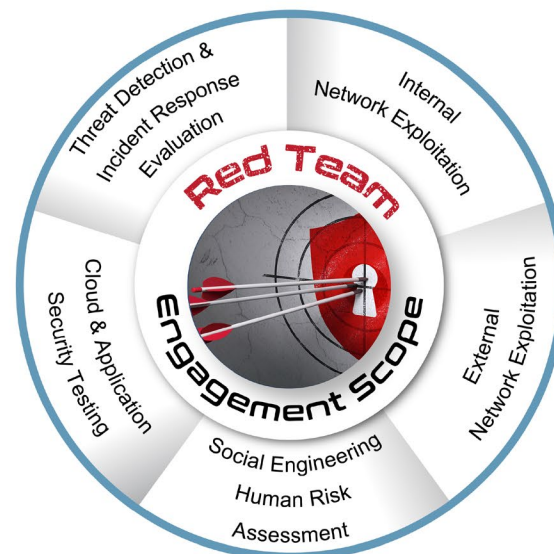
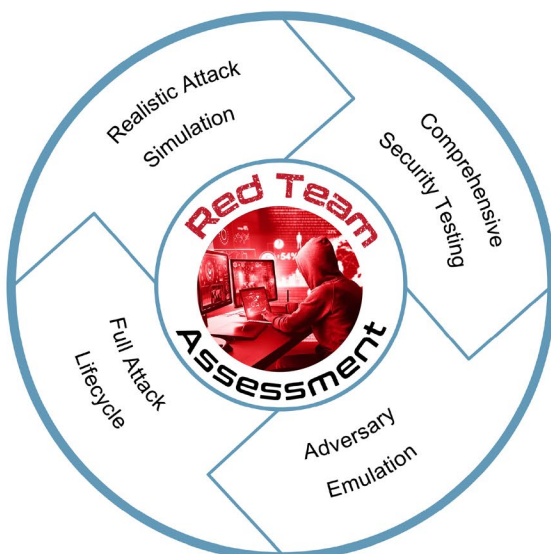
## Web Application Pen Test





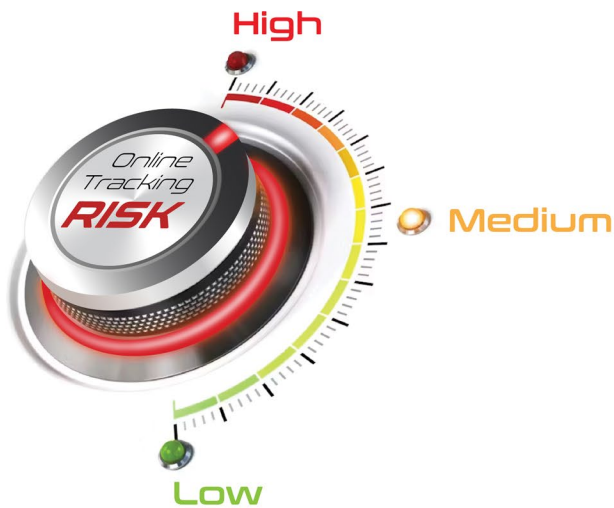
## Red Team Exercise

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





# 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

”



AI

Certification Training

HITRUST

HIPAA

NIST

Cyber Defense

CMIMC

Compliance

Online Store

Client Reference

- ✖ 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 campaigns 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

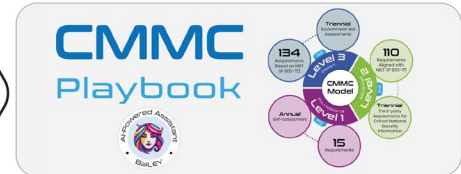
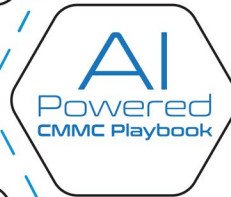
Dear ,

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

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



**Surgically Defined CMMC Assessment Process**



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.”



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**



**DoD CMMC Certification Training Content**  
 Approved and Authorized

**DoD CMMC Certification Training Provider**  
 Approved and Authorized





## 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.

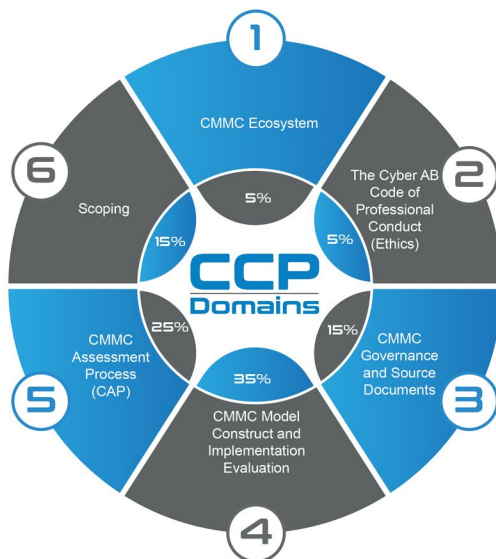
## Why ecfirst for CCP Training?

- ❌ 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!

## 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>

## CMMC Certified Professional (CCP)



## 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
1	CCP Pre Program Prep			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	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	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	10
7	Scoping Blueprint Domain 6	15%	Domain 6 & Review Friday, Day 4 8:30 am - 12:30 pm	4
8	Practice Exam & Review			

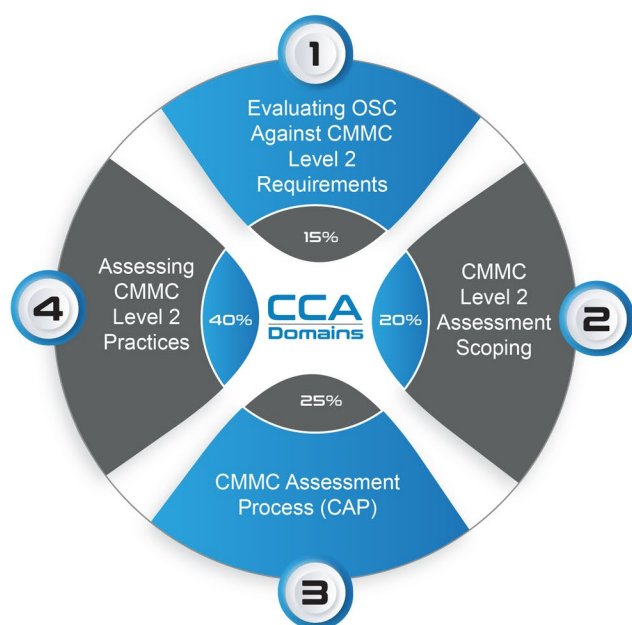
## Intended Audience

- ❌ 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

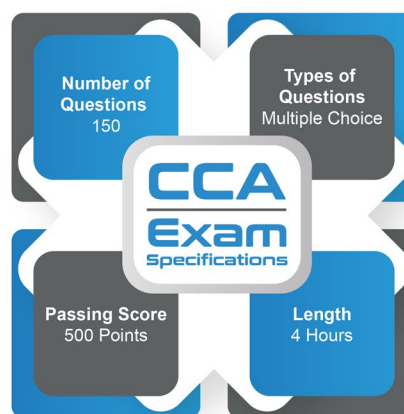
## Summary

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
1	CCA Pre Program Prep			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	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	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	10
6	Practice Exam & Review		Review and Final Quiz Friday, Day 4 8:30 am - 12:30 pm	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!

## Week 1

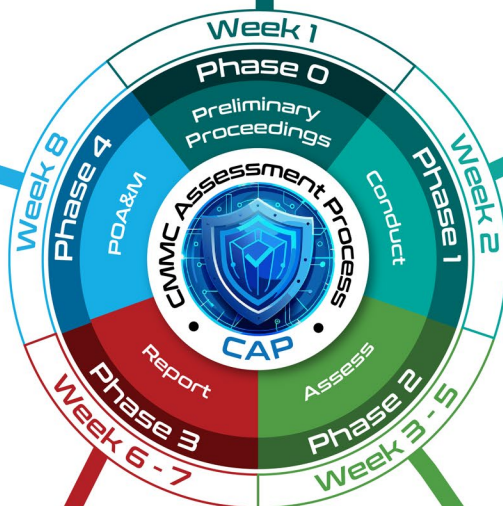
- Receive CMMC Assessment Request from OSC
- Confirm the Entity/Entities to be Assessed
- Frame the Assessment
- Identify and Manage Initial COI
- Execute Contractual Agreement

## 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

## Week 8

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



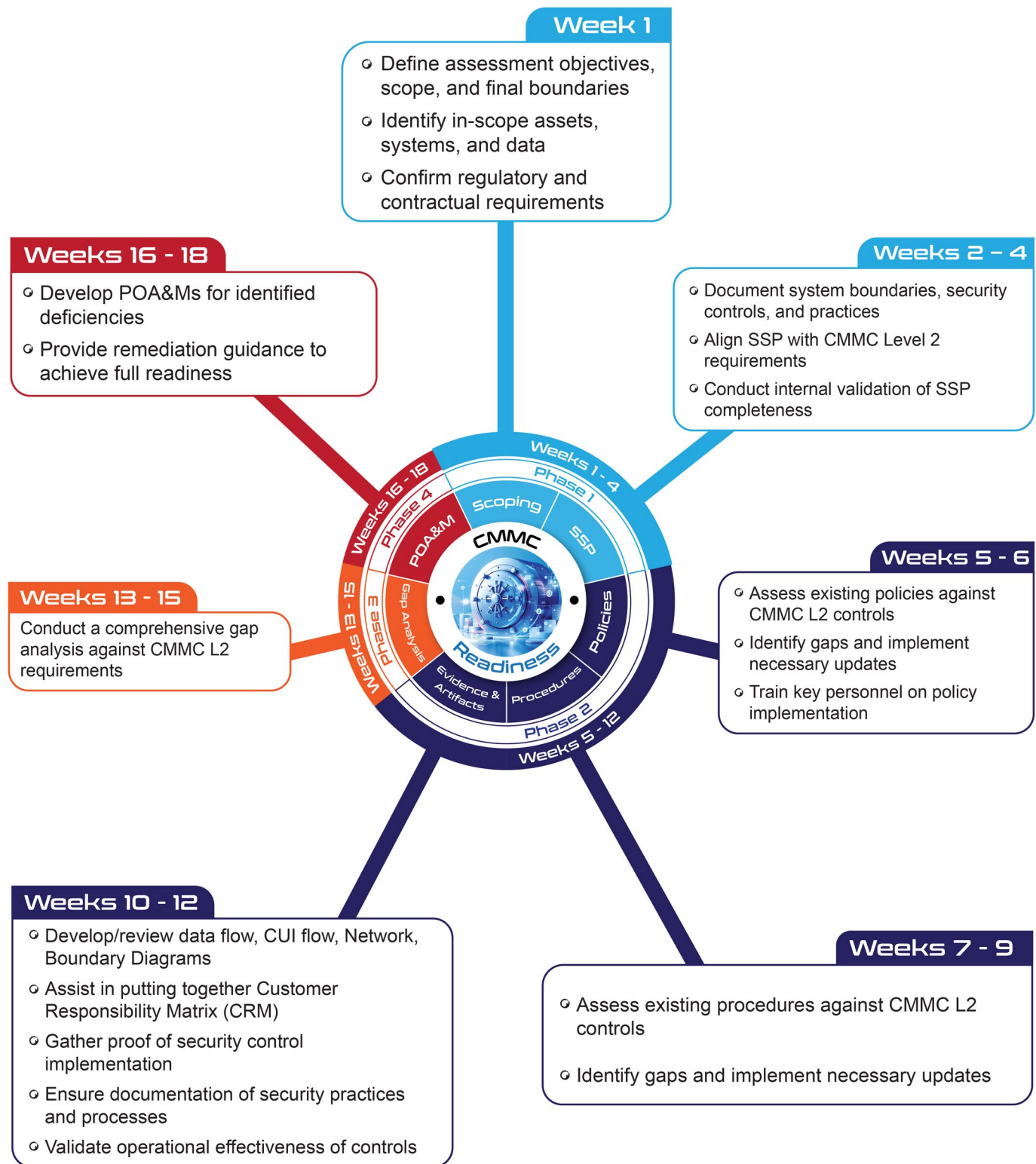
## Weeks 3 - 5

- 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)





# 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 Level 1 Template



### SSP Level 2 Template



**SSP.ai**

SSP Portal

Home / SSP Portal

Back



SSP Scope



Organization Information



Security Controls



SSP Questionnaire



Dashboard



SSP Plan

Download

Print

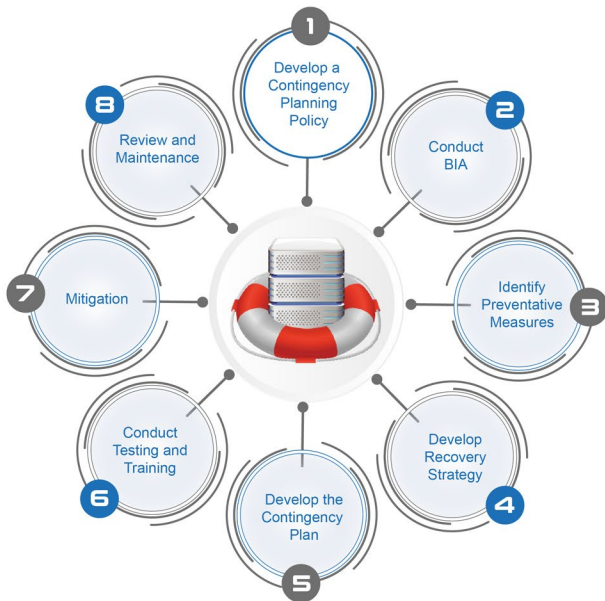
Subscription

## SSP Report





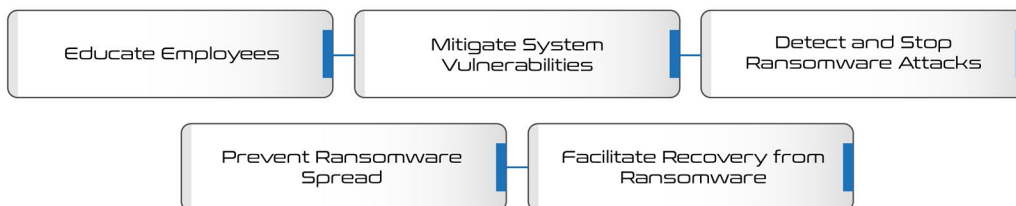
## Business Impact Analysis (BIA)



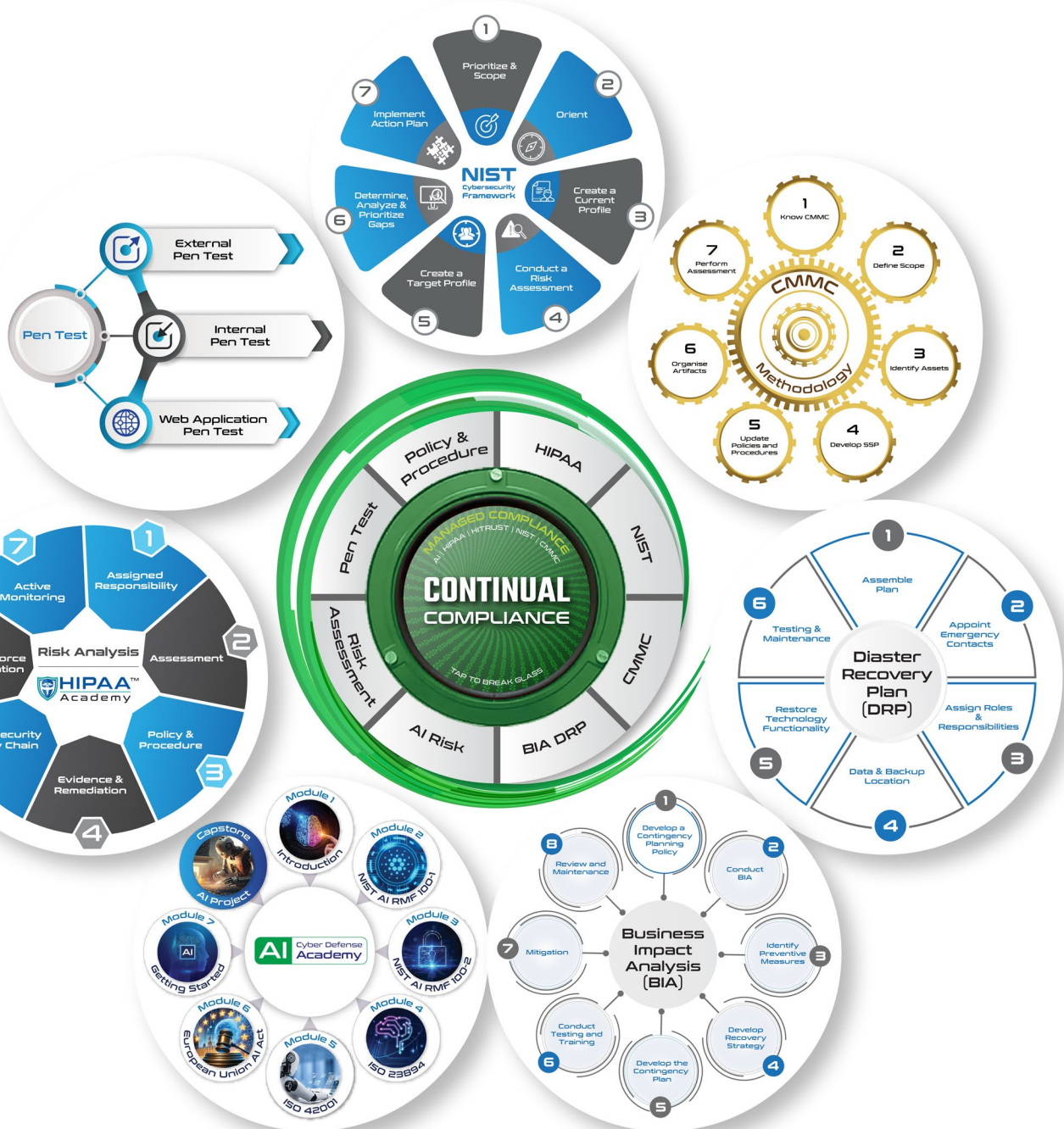
## IT Disaster Recovery Plan



## Ransomware Resilience







## Consulting (ODC)

Fixed-rate

Expert Advisors

No Long-term Commitment

Short Term Consulting

Pen Test

ON DEMAND CONSULTING  
HIPAA | HITRUST | NIST | CMMC  
**COMPLIANCE  
EMERGENCY**  
TAP TO BREAK GLASS

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

## Policy and Procedures

Security Policy  
Template  
July 1, 2024



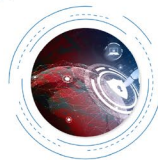
ecfirst

Cyber Procedures  
Template  
July 1, 2024



ecfirst

InfoSec Procedures  
Template  
July 1, 2024



ecfirst

Privacy Policy  
Template  
July 1, 2024



ecfirst

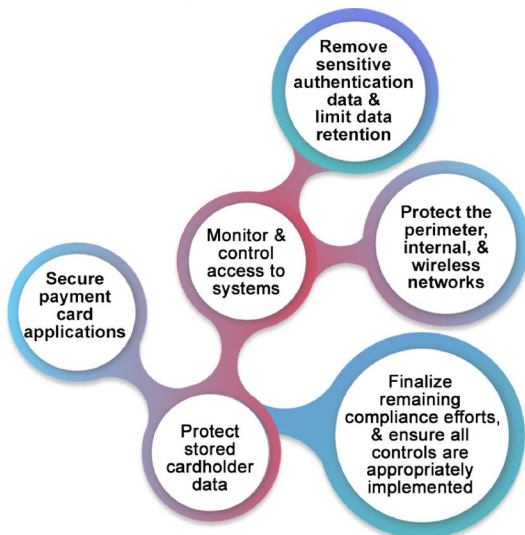


### PCI DSS Readiness Assessment

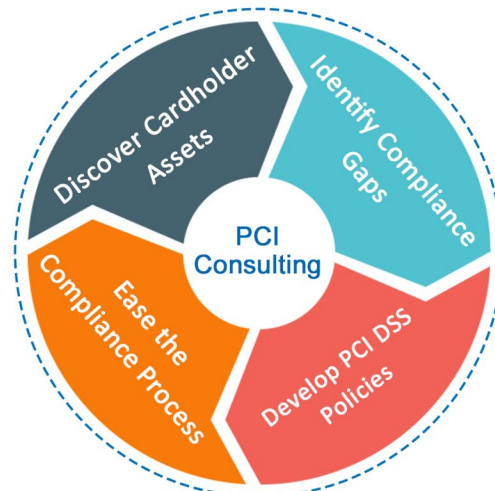
- ❖ Review of compliance against PCI DSS v4.0 requirements
- ❖ Identify gaps & risks in protecting cardholder data
- ❖ Deliver actionable assessment report with findings
- ❖ Provide prioritized remediation plan & timeline
- ❖ Executive summary for leadership & stakeholders



### PCI DSS Goals



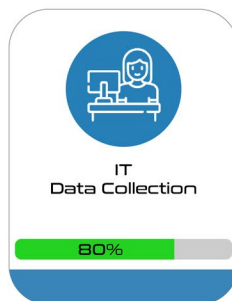
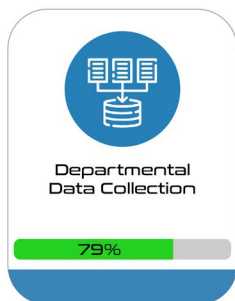
### PCI Consulting



### PCI DSS Portal

**TRACER**<sup>SM</sup>  
ASSET RISK MANAGEMENT

**ABC**  
CORP



### PCI DSS





# GDPR Compliance Pre-Assessment



## 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 Assessment Report



## 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

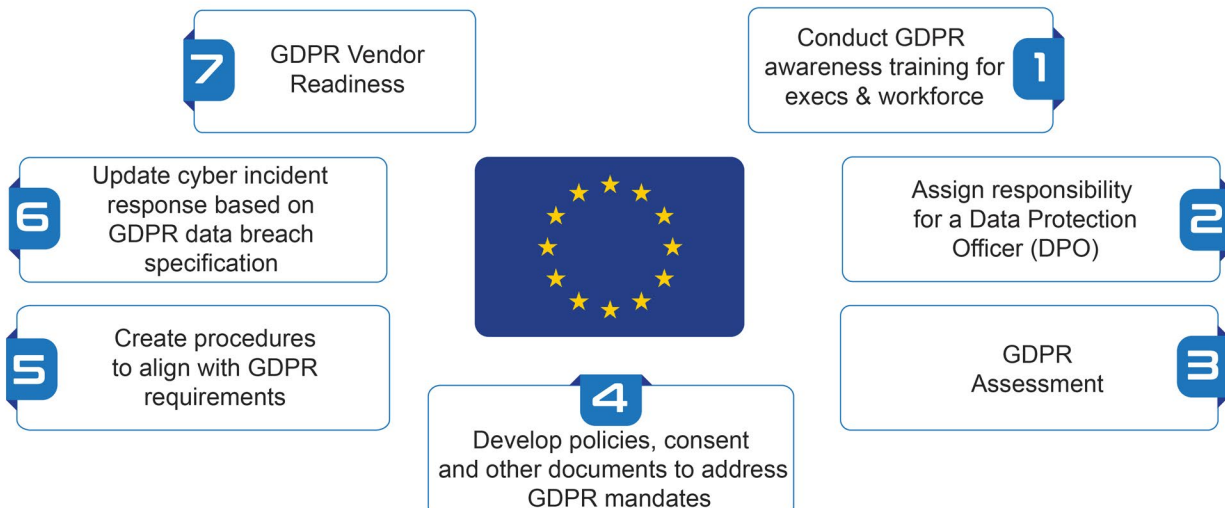
## GDPR Signature Methodology



## Purpose & Scope



## Establish a Credible GDPR Program



AI

Certification  
Training

HITRUST

HIPAA

NIST

Cyber  
Defense

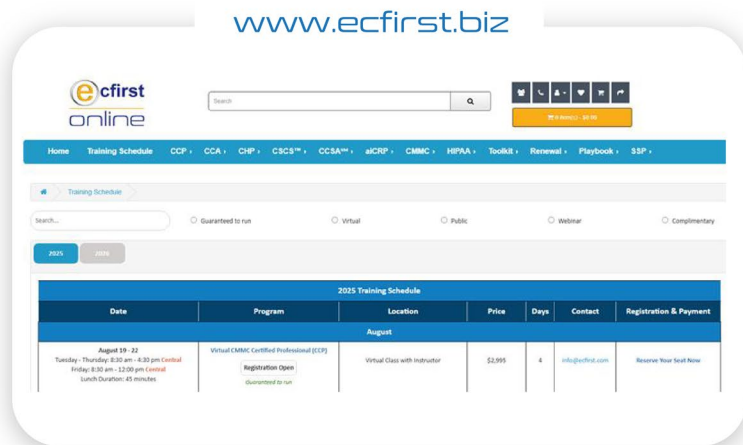
CMIMC

Compliance

Online  
Store

Client  
Reference

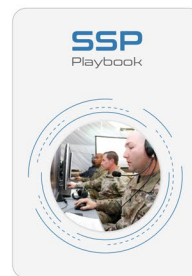
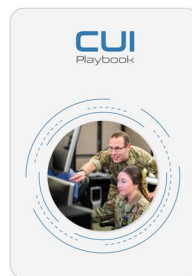
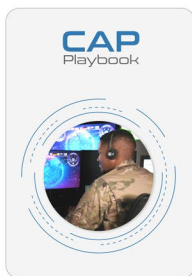
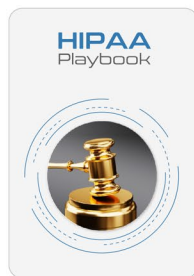
# Online Store



## Training



## Playbooks



## Templates

CMMC

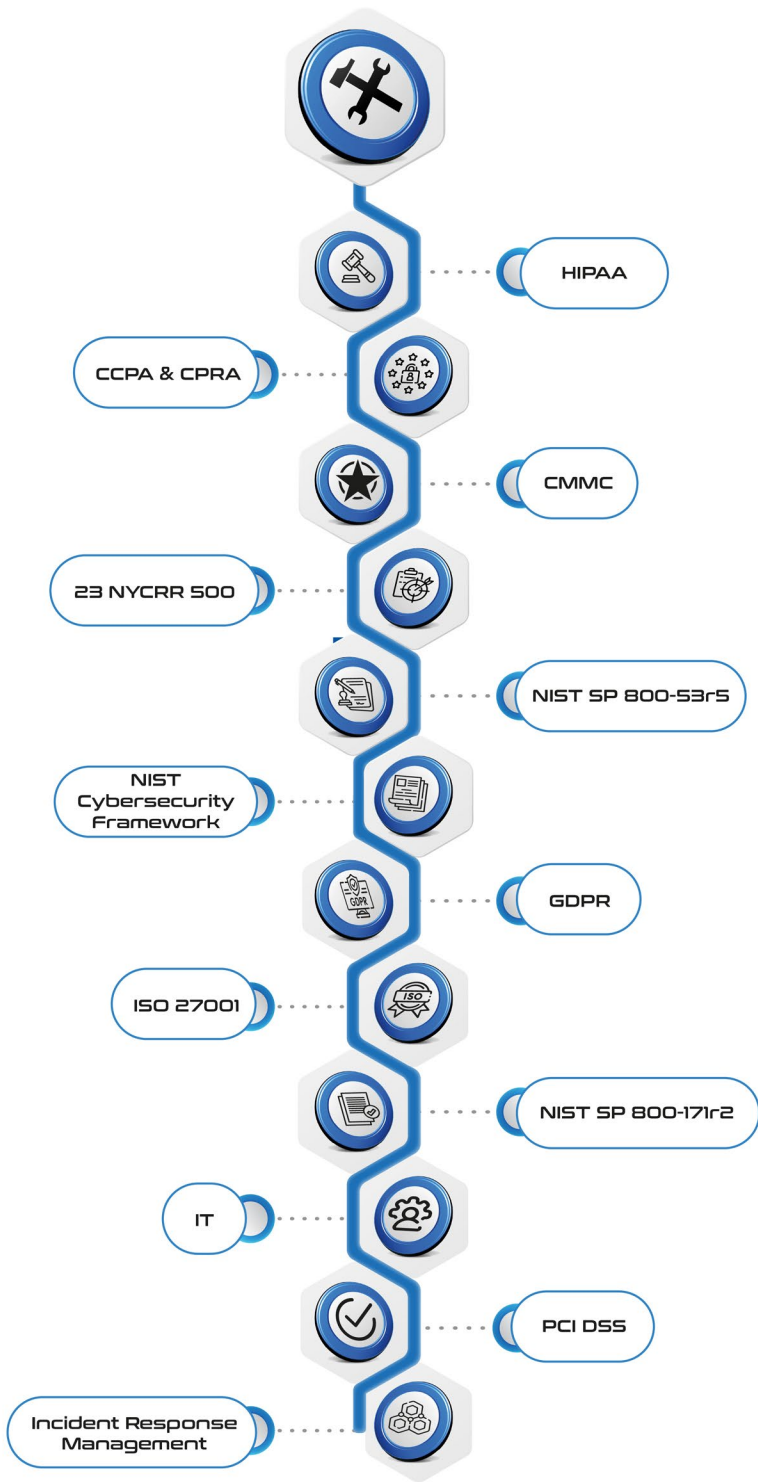
HIPAA

GDPR

NIST

SSP

Toolkit Packages



Components







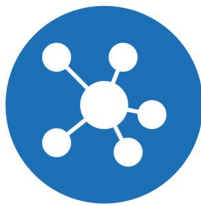
**Policy  
Template**



**Procedure  
Template**



**SSP Template**



**Mappings**

- ✧ CMMC → NIST Cybersecurity Framework
- ✧ CMMC → NIST SP 800-171r2
- ✧ CMMC → NIST SP 800-53r5

- ✧ CMMC Ecosystem
- ✧ CMMC Domains
- ✧ CMMC Level 1 Practices
- ✧ CMMC Level 1 Assessment Guidance
- ✧ CMMC Level 1 & 2 Assessment Objective
- ✧ CMMC Level 2 Practices
- ✧ CMMC Reciprocity



**Infographics**



## 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

## 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**

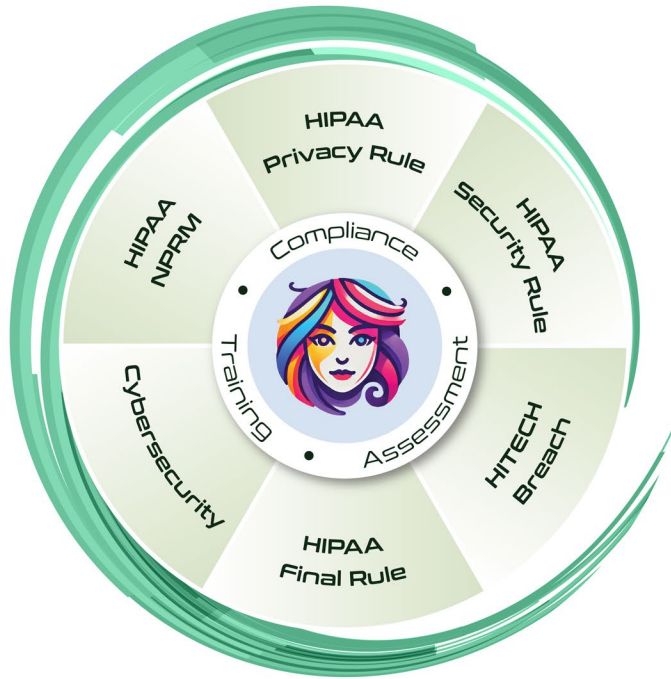
- ✳ Cybersecurity Controls
- ✳ Cybersecurity
- ✳ NIST Cybersecurity



**Mappings**

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





### 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



## Quick Links

Home

CMMC Final Rule

CMMC Level

CMMC Domains

Domains/Roles/Topics

CMMC Training

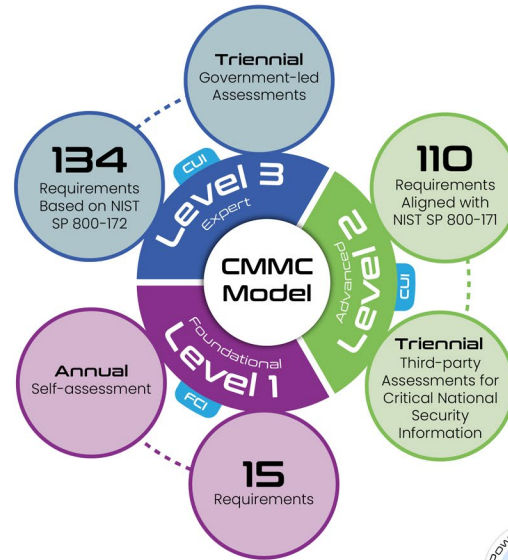
Source Documents

Getting Started with CMMC

DoD CUI Mandatory Training

CMMC Ecosystem

CMMC News



## Domains

Level 1

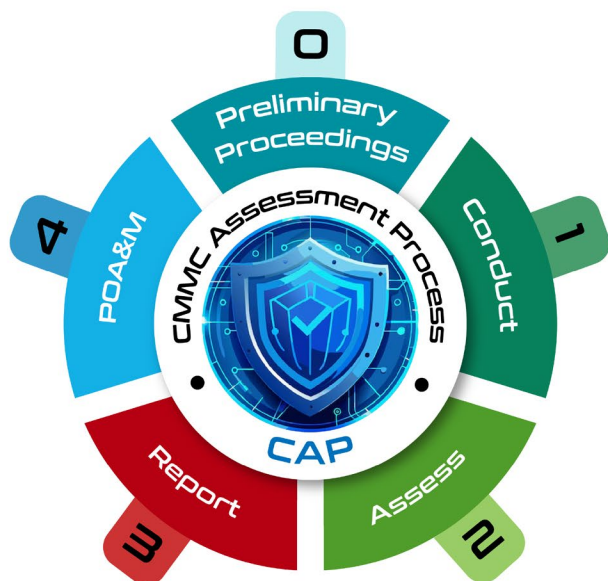
Level 2

Level 3



## Explore





## Quick Links

- Home
- ecfirst CAP Doctrine
- CMMC Assessment Readiness
- CMMC Training
- Assessment Phases
  - Phase 0: Primary Proceedings
  - Phase 1: Conduct the Pre-Assessment
  - Phase 2: Assess Conformity
  - Phase 3: Report Assessment Results
  - Phase 4: POA&M
- CMMC Source Documents
- Assessment Templates



## ecfirst CAP Doctrine



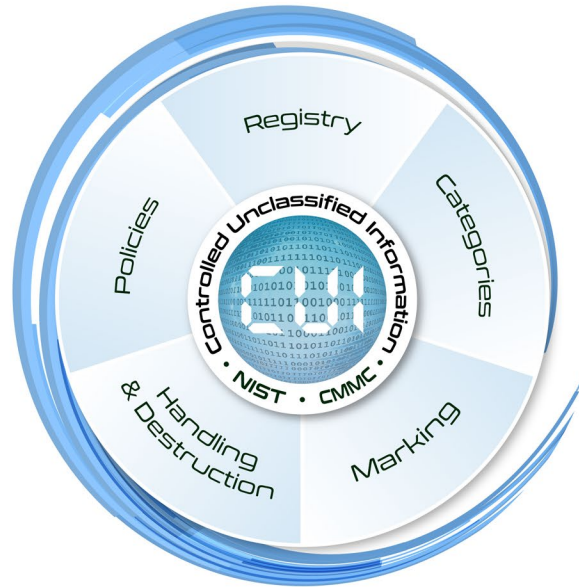
## CMMC Assessment Readiness





## Quick Links

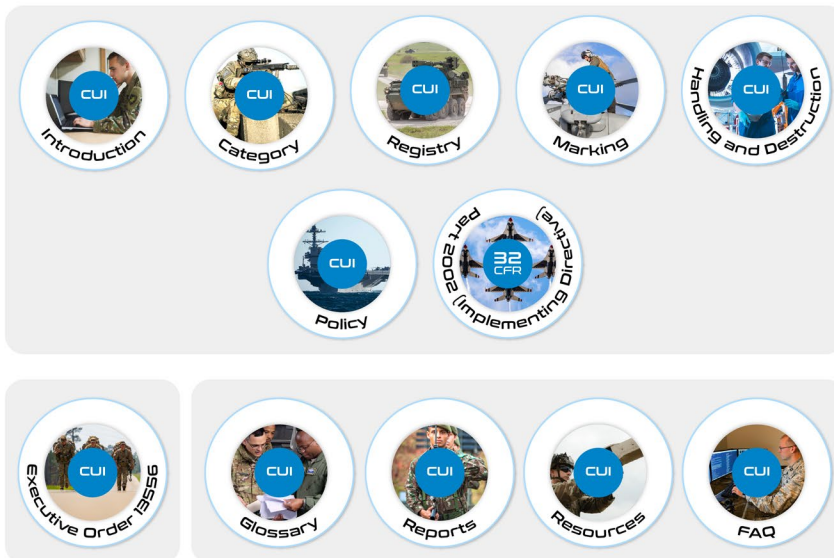
Home	
DoD CUI References	^
Introduction	
CUI Category	
CUI Registry	
CUI Marking	
CUI Policy	
FAQ	
NARA CUI References	^
Introduction	
CUI Category	
CUI Registry	
CUI Marking	
CUI Handling and Destruction	
CUI Policy	
CUI EO 13556	
32 CFR Part 2002	
CUI Glossary	
CUI Reports	
CUI Resources	
FAQ	
Training	



## DoD CUI References



## NARA CUI References



## Training Resources





## 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

CONTENTS	
1. Introduction	1
2. System Identification	2
3. System Environment	3
4. System Requirements	4
5. System Security Plan	5
6. System Security Plan	6
7. System Security Plan	7
8. System Security Plan	8
9. System Security Plan	9
10. System Security Plan	10
11. System Security Plan	11
12. System Security Plan	12
13. System Security Plan	13
14. System Security Plan	14
15. System Security Plan	15
16. System Security Plan	16
17. System Security Plan	17
18. System Security Plan	18
19. System Security Plan	19
20. System Security Plan	20
21. System Security Plan	21
22. System Security Plan	22
23. System Security Plan	23
24. System Security Plan	24
25. System Security Plan	25
26. System Security Plan	26
27. System Security Plan	27
28. System Security Plan	28
29. System Security Plan	29
30. System Security Plan	30
31. System Security Plan	31
32. System Security Plan	32
33. System Security Plan	33
34. System Security Plan	34
35. System Security Plan	35
36. System Security Plan	36
37. System Security Plan	37
38. System Security Plan	38
39. System Security Plan	39
40. System Security Plan	40
41. System Security Plan	41
42. System Security Plan	42
43. System Security Plan	43
44. System Security Plan	44
45. System Security Plan	45
46. System Security Plan	46
47. System Security Plan	47
48. System Security Plan	48
49. System Security Plan	49
50. System Security Plan	50

## Training Resources



“ Highly effective webinar with a strong overview of organizational needs and AI risk management lifecycle. ”

“ Terrific session on AI Risk Management & HIPAA; valuable insights. ”

“ Educative briefing on AI Risk Management. ”

“ Impressive AI webinar; loaded with pertinent information. ”

“ Excellent content and resources. Educative briefing on AI Risk Management. ”

“ Fantastic presentation with actionable items and resources. ”

“ ecfirst keeps us informed and current with evolving cybersecurity challenges. ”

“ Conversation style, confidence, and passion stood out. ”

“ Excellent knowledge, clear discussions & highly effective webinar. ”

“ Honest, novel insights on AI disruption. ”

“ Instructor brings the latest insights, including AI NIST RMF 100-1. ”

“ Well-organized presentation with impressive subject knowledge. ”



“

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.

”

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.

”

“

Instructor made a complex topic more understandable. Highly recommended.

”

“

Covered important frameworks and laws in cybersecurity.

”

“

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

”

“

Good information and materials to elevate our compliance program.

”

“

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

”

“

A crash course covering cybersecurity assessment, NIST and more.

”

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.

”

“

ecfirst provides clear, actionable recommendations that align with industry best practices.

”

“

Dynamic delivery kept the class interesting.

”

“

The training provided clarity on complex cloud compliance issues.

”

“

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

”

“

The training was point on for the core material.

”

“

Great overview of cloud security with real-world relevance.

”





“

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.

”

Guided us every step of the way  
Always delivered without delays  
HITRUST experience was invaluable  
Appropriate SMEs answered all questions

## 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

“

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

”



## GALEN DATA

“

Thank you for your support and guidance—ecfirst's service is exceptional, and I wouldn't want to go through HITRUST with anyone else.

”



“

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.

”



ecfirst is flexible in addressing HIPAA compliance needs

Professionalism during the HIPAA risk assessment was appreciated

Chosen for their deep commitment to HIPAA and HITECH Act compliance

Excited to collaborate with ecfirst on cyber challenges and HIPAA compliance requirements

## References

A leader in helping hospitals and health systems meet privacy and security regulatory requirements.

Highly recommend ecfirst to covered entities and business associates

A trusted partner focused on long-term, successful relationships

An optimal partner for meeting U.S. federal and state mandates

A trusted partner focused on long-term, successful relationships

**DISCOVERY**  
Behavioral Health





“

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.

”



“

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.

”



“

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

“

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

”

“

Focused materials and explanations were extremely helpful.

”

“

Clear, concise, and professional.

”

“

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

”

“

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

”

“

I valued the practical insights and guidance on CMMC assessment.

”

“

Very comprehensive, detailed, and professional. Absolutely recommend.

”

“

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

“

The CCA program has improved a lot, especially with the web portal and the addition of scenario-based questions that help mimic the real exam.

”

“

Very professional and exceptionally detailed. Empowered and excited.

”

“

Real-world experiences in discussions was awesome.

”

“

Loved the quizzes, real-world examples, and assessment templates.

”

“

Focused materials and explanations were extremely helpful.

”

“

The CCA class was AWESOME. The best class I've taken in 10 years.

”

“

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

”

“

Fantastic training, informative, concise, with helpful resources.

”

“

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

”



# Devoted to Our Clients

Ready to Serve  
The CMMC Ecosystem

Iowa's  
**1<sup>st</sup>**

America's  
**52<sup>nd</sup>**



“

The CMMC CCA Program was an incredibly insightful training experience. I really like the CCA practice tests and the resources available in the CCA Academy Portal, especially the addition of scenario-based questions that help mimic the real exam.

”

**HITRUST**  
Authorized External Assessor

“

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.**

”

Tim Sandberg  
VP of IT Operations | **GALEN DATA**

“

No organization provides the depth of HIPAA expertise and hands-on experience in enabling compliance with regulations as ecfirst, home of the HIPAA Academy.

”

“

ecfirst has consistently delivered high-quality cybersecurity services and compliance solutions.

”

“

ecfirst has been a trusted advisor, ensuring our organization remains compliant and secure.

”





## Get Started



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



[Info@ecfirst.com](mailto:Info@ecfirst.com)



[www.ecfirst.com](http://www.ecfirst.com) | [www.ecfirst.biz](http://www.ecfirst.biz)

