

Program CATALOG



Message from the Chief Executive



Welcome to Pabrai!

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

Why Pabrai?

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 are proud to partner with organizations of all sizes across industries, guided by a single mission: to earn and strengthen 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 **Pabrai DNA** to your success.

Let's make it happen!



Uday Ali Pabrai

Global AI Cyber Defense Thought Leader





Ali Pabrai

Chairman & CEO



Arshiyaan Pabrai

Exec VP & CAIO

Table of Contents



AI	Why Pabrai for AI	5
	Virtual CAIO Program	6
	AI Risk Management Assessment	7
	aiCRP Certification	8
Certification Training	AI HIPAA Cyber Defense	9
	CHP Certification	10
	CSCS™ Certification	11
	CCSA™ Certification	12
	CMMC for Executives	13
HITRUST	Why Pabrai for HITRUST	14
	HITRUST e1 Certification	15
	HITRUST i1 Certification	16
	HITRUST r2 Certification	17
HIPAA	Why Pabrai for HIPAA	18
	Risk Assessment	19
	HIPAA End-User Training	20
NIST	Why Pabrai for NIST	21
	NIST Risk Assessment	22
	NIST Cybersecurity Framework 2.0	23
	NIST SP 800-53 r5	24
	NIST SP 800-171 r2	25
	NIST SP 800-171 r3	26
	NIST SP 800-161 r1	27
Cyber Defense	Cybersecurity Assessment	28
	CloudFirst Assessment	29
	Pen Test	30
	Red Team Exercise	31
	Online Tracking Assessment	32
	Social Engineering	33
	TRACER™ Portal	34
CMMC	Why Pabrai for CMMC	35
	CCP Training	36
	CCA Training	37
	CMMC Advisory Services	38
	CMMC Assessment Process	41
	CMMC Readiness	42
Compliance	Ransomware Readiness BIA DRP	43
	Managed Compliance	44
	On Demand Consulting	45
	VISO & Infosec Staffing Program	46
	PCI DSS Pre-Assessment	47
	GDPR Compliance Pre-Assessment	48
Online Store	Online Store	49
	Toolkits Cyber CMMC HIPAA NIST	50
	Playbooks HIPAA CMMC CAP CUI AI HITRUST	62
	SSP Playbook Template Portal	68
Client References	AI	72
	CHP	73
	CSCS™	74
	CCSA™	75
	HITRUST	76
	HIPAA	77
	CMMC	78
	CCP	79
	CCA	80



AI Governance Methodology

Virtual AI Governance and Risk Management Program

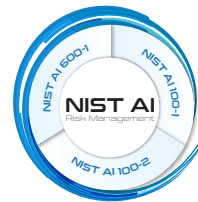
CAIO
Chief Artificial Intelligence Officer



aiCRP
AI Cyber Risk Professional
Online | Self-Paced

AI Cyber Risk Certification Training

AI Governance Reference



AI Governance Playbook



Learn More

AI and Gen AI Governance Playbook

AI Risk Management Assessment
AI Cyber Certification

HITRUST
Authorized External Assessor



AI Toolkit
www.ecfirst.biz/ai



AI Governance Methodology

Virtual AI Governance and Risk Management Program

CAIO
Chief Artificial Intelligence Officer



aiCRP
AI Cyber Risk Professional
Online | Self-Paced

AI Cyber Risk Certification Training

AI Governance Reference



AI Governance Playbook



Learn More

AI and Gen AI Governance Playbook

AI Risk Management Assessment
AI Cyber Certification

HITRUST
Authorized External Assessor



AI Toolkit
www.ecfirst.biz/ai



AI Governance Methodology

Virtual AI Governance and Risk Management Program

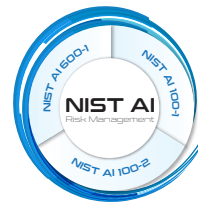
CAIO
Chief Artificial Intelligence Officer



aiCRP
AI Cyber Risk Professional
Online | Self-Paced

AI Cyber Risk Certification Training

AI Governance Reference



AI Governance Playbook



Learn More

AI and Gen AI Governance Playbook

AI Risk Management Assessment
AI Cyber Certification

HITRUST
Authorized External Assessor



AI Toolkit
www.ecfirst.biz/ai

AI Governance

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

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

Customized

Flat Rate

Fixed Cost

Flexible

AI Governance Program



AI Risk Management Assessment



1



2



3



NIST AI 100-1 • ISO 23894 • ISO 42001

AI Risk Assessment



Organization Questionnaire



Scoping Questionnaire



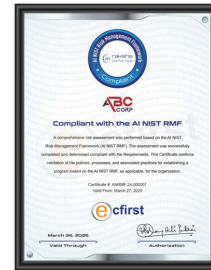
Policy



Assessment



Report Dashboard

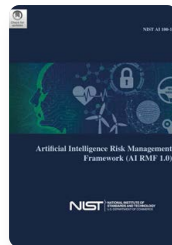


Certificate

Sources



ISO 23894



NIST AI 100-1



ISO 42001

AI

Certification
Training

HITRUST

HIPAA

NIST

Cyber
Defense

CMIMC

Compliance

Online
Store

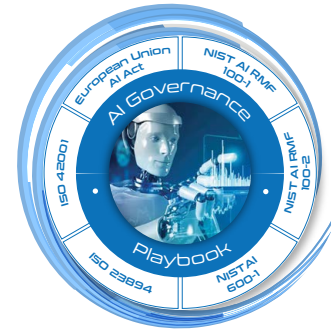
Client
Reference

The Industry's First AI Cyber Risk Management Training Program



AI Governance Risk Management Playbook

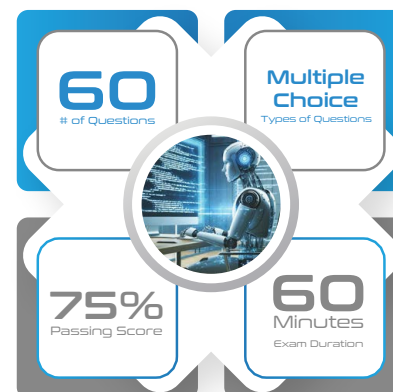
Gen AI Playbook



What's in it for you?

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

AI Exam Specifications



Digital Badge

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





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



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



An Executive CMMC Program

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



Healthcare Industry's First & Leading HIPAA Credential



HIPAA Playbook



What's in it for you?

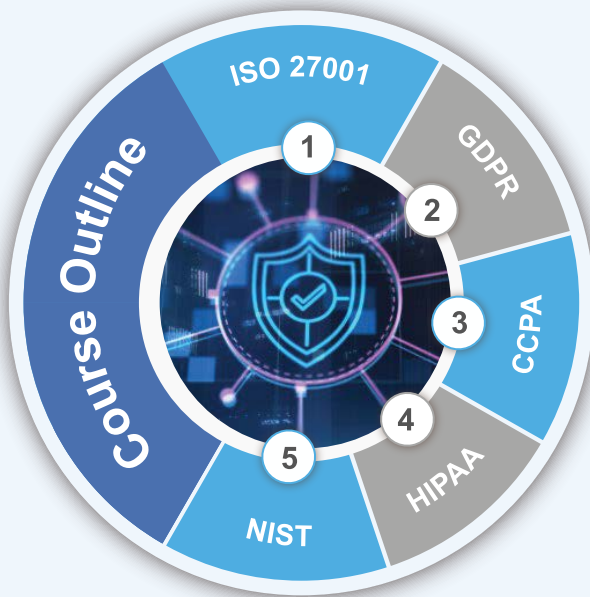
- ✦ Analyze the latest updates in HIPAA Privacy, HIPAA Security, and HITECH Breach mandates
- ✦ Examine OCR HIPAA settlements to understand the bar for HIPAA compliance
- ✦ Review HIPAA compliance challenges and best practices for Covered Entities and Business Associates
- ✦ Understand HIPAA Safe Harbor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

Digital Badge

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



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

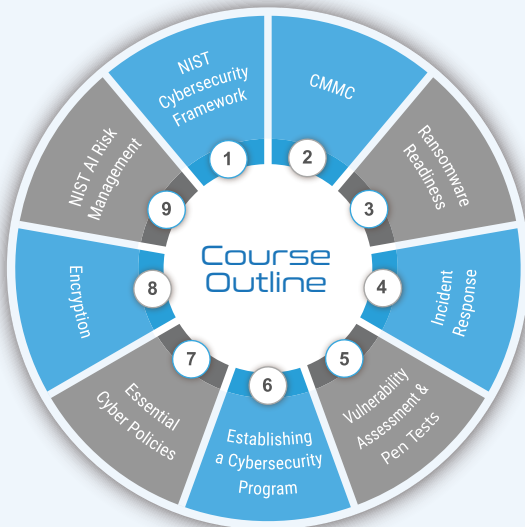
Digital Badge

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



Virtual | Online

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.





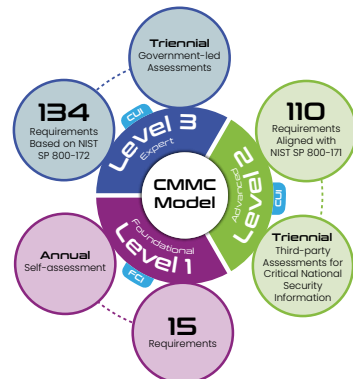
Learning Objectives

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



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

CMMC
Playbook

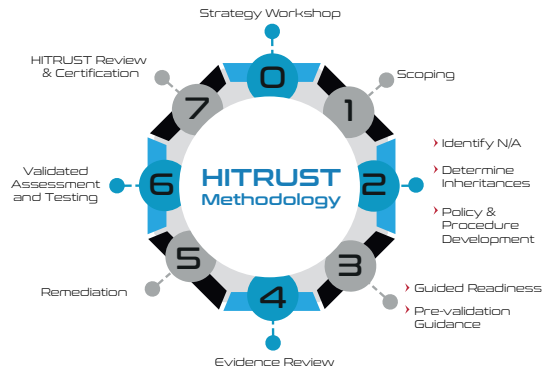


CMMC
For Management



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

Signature Methodology



Devoted to Client Success

HITRUST Assessor Council

Member, AI Committee

HITRUST Commitment

COLLABORATE²⁴
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



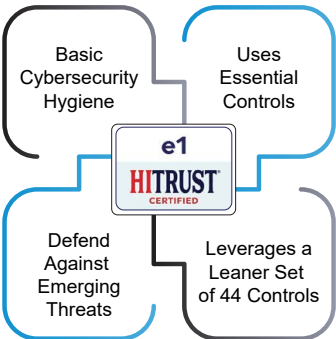
Monthly Payment

Multi year Engagement

Flat Price

e1 Essentials

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



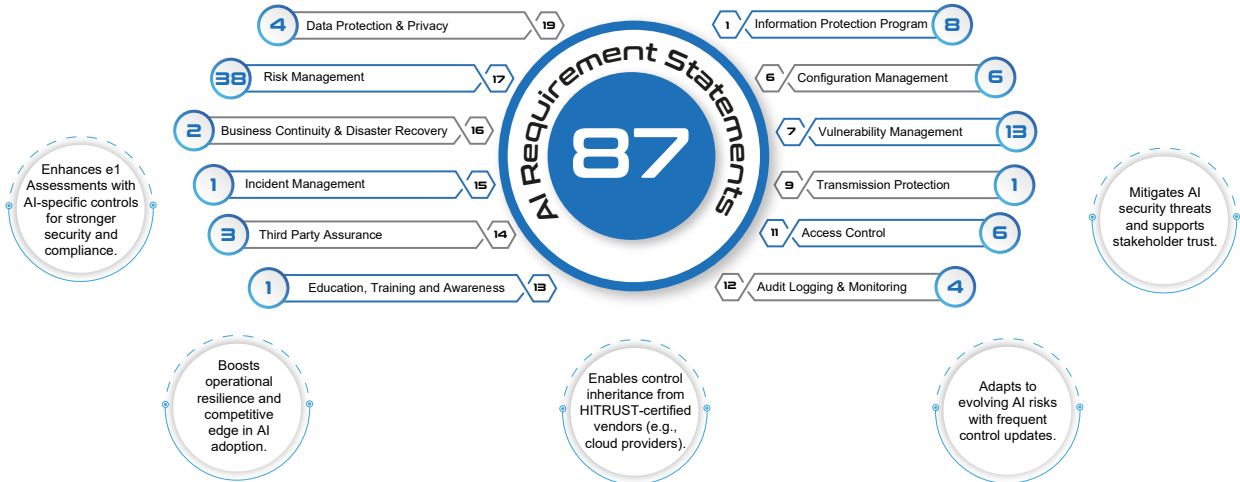
HITRUST e1 and HIPAA

- ✖ 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.

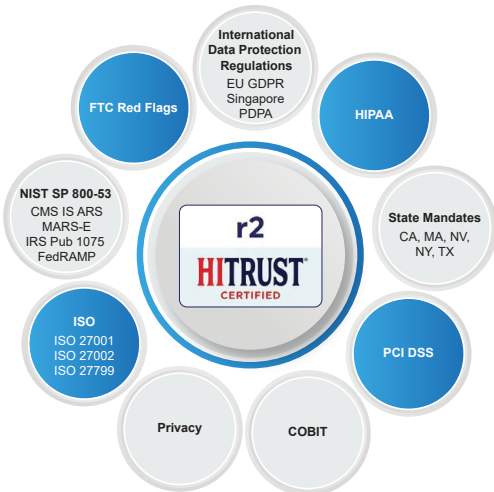
Assessment object auto-generated in MyCSF, with a **30-day** planning period and a **90-day** fieldwork period.



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



HITRUST AI Risk Requirements



HITRUST AI Cybersecurity Requirements



HIPAA

Why Pabrai?



HIPAA Signature Methodology

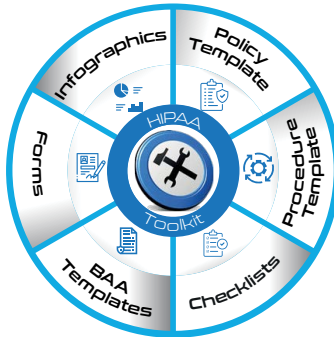
Industry Leading HIPAA Certification Training
Updated with NPRM

CHP Certified HIPAA Professional
HIPAA Academy



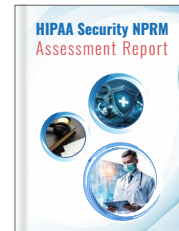
Delivering HITRUST Certification Since 2016

AI Powered HIPAA Playbook



HIPAA Toolkit
www.ecfirst.biz

HIPAA NPRM Assessment



HIPAA Compliance Attestation

AI

Certification Training

HITRUST

HIPAA

NIST

Cyber Defense

CMIMC

Compliance

Online Store

Client Reference

Risk Assessment

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



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

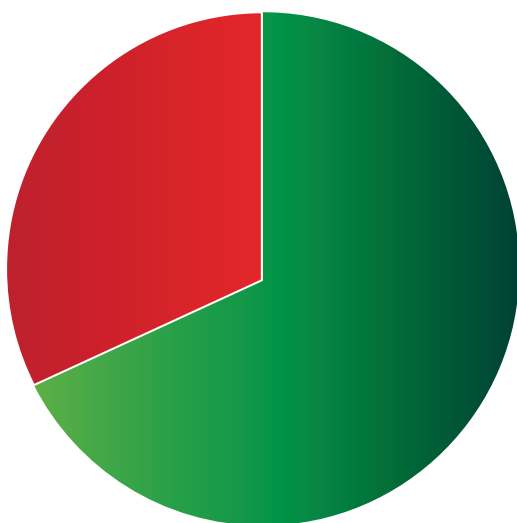
Grade	Security Rule
D	Administrative Safeguards
F	Physical Safeguards
A	Technical Safeguards
B	Organizational Requirements
F	Policies, Procedures, and Documentation
Privacy Rule	
B	Administrative Requirements
A-	Uses and Disclosures
Breach Notification	
C	Reporting

Signature Methodology

HIPAA * NIST

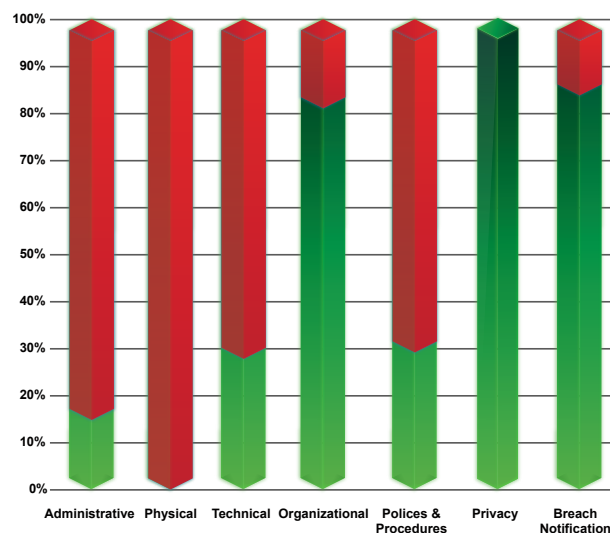


Compliance Status



■ 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 Threat

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

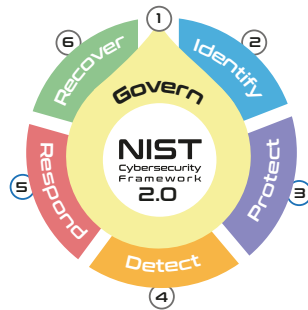
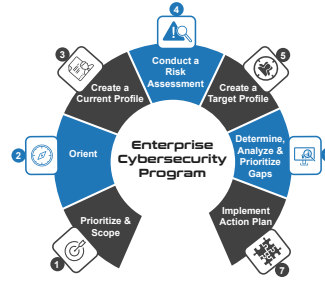
4 HITECH Breach Start

5 Cybersecurity Fundamentals Start

6 Appendix A: Acronyms Start

7 Appendix B: Glossary Start

NIST Signature Methodology



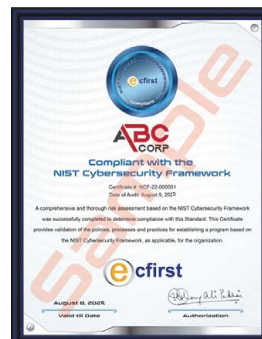
NIST 2.0 Assessment

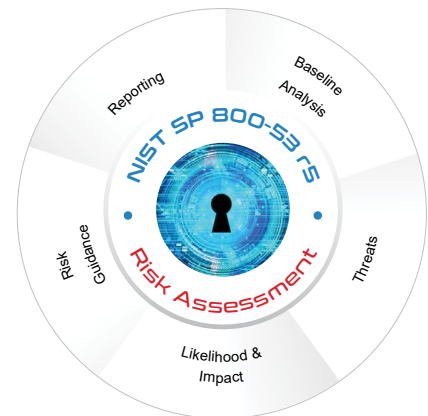
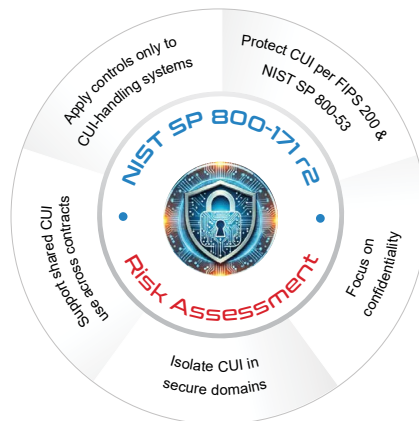
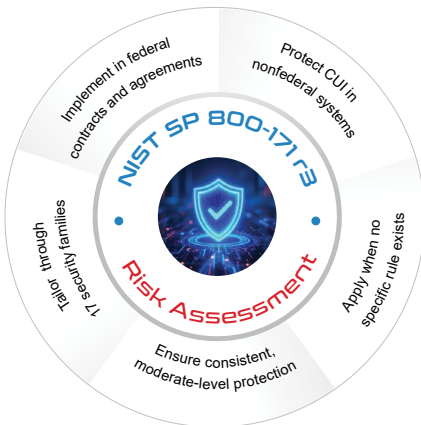
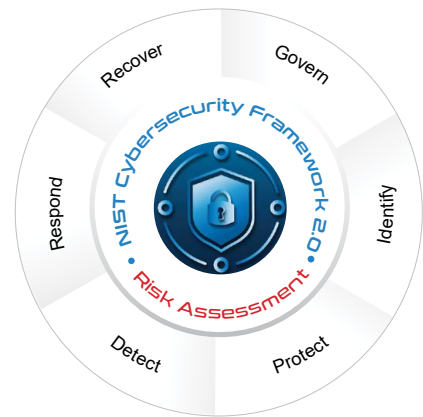
Industry Leading Cybersecurity Certification Training

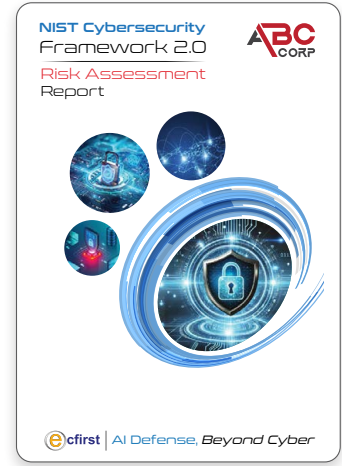
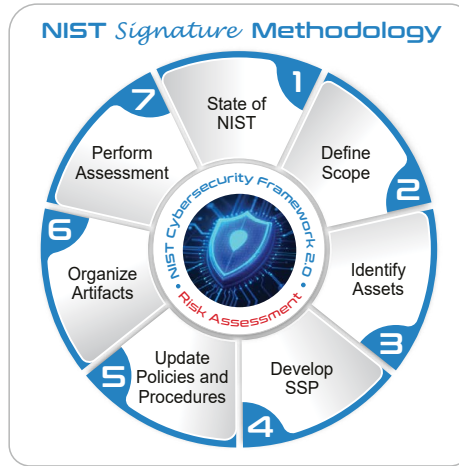
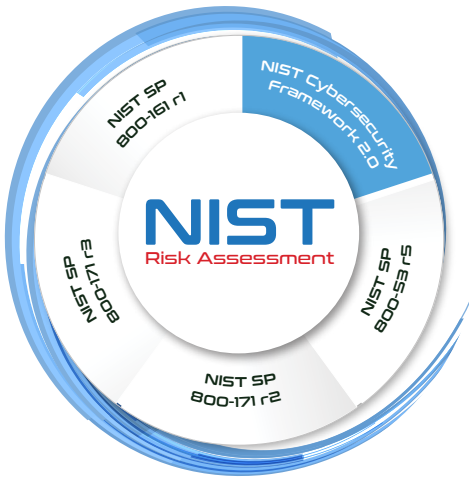


NIST Risk Assessment Report

NIST Compliance Attestation







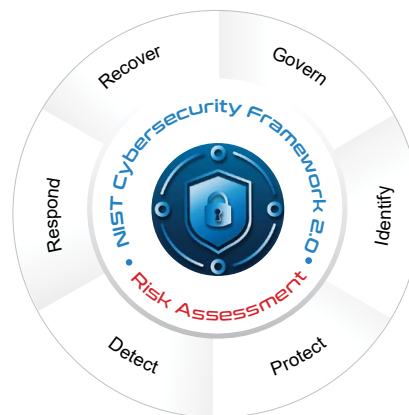
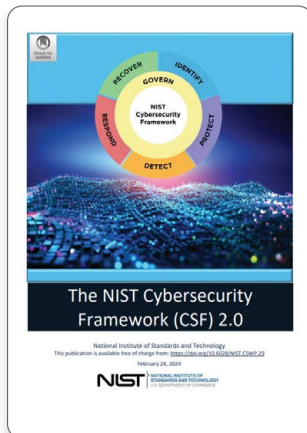
NIST Cybersecurity Framework 2.0 Risk Assessment Portal

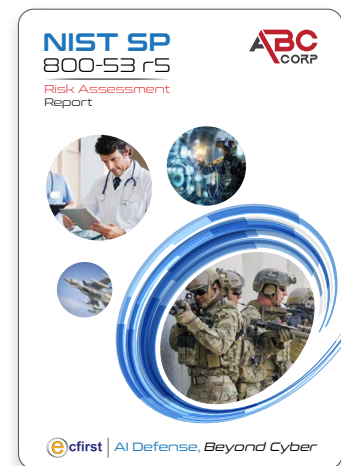
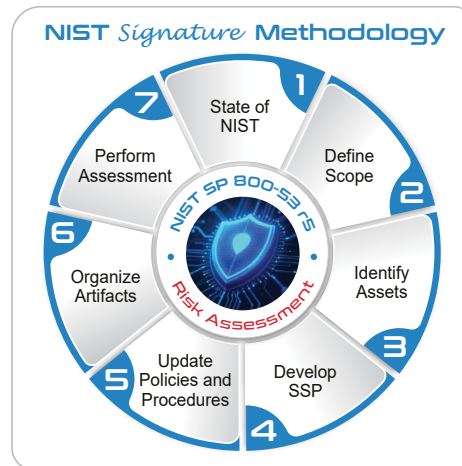


NIST Cybersecurity Framework 2.0

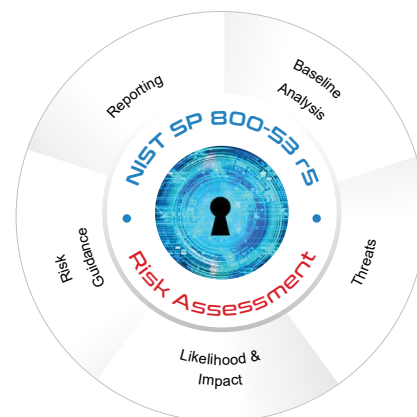
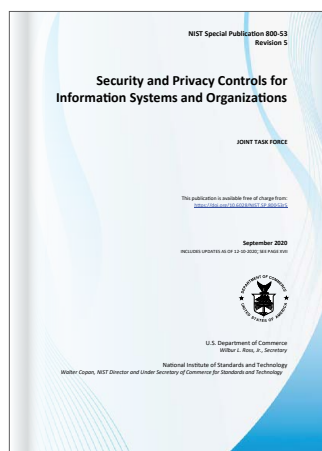
Back

Home / Data Collection Forms / NIST Cyber Security Framework 2.0 / Phase 1 - Planning

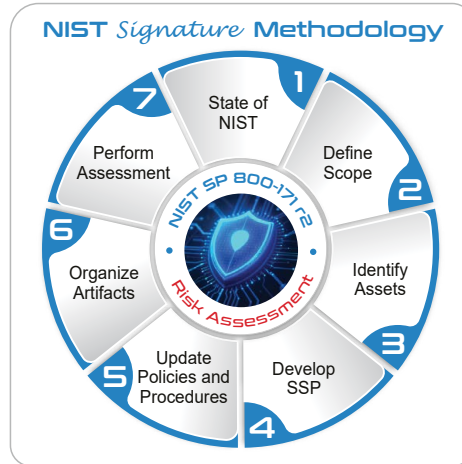




NIST SP 800-53 r5 Risk Assessment Portal



NIST SP 800-171-r2 Risk Assessment



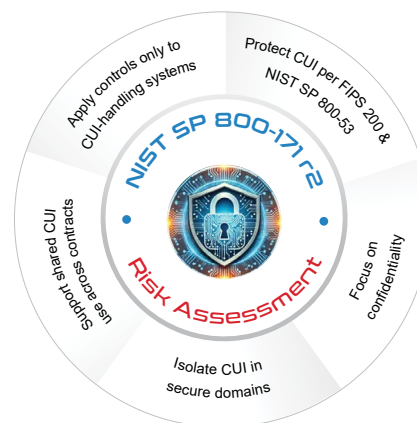
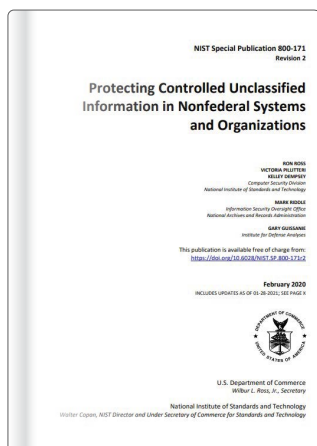
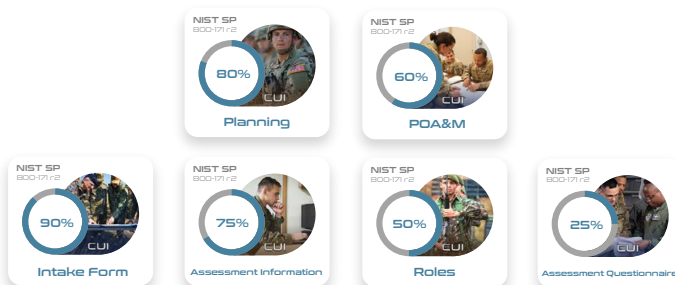
NIST SP 800-171 r2 Risk Assessment Portal



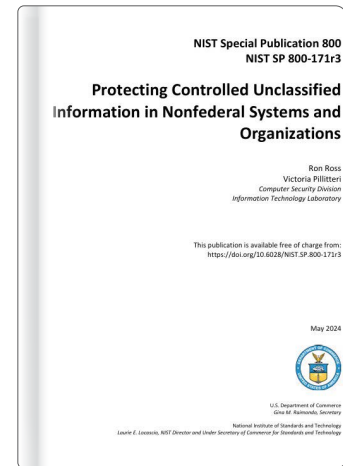
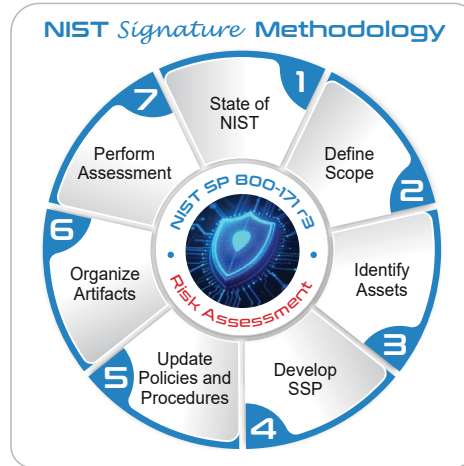
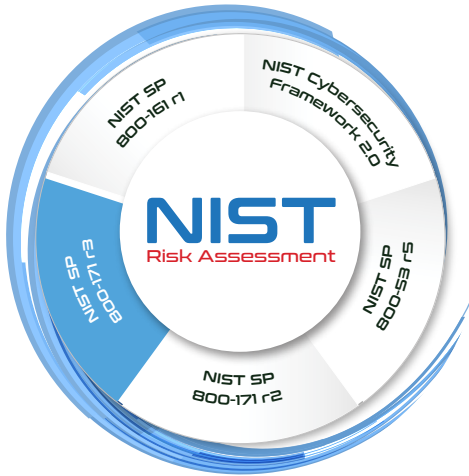
NIST SP 800-171r2

Back

Home / Data Collection Forms / NIST SP 800-171r2 / Phase 1 - Planning



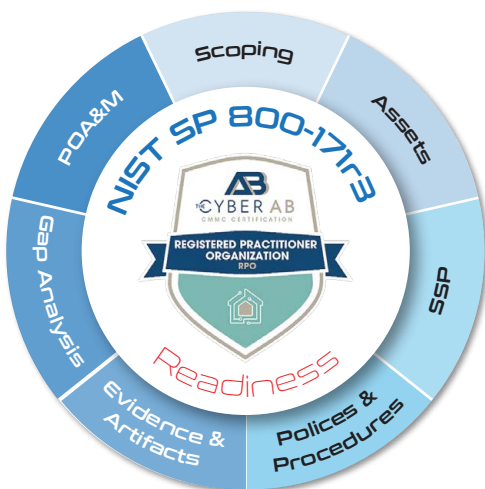
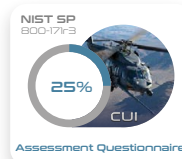
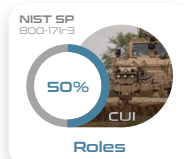
NIST SP 800-171-r3 Risk Assessment

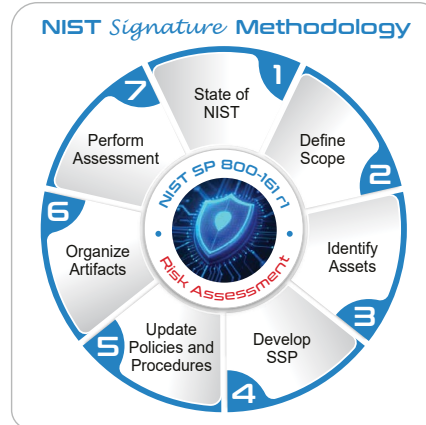


NIST SP 800-171r3 Risk Assessment Portal | ABC CORP

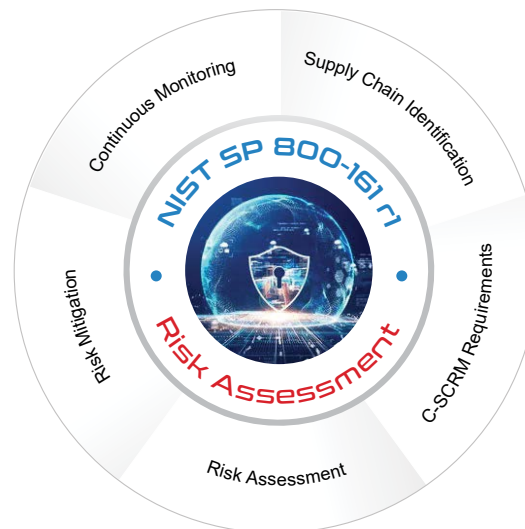
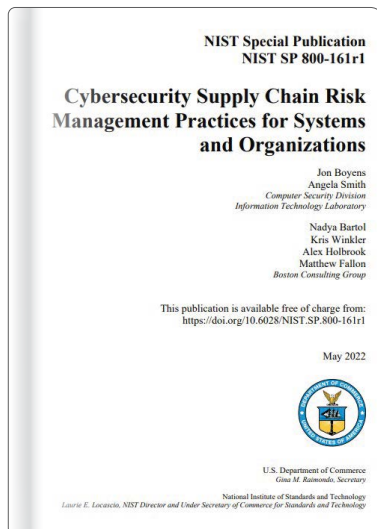
NIST SP 800-171r3

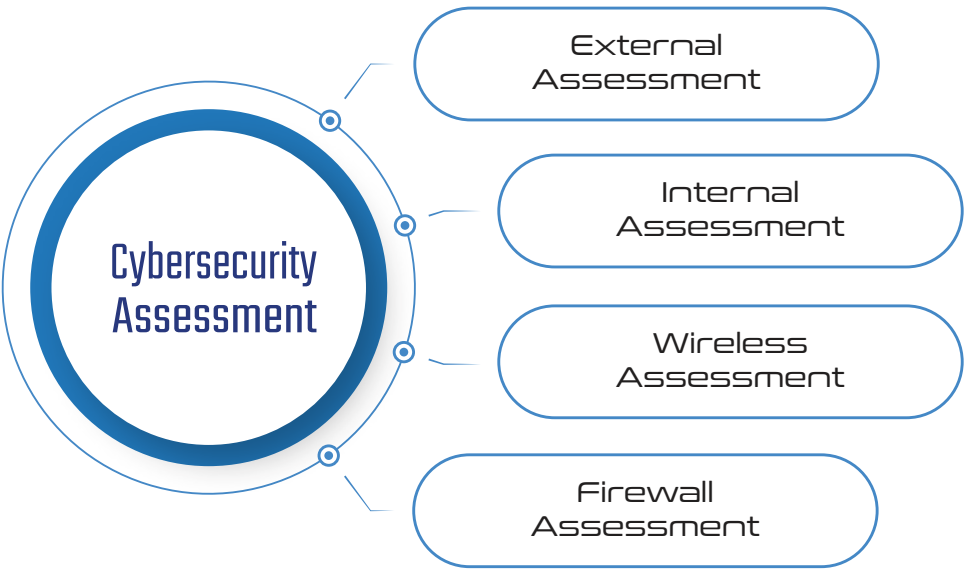
Home / Data Collection Forms / NIST SP 800-171r3 / Phase 1 - Planning





NIST SP 800-161 r1 Risk Assessment Portal





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 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

Compliance Status Example



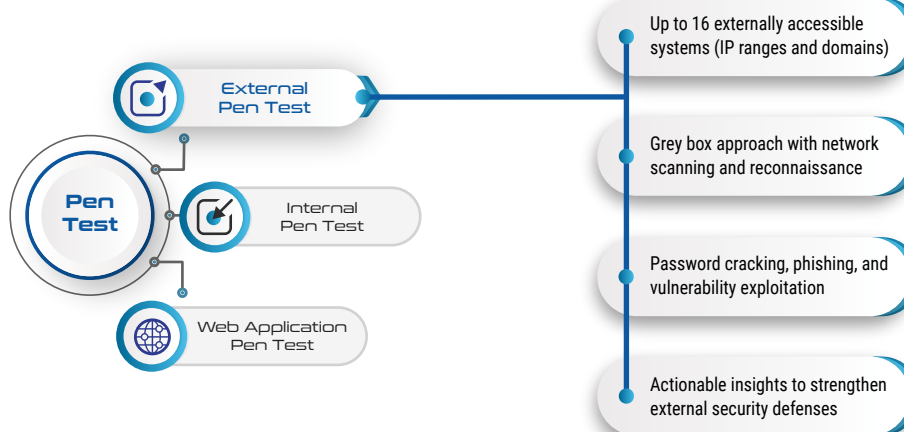
Compliant Not Compliant N/A

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

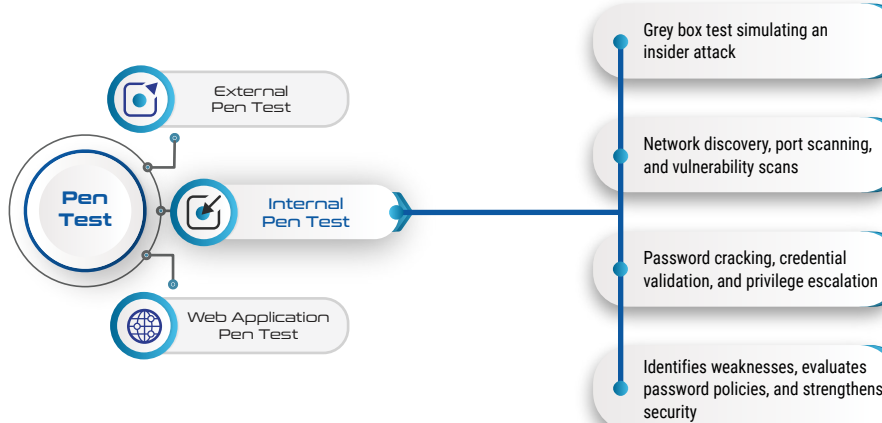
Significant Findings



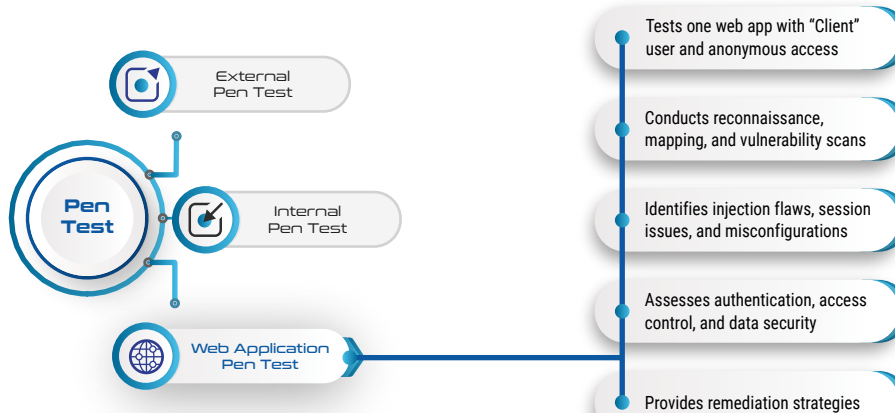
External Pen Test

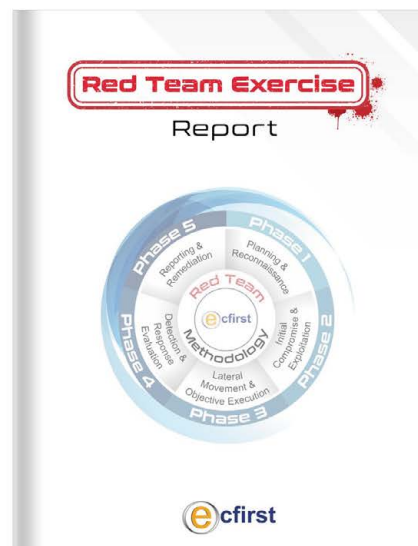
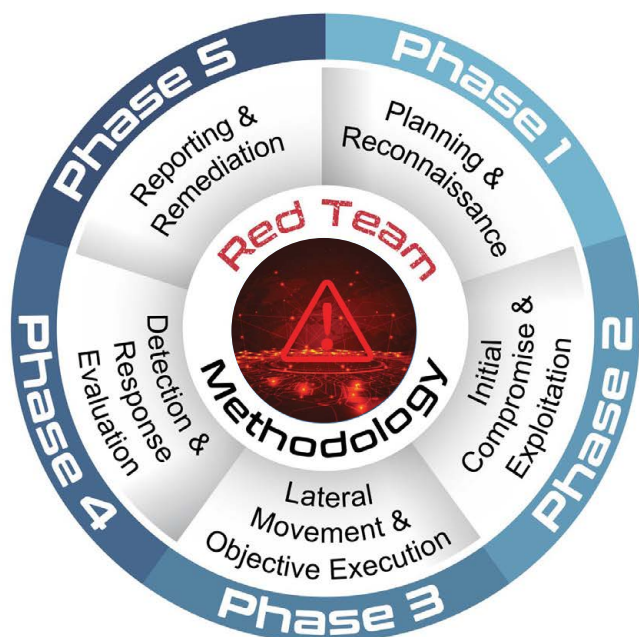


Internal Pen Test



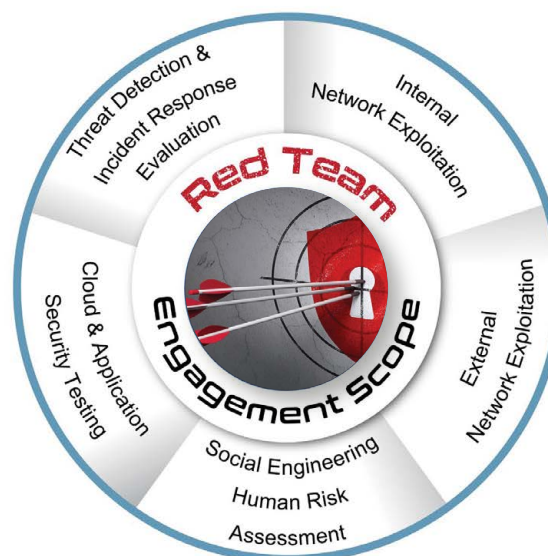
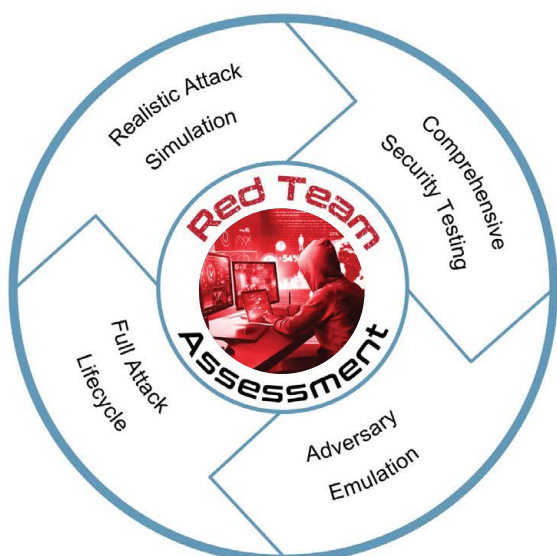
Web Application Pen Test



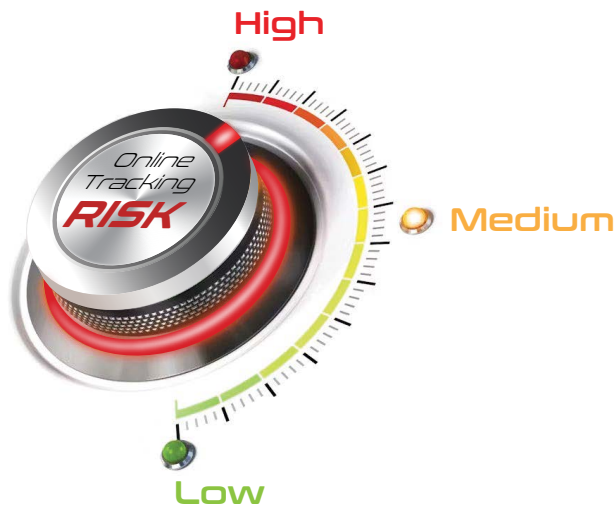


Red Team Exercise

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

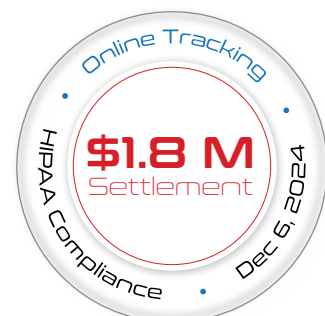
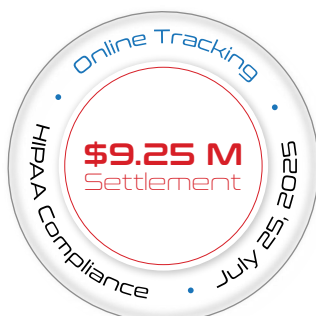


Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates

“

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.

”



- ✘ 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

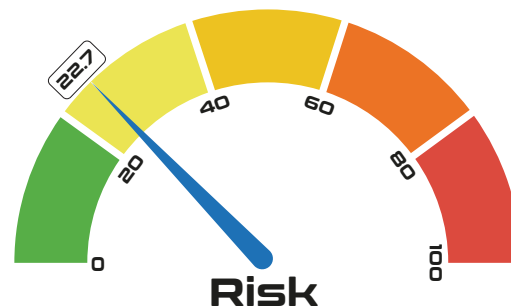
Campaign Start Date	Number of Phishing Victims
Dec 6, 2021	11

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:

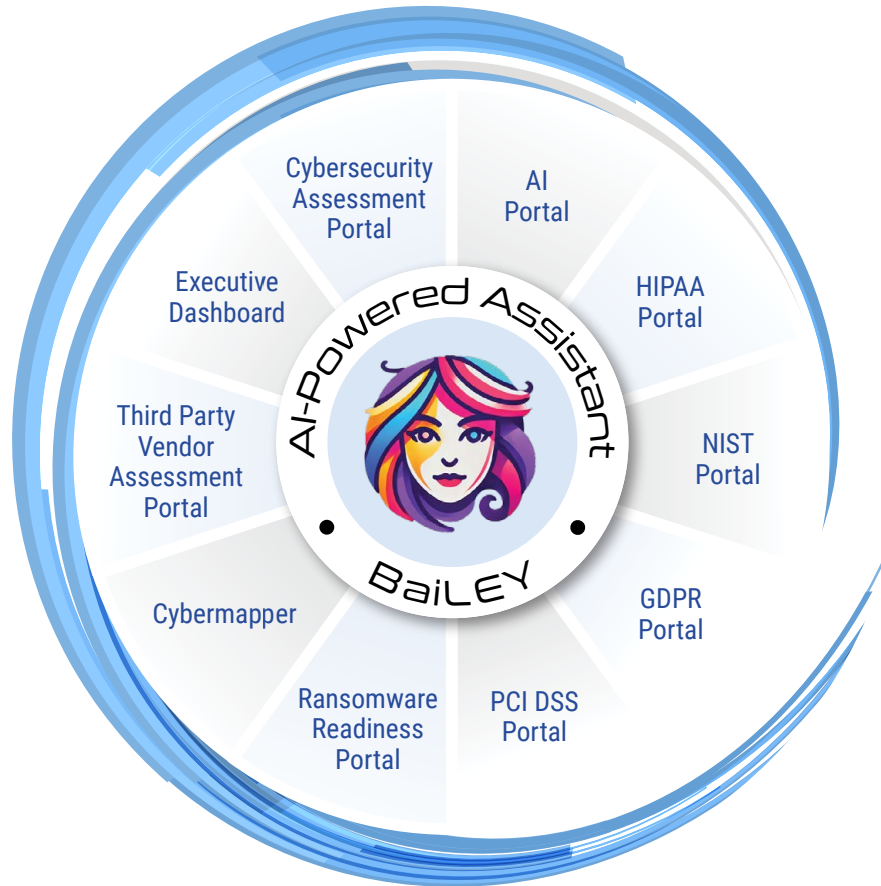
From: C. Spelling <corey.spelling@marketplace-gov.net>
 Reply-To: C. Spelling <corey.spelling@marketplace-gov.net>
 Subject: Health insurance
 @ 2017HealthInsurance.pdf

Dear ,

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

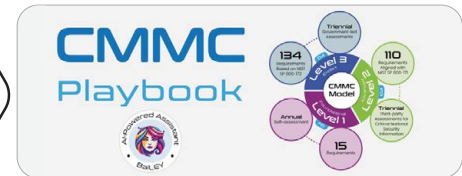
Please look over it and let us know if you have questions.

Best Wishes,
 Corey Spelling



Credentialed Staff

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 Pabrai CCP Academy! I appreciated my ecfirst experience."



CCA Reference

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



CMMC Readiness Mock Assessment



DoD CMMC Certification Training Content
 Approved and Authorized

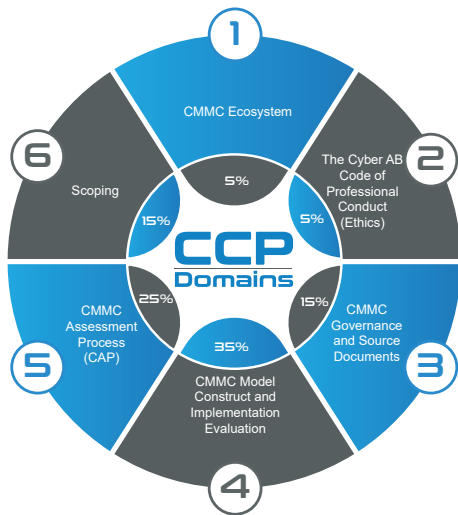
DoD CMMC Certification Training Provider
 Approved and Authorized



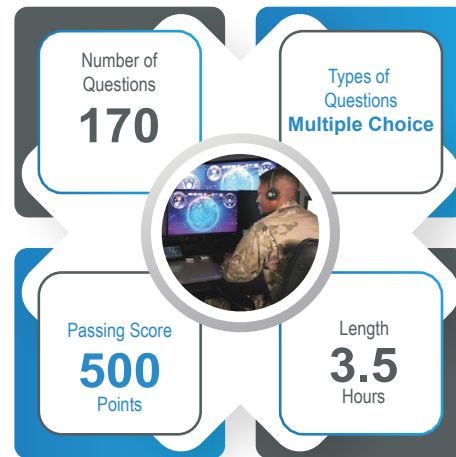
Summary

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.

CMMC Certified Professional (CCP)



CCP Exam Specifications



This is not an open book exam

Intended Audience

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

Domain Exam Weight

#	Domain	Exam Weight	CCP Program	Hours
1	CCP Pre Program Prep			2
2	CMMC Ecosystem Blueprint Domain 1	5%		
3	The Cyber AB Code of Professional Conduct (Ethics) Blueprint Domain 2	5%	Domain 1, 2 & 3 Tuesday, Day 1 8:30 am - 4:30 pm Offline Prep: 2 Hours	10
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			

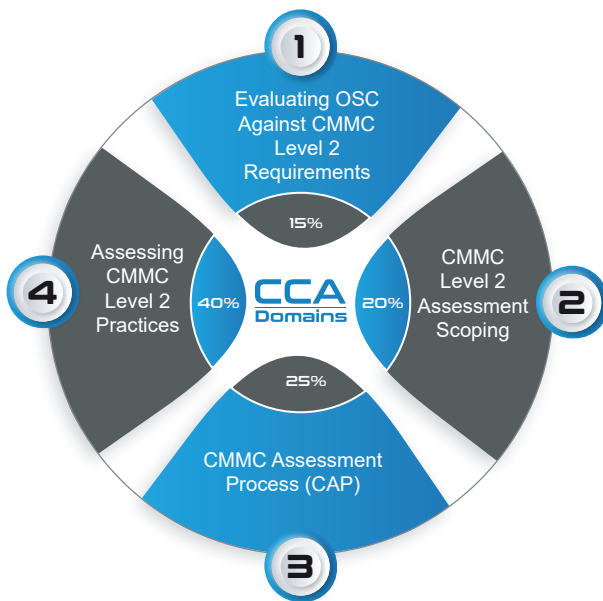
Client Reference

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

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%	Domain 3 Wednesday, Day 2 8:30 am - 4:30 pm Group Exercises: 7 35 Minutes Offline Prep: 2 Hours	10
4	CMMC Assessment Process (CAP) Blueprint Domain 3	25%	Domain 4 Thursday, Day 3 8:30 am - 4:30 pm Group Exercises: 10 60 Minutes Offline Prep: 2 Hours	10
5	Assessing CMMC Level 2 Practices Blueprint Domain 4	40%	Review and Final Quiz Friday, Day 4 8:30 am - 12:30 pm	4
6	Practice Exam & Review			

Intended Audience

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

Client Reference

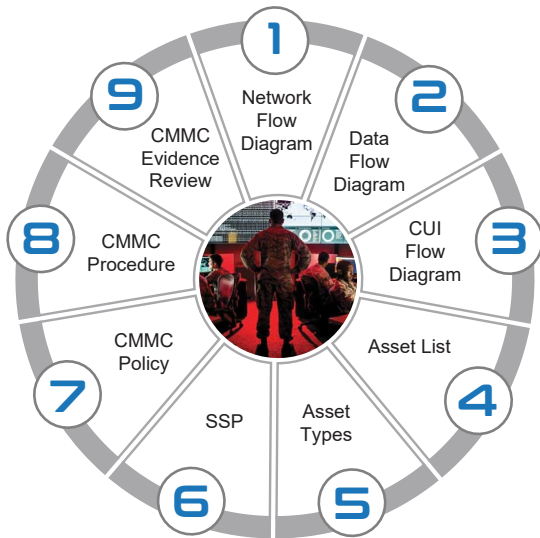
“

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

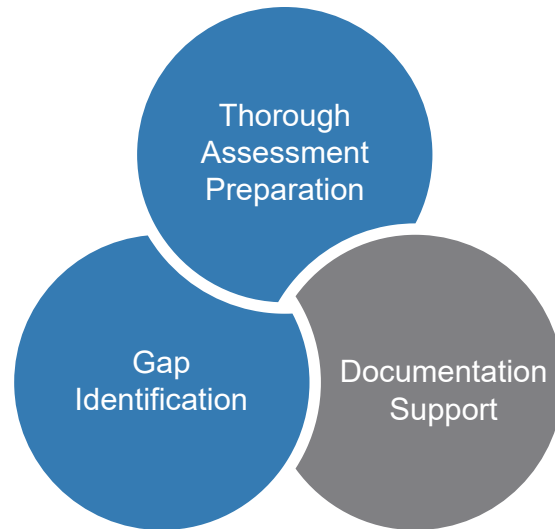
Practical, real-world CMMC assessment Scenarios presented, including insight on a credible SSP.

”

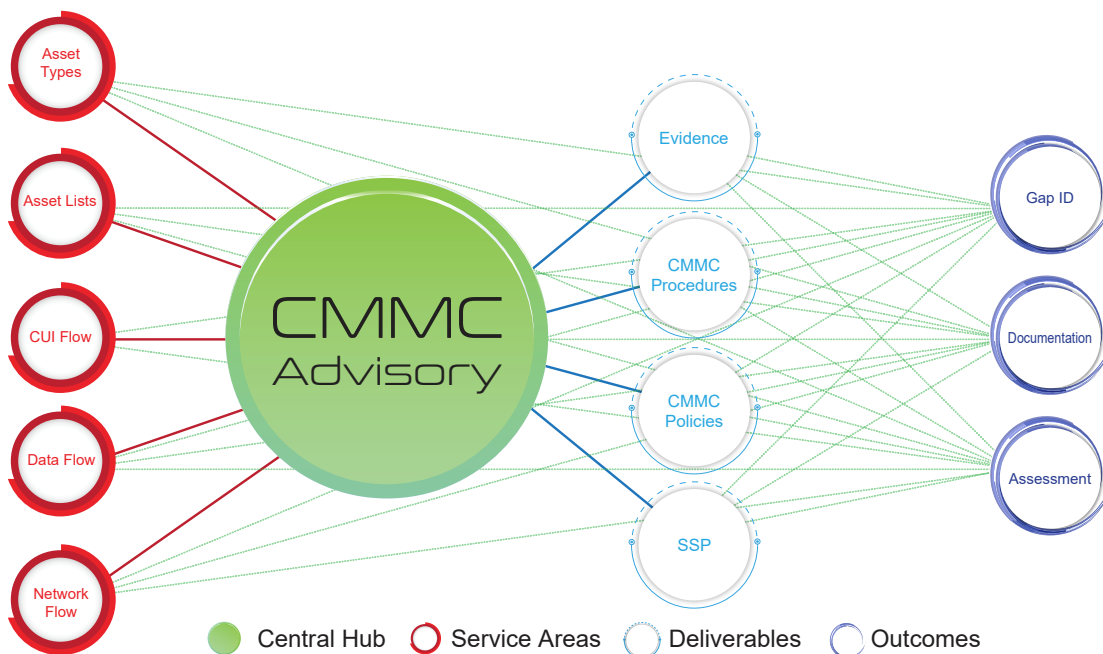
Advisory Guidance



Compliance Support



CMMC Advisory Services Flow





Purpose

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

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

Submit Annual Affirmation in SPRS

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

Validate Continuous Compliance

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

Executive Review & Affirmation

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

Creates legal accountability
False declaration carries liability

Confirm No Significant Changes

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

Material changes may require a new assessment

Review POA&M Status (if Applicable)

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

Conditional Level 2 must reach Final status

Verify Control Effectiveness

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





Purpose

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

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

Submit Annual Affirmation in SPRS

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

Validate Continuous Compliance

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

Executive Review & Affirmation

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

Creates legal accountability
False declaration carries liability

Confirm No Significant Changes

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

Material changes may require a new assessment

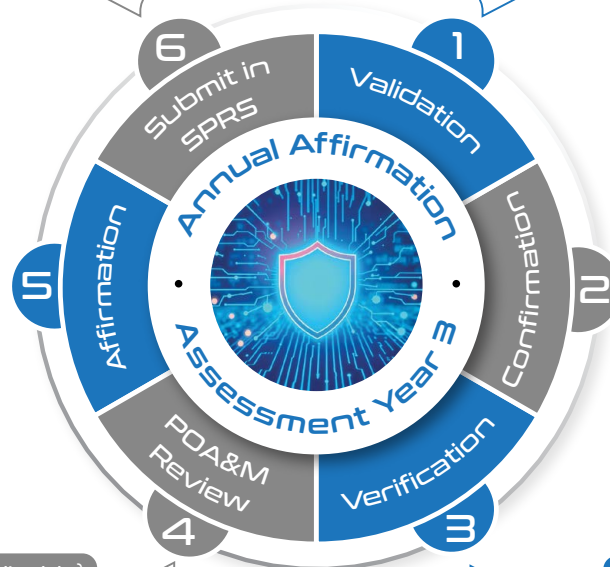
Review POA&M Status (if Applicable)

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

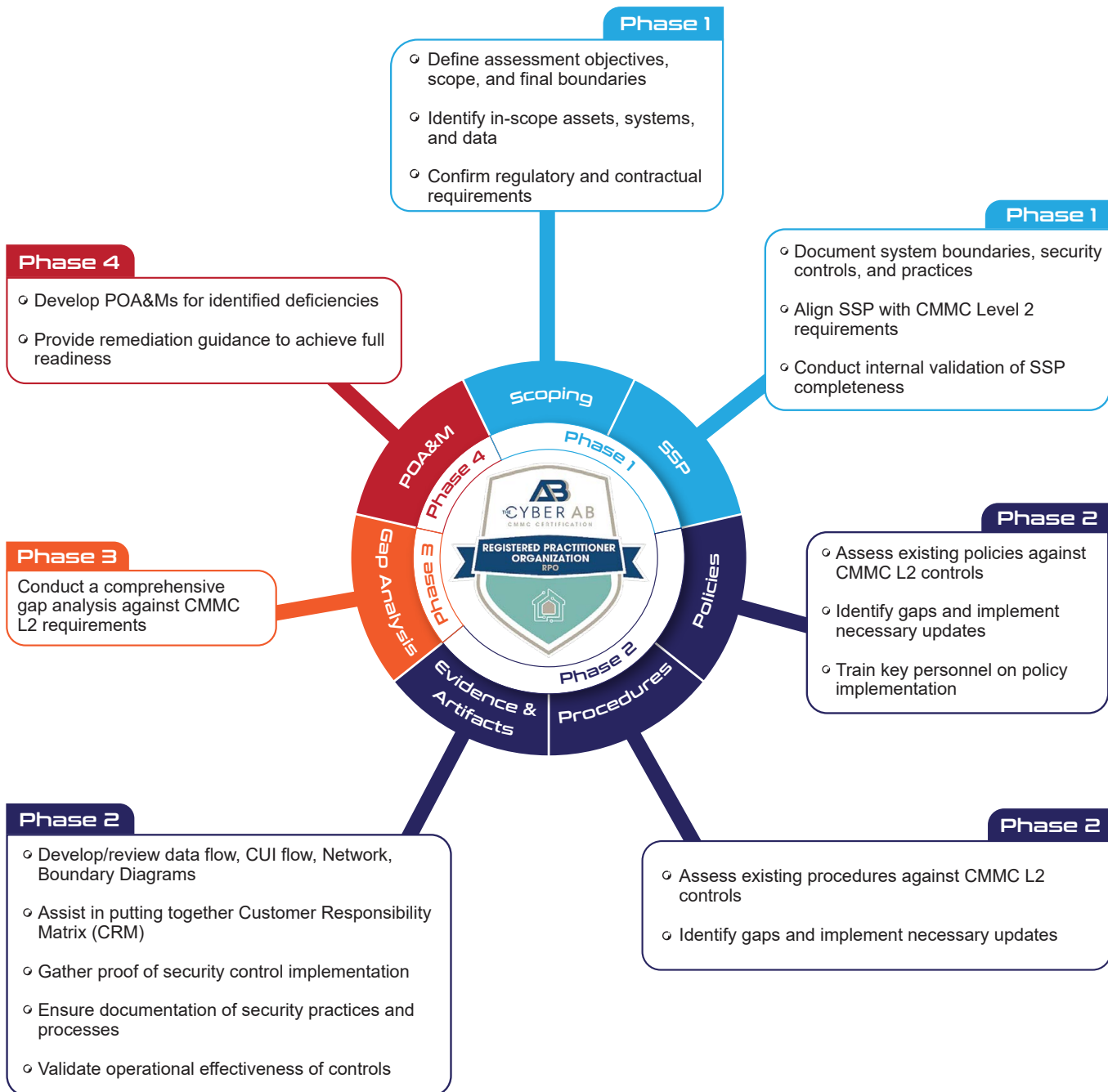
Conditional Level 2 must reach Final status

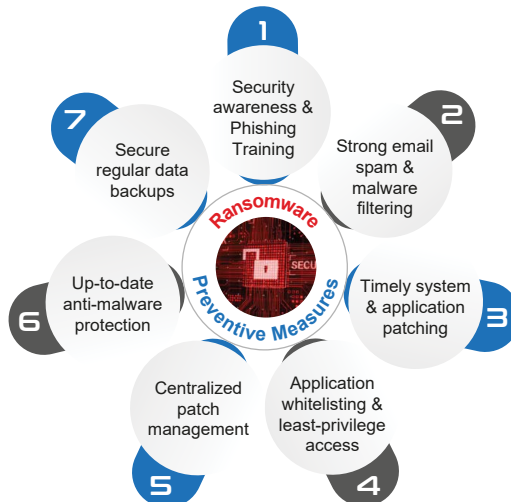
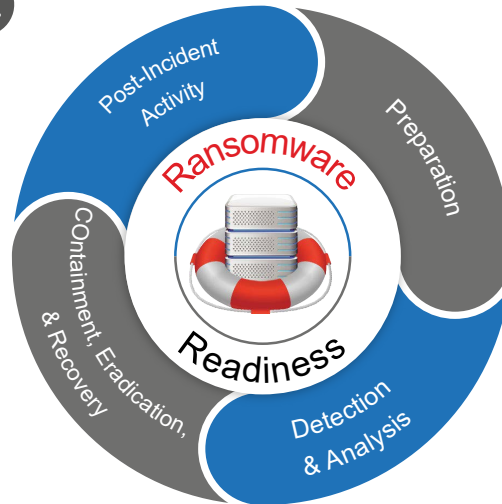
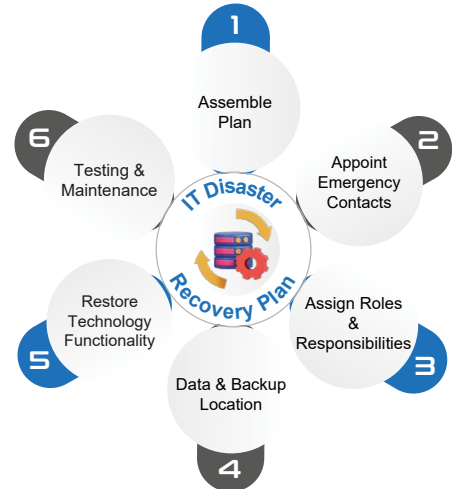
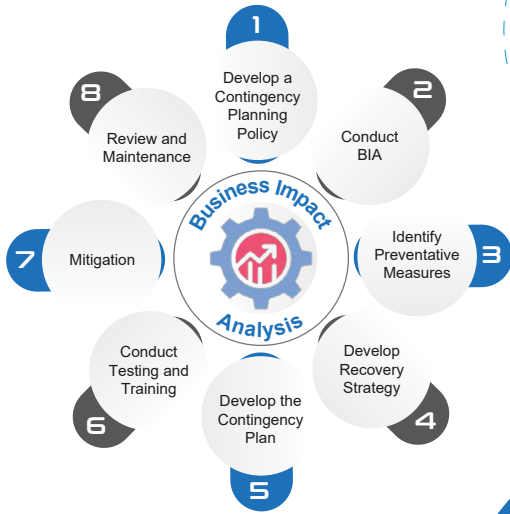
Verify Control Effectiveness

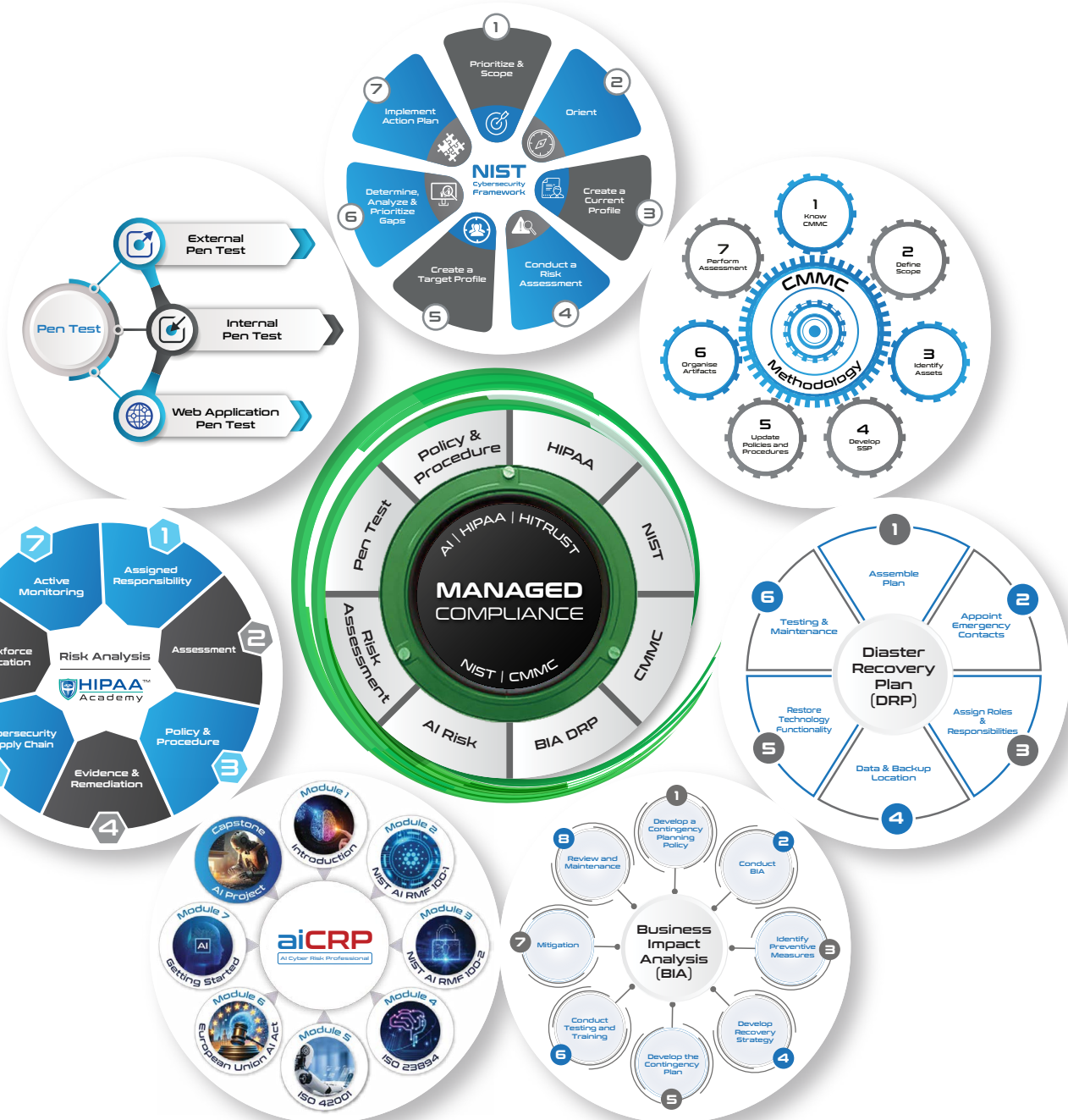
- Controls must be:
 - Implemented
 - Operating effectively
 - Continuously maintained
- Review supporting evidence:
 - Monitoring / SIEM logs
 - Access control enforcement
 - Incident response records
 - Training records











On Demand (OD)

Fixed-rate

Expert Advisors

No Long-term Commitment

Short Term Consulting

Pen Test

ON DEMAND
AI | 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

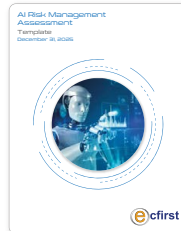
Compliance Solutions

IT Disaster Recovery Plan

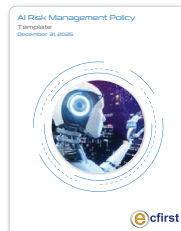
Social Engineering

Business Continuity

AI Cyber Program



Policies and Procedures



AI

Certification
Training

HITRUST

HIPAA

NIST

Cyber
Defense

CMMC

Compliance

Online
Store

Client
Reference

VISO & InfoSec Staffing Program



AI

Certification Training

HITRUST

HIPAA

NIST

Cyber Defense

CMMC

Compliance

Online Store

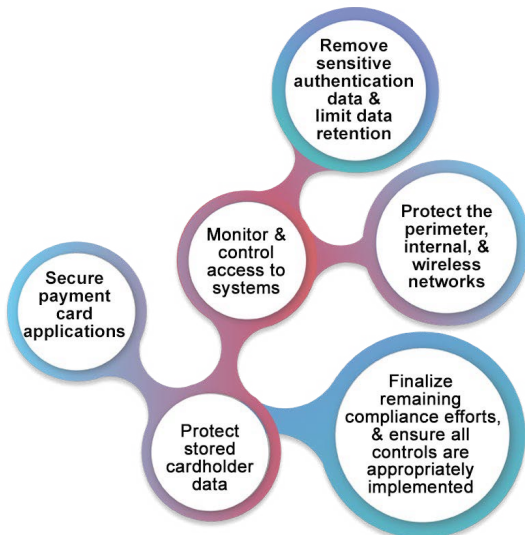
Client Reference

PCI DSS Readiness Assessment

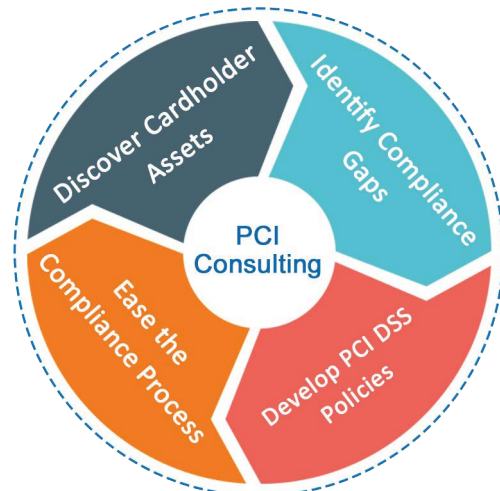
- ❖ Review of compliance against PCI DSS v4.0 requirements
- ❖ Identify gaps & risks in protecting cardholder data
- ❖ Deliver actionable assessment report with findings
- ❖ Provide prioritized remediation plan & timeline
- ❖ Executive summary for leadership & stakeholders



PCI DSS Goals



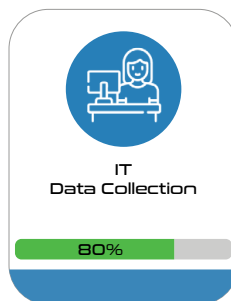
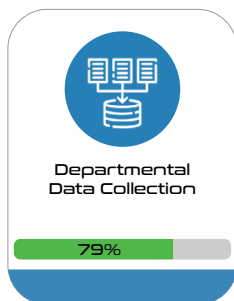
PCI Consulting



PCI DSS Portal

TRACERSM
ASSET RISK MANAGEMENT

ABC
CORP



PCI DSS



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



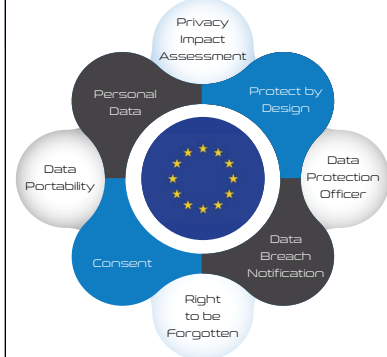
GDPR: Who, What, Why?

- ✘ 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

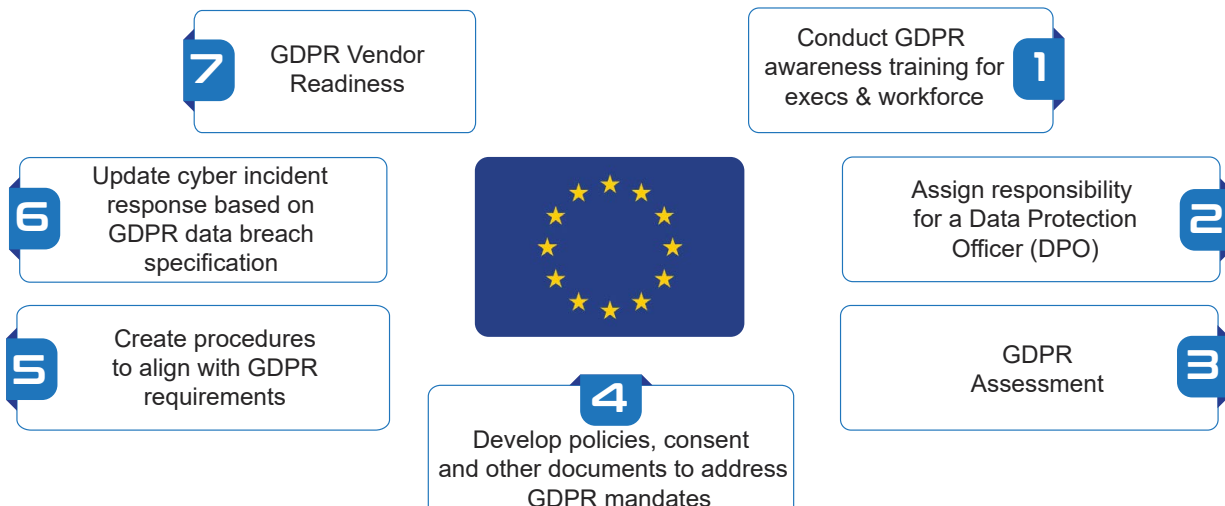
GDPR Signature Methodology

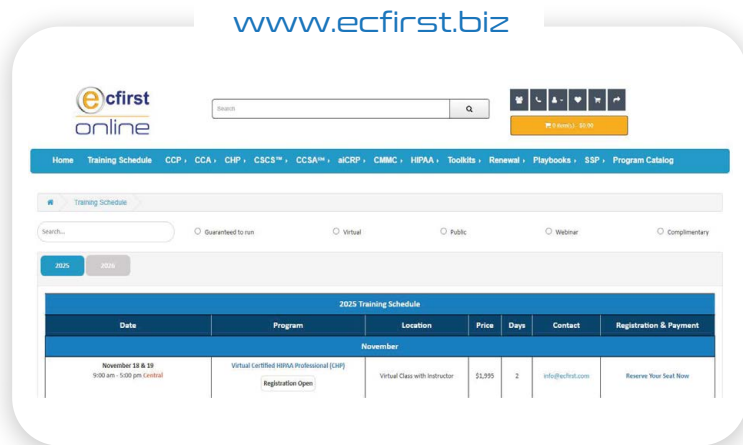


Purpose & Scope



Establish a Credible GDPR Program

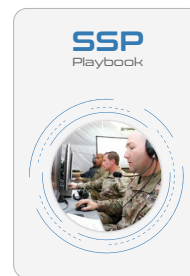
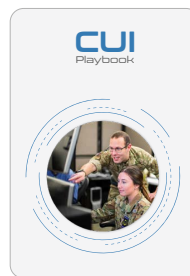
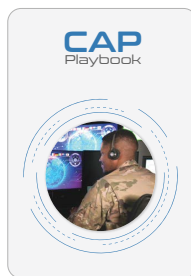
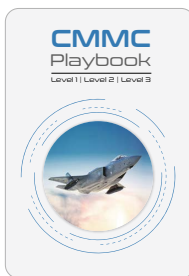
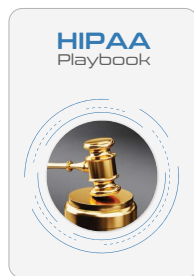




Training



Playbooks



Templates

CMMC

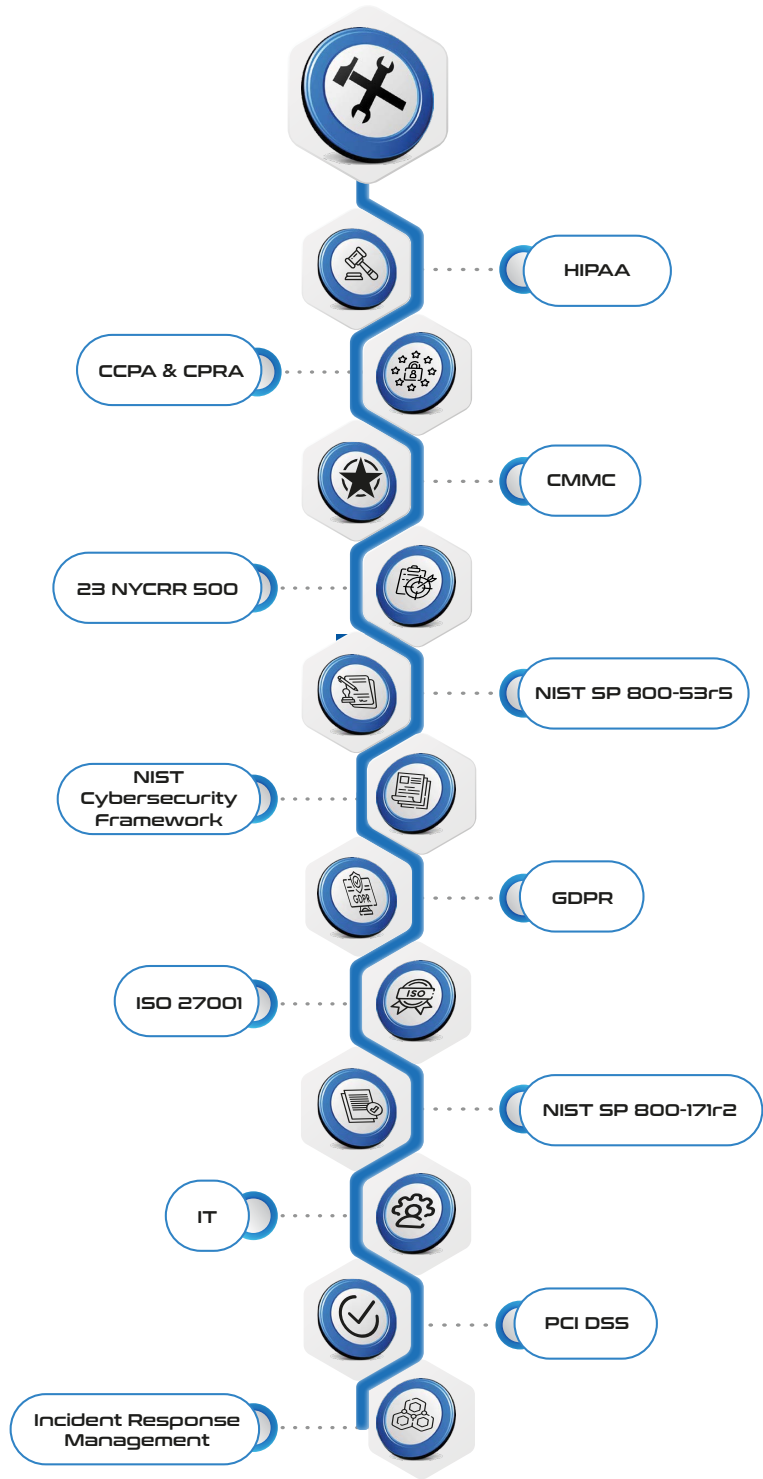
HIPAA

GDPR

NIST

SSP

Toolkit Packages



Components





Quick Links

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

CMMC

Level 1

Playbook





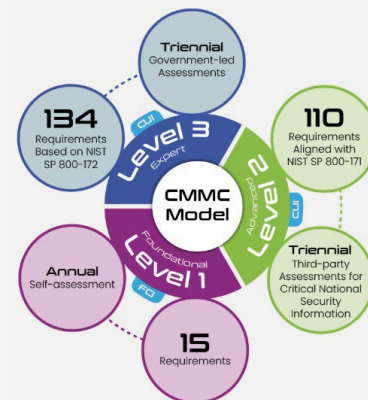
Quick Links

- [Home](#)
- [CMMC Final Rule](#)
- [CMMC Level](#)
- [CMMC Domains](#)
- [Domains/Roles/Topics](#)
- [CMMC Training](#)
- [Source Documents](#)
- [Getting Started with CMMC](#)
- [DoW CUI Mandatory Training](#)
- [CMMC Ecosystem](#)
- [CMMC News](#)

CMMC

Level 2

Playbook





Home Course Access My Dashboard karthick

Quick Links

- Home
- CMMC Level
- CMMC Domains
- Domains/Roles/Topics
- CMMC Final Rule
- CMMC Documents
- CMMC Source Documents
- NIST Resources
- NIST Cybersecurity Supply Chain Risk Management References
- CMMC SSP Sample
- CMMC Toolkits

CMMC

Level 3

Playbook

The diagram shows the CMMC Model with three levels of requirements:

- Level 1 (Foundational):** 15 Requirements
- Level 2 (Advanced):** 110 Requirements Aligned with NIST SP 800-171
- Level 3 (Expert):** 134 Requirements Based on NIST SP 800-172

Additional assessments are shown:

- Annual Self-assessment** (linked to Level 1)
- Triennial Government-led Assessments** (linked to Level 3)
- Triennial Third-party Assessments for Critical National Security Information** (linked to Level 2)

Home



CMMC 2.0 Level 1 Self-Assessment

Back

Phase 1

Planning

Phase 2

Questionnaire

Phase 3

Verification

Phase 4

Generate Report



Dashboard



CMMC Level 1 Playbook



Phase 1 Planning



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

Back



Intake Form

100%



Client Information

87.1%



Roles

93.8%



SSP Scope Document



General Questionnaire

25%

Phase 2 Questionnaire

CMMC 2.0 Level 1 / Phase 2 Questionnaire

[Back](#)

Show entries

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

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

Showing 1 to 2 of 21 entries

[Previous](#) [1](#) [2](#) [3](#) [Next](#)

[Submit your Questionnaire](#)

Phase 3 Verification



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

[Back](#)

Phase
3

Verification
Phase 1

Phase
3

Verification
Phase 2

Dashboard



CMMC 2.0 Level 1 Self-Assessment / Dashboard

Back

Phase 1 Planning

Intake Form

90%

Client Info

36%

Roles

100%

General

100%

Phase 2 Questionnaire

100%

Evidence

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

Display Name	Account Enabled	Operating System	Operating System Version	Make/OEM	Join Type (trust Type)	MDM Display Name	Is Compliant	Registration Time	Approximate Last Signin Date/Time	Device ID	Is Managed
Surface	TRUE	Windows	10.0.22000.194	Microsoft	Azure AD registered			08-10-2021 11:44	28-01-2022 13:37	09494c70-581a-4136-b6d0-51a895175a1a	
Phone	TRUE	iOS	14.4.2	Apple	Azure AD registered			04-05-2021 06:30	17-11-2021 04:51	6d4d4d6f-312e-423a-8c5a-0274e98ba5f1	
Lenovo	TRUE	Windows	10.0.19043.1526	Lenovo	Azure AD joined			08-12-2020 22:30	26-02-2022 11:58	5a0d794e-109f-8679-beee-eb55225c329d	
DESKTOP-06A2TC8	TRUE	Windows	10.0.19043.1526	Dell	Azure AD joined	Microsoft Intune	TRUE	27-07-2021 15:17	28-02-2022 16:49	13f05a61-754d-4844-b765-577513f7a005	TRUE
explorer	TRUE	MacMDM	12.1 (21C52)	Apple	Azure AD registered	Microsoft Intune	FALSE	24-01-2022 12:58	24-01-2022 12:58	a612c78c-1054-4d5f-a876-eb0c204c3c0f	FALSE
system_05	TRUE	Windows	10.0.19043.1526	Dell	Azure AD registered			16-02-2022 19:40	16-02-2022 19:40	8ac138f9-91af-44ac-a955-a042146f780f	
SYSTEM_07	TRUE	Windows	10.0.19043.1466	Dell	Azure AD registered			06-02-2022 19:34	06-02-2022 19:34	425d30d1-4c1a-4a0b-9678-3c7d50a70798	
Phone	TRUE	iOS	14.6	Apple	Azure AD registered			27-07-2021 07:58	18-02-2022 06:48	6d99e550-cd77-423a-8c5a-0274e98ba5f1	
DESKTOP-GG54F2	TRUE	Windows	10.0.19043.1526	Dell	Azure AD joined	Microsoft Intune	TRUE	02-06-2021 09:55	23-02-2022 12:32	6d99e550-cd77-423a-8c5a-0274e98ba5f1	TRUE
VA-WL03	TRUE	Windows	10.0.19042.1566	Dell	Azure AD registered			04-03-2022 08:39	04-03-2022 08:39	6d99e550-cd77-423a-8c5a-0274e98ba5f1	
SYSTEM18	TRUE	Windows	10.0.19043.985	Dell	Azure AD registered			04-06-2021 00:00	04-06-2021 00:00	7f4c5d7b-43ef-4104-9681-3c1a840b184c	
DESKTOP-CVN12L	TRUE	Windows	10.0.19042.1415	Dell	Azure AD joined	Microsoft Intune	FALSE	19-07-2021 09:15	22-12-2021 16:24	ca2cd150-4c3b-401a-b779-c69563818498	TRUE
System26	TRUE	Windows	10.0.19043.1526	Dell	Azure AD registered			16-02-2022 01:22	16-02-2022 01:22	77d9af4b-7707-49f1-8307-5ba85e15d8b7	
SYSTEM08	TRUE	Windows	10.0.19044.1526	Dell	Azure AD registered			16-02-2022 20:07	16-02-2022 20:07	9e557d55-091a-42b6-8c20-4a38263c6538	
DESKTOP-88U48Q	TRUE	Windows	10.0.19042.1237	Dell	Azure AD registered			05-10-2021 09:57	26-02-2022 11:35	5d4c5b4b-5c4d-4a02-9167-f31248e9c24a	
explorer	TRUE	MacMDM	12.2.1 (21D62)	Apple	Azure AD registered	Microsoft Intune	TRUE	24-01-2022 13:38	26-02-2022 15:18	32c10d6f-7d31-4a79-9d77-3c95eeb39fa5	TRUE
Adrian	TRUE	MacMDM	12.2.1 (21D62)	Apple	Azure AD registered	Microsoft Intune	TRUE	17-05-2021 13:10	27-02-2022 02:50	722a11ae-9ac7-4742-831a-819864a89af2	TRUE
System05	TRUE	Windows	10.0.19041.867	Dell	Azure AD registered			12-04-2021 21:33	05-07-2021 20:48	61c7aac5-9399-49a1-5a93-23676a024ba1	
DESKTOP-FHV9FAE	TRUE	Windows	10.0.19043.1526	Dell	Azure AD joined	Microsoft Intune	TRUE	30-10-2020 10:45	26-02-2022 14:31	6d99e550-cd77-423a-8c5a-0274e98ba5f1	TRUE
Phone	TRUE	iOS	15.1.1	Apple	Azure AD registered			11-01-2022 15:29	03-03-2022 15:21	6d99e550-cd77-423a-8c5a-0274e98ba5f1	
DESKTOP-GUDUON	TRUE	Windows	10.0.19042.1110	Dell	Azure AD joined	Microsoft Intune	TRUE	21-02-2020 13:50	27-07-2021 06:31	719ccc65-7a9f-4a29-9445-2a006a152a9d	FALSE
samsungSM-G973U	TRUE	Android	11 LG	Samsung	Azure AD registered			21-04-2021 16:28	21-11-2021 16:59	a5f4082a-239d-4a58-a72f-10f4c0b142b5	
OPPOHQ215	TRUE	Android	11 LG	LG	Azure AD registered			28-05-2021 09:52	28-07-2021 10:25	7f5ba3a5-53ba-4a48-9e53-a057964e0d44	
DESKTOP-574SDMK	TRUE	Windows	10.0.18363.0	Dell	Azure AD registered			25-05-2021 15:59	03-11-2021 04:34	aef978ba-a083-423d-9027-5794095d6a89	
SYSTEM10	TRUE	Windows	10.0.19041.867	Dell	Azure AD registered			15-04-2021 05:20	23-09-2021 20:32	627407fd-cbe7-4628-872e-2371559f365a	
System09	TRUE	Windows	10.0.19043.1237	Dell	Azure AD registered			01-08-2021 20:40	06-03-2022 23:23	901a1e06-3c4d-421b-ba05-126453977087	

Home



Home / Assessment / CMMC 2.0 Level 2 Engagement

Back

Phase 1

Planning

Phase 2

Assessor Review
of Phase 1

Phase 3

Assessment

Phase 4

Report

Phase 5

POA&M



Client Phase



ecfirst | Assessor
Phase

CMMC Reference

Readiness Portal

Policy Template



Phase 1 Planning



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

Back



Intake Form

100%



Client
Information

96.8%



Roles

31.3%



SSP Scope
Document



General
Questionnaire

29%

Phase 2 Questionnaire



Home / Assessment / CMMC 2.0 Level 2 Engagement / Verification of Phase 1

Back

AC.L2-3.1.1

AC.L2-3.1.2

AC.L2-3.1.3

AC.L2-3.1.4

AC.L2-3.1.5

AC.L2-3.1.6

AC.L2-3.1.7

AC.L2-3.1.8

AC.L2-3.1.9

AC.L2-3.1.10

AC.L2-3.1.11

AC.L2-3.1.12

AC.L2-3.1.1

1/6

Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

Authorized users are identified [a]

Are authorized users identified as part of the system access control process?

SSP Response

Yes

**SYSTEM SECURITY
PLAN.docx**

Access Control measures are implemented, including Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and Least Privilege Access policies, as outlined in page #2 of the System Security Plan document.

SSP Status

Met

Not Met

Not Applicable (N/A)

SSP Remarks

Prev 1 2 3 4 5 6 Next

Phase 3 Verification



Home / Portal / CMMC Level 2 Assessor Section / Assessor Workbook

Back

Show 10 entries

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

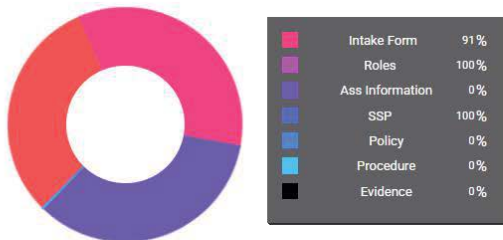
Requirement ID	Requirement Description	Action
Access Control, Domain 1		
AC.L2-3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	
AC.L2-3.1.1	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	

Dashboard

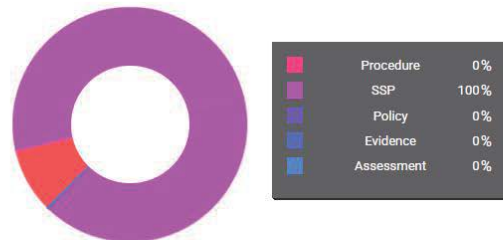


Home / Assessment / CMMC 2.0 Level 2 Engagement / CMMC Level 2 Dashboard

Phase 1 Planning



Assessors Review of Phase 1



Final Report

AI

Certification
Training

HITRUST

HIPAA

NIST

Cyber
Defense

CMIMC

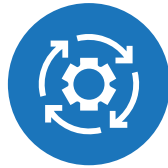
Compliance

Online
Store

Client
Reference



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

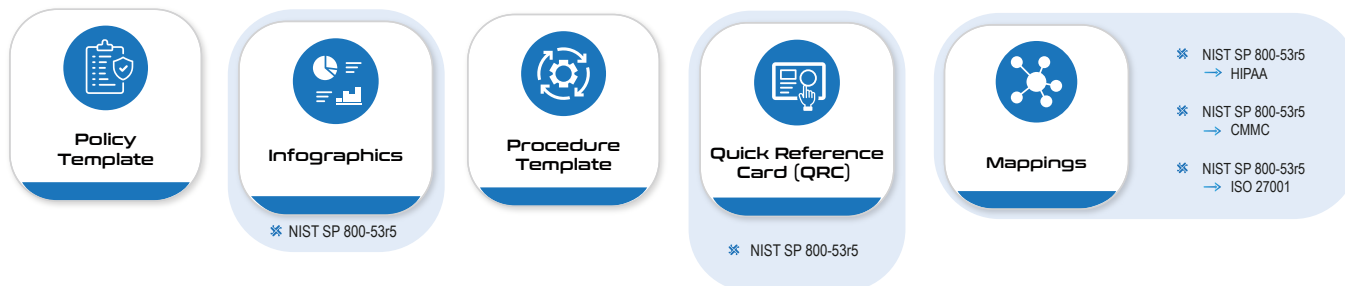
- ❖ HIPAA for Business Associate
- ❖ HIPAA Safe Harbor



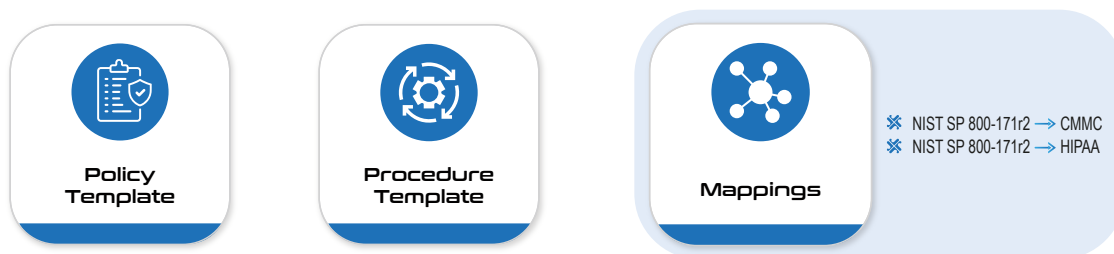
Quick Reference Cards (QRC)

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

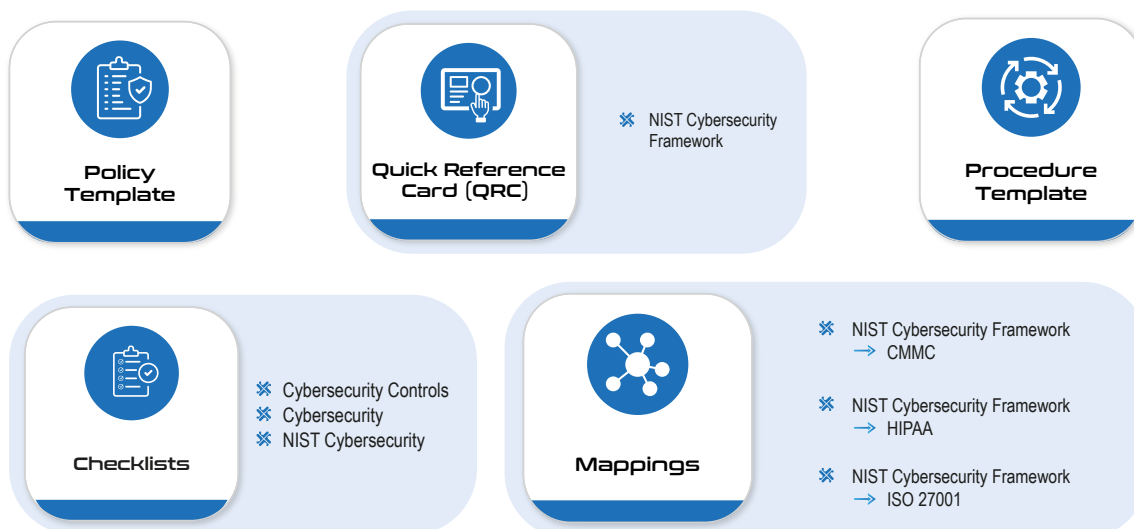
NIST SP 800-53r5 Toolkit



NIST SP 800-171r2 Toolkit



NIST Cybersecurity Framework Toolkit



Quick Links

Home

HIPAA Mandates

HIPAA Privacy Rule

HIPAA Security Rule

HIPAA Security NPRM

HITECH Breach

HIPAA FAQ

Cybersecurity

OCR Resolution Agreements

Ransomware Guidance

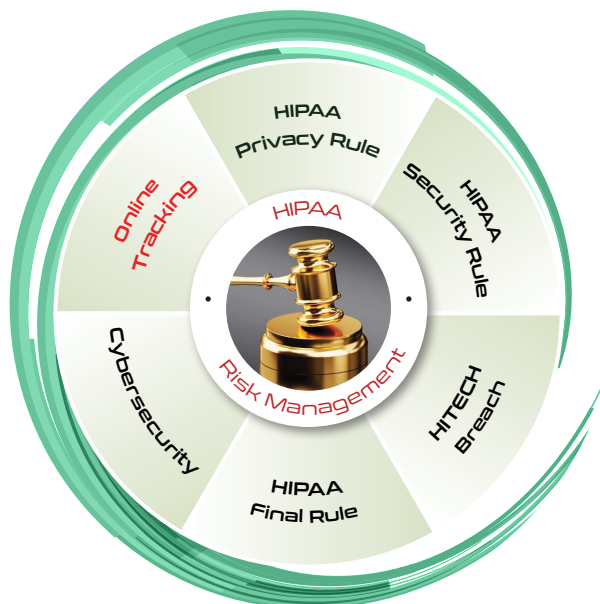
References

Posters

Templates

Training

Other Regulations



HIPAA Privacy Rule



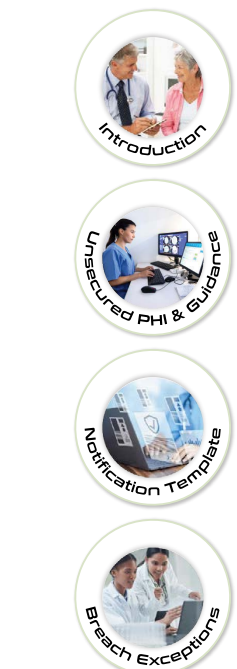
HIPAA Security Rule



HIPAA Security NPRM

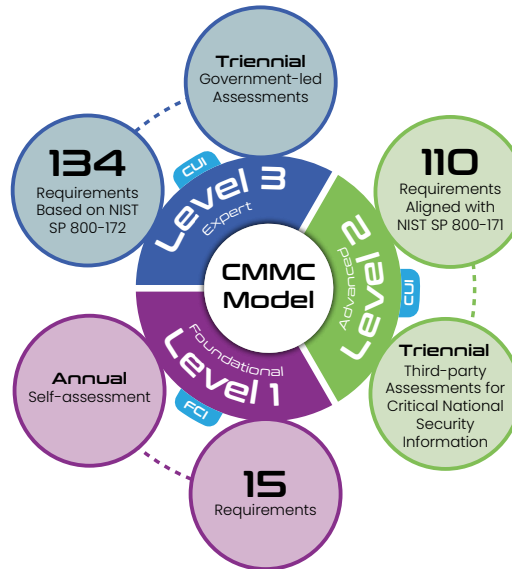


HITECH Breach



QUICK LINKS

- Home
- CMMC Level
- CMMC Domains
- Domains/Roles/Topics
- CMMC Final Rule
- CMMC Documents
- CMMC Source Documents
- NIST Resources
- NIST Cybersecurity Supply Chain Risk Management References
- CMMC SSP Sample



Domains

CMMC Playbook

CMMC LEVEL: Level 1, Level 2, Level 3

EXPLORE BY: Domains, Roles, Topics

Access Control (AC) 22 controls

- ACL2-3.1.1** Authorized Access Control [CUI Data]
Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
- ACL2-3.1.2** Transaction & Function Control [CUI Data]
Limit system access to the types of transactions and functions that authorized users are permitted to execute.
- ACL2-3.1.3** Control CUI Flow
Control the flow of CUI in accordance with approved authorizations.
- ACL2-3.1.4** Separation of Duties
Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
- ACL2-3.1.5** Least Privilege
Employ the principle of least privilege, including for specific security functions and privileged accounts.
- ACL2-3.1.6** Non-Privileged Account Use
Use non-privileged accounts or roles when accessing nonsecurity functions.
- ACL2-3.1.7** Privileged Functions

Quick Links

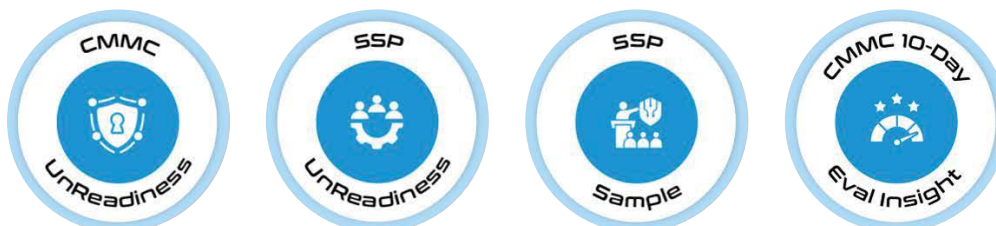
Home	
ecfirst CAP Doctrine	▼
CMMC Assessment Readiness	▼
CMMC Training	▼
Assessment Phases	
Preliminary Proceedings	
Phase 1: Conduct the Pre-Assessment	
Phase 2: Assess Conformity	
Phase 3: Report Assessment Results	
Phase 4: POA&M	
CMMC Source Documents	
Assessment Templates	



ecfirst CAP Doctrine

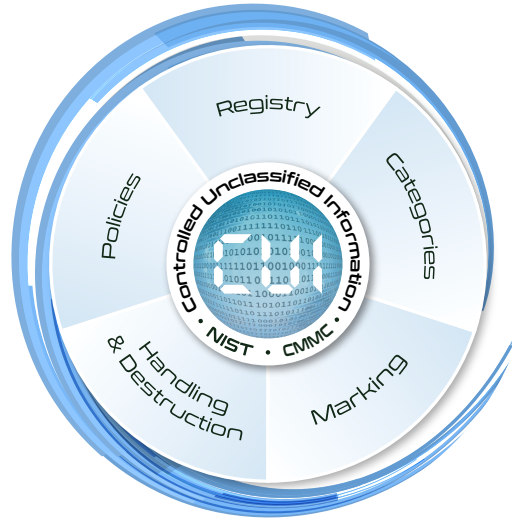


CMMC Assessment Readiness



Quick Links

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



CUI | Department of Defense



About CUI



CUI | National Archives Records Administration (NARA)



Training Resources



AI Governance Playbook

Quick Links

[Home](#)

[AI Guidance](#)

[NIST AI RMF](#)

[Explore the Playbook](#)



AI Guidance



NIST AI RMF



Explore the Playbook

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

Previous 1 2 3 4 5 ... 8 Next



Quick Links

Home

HITRUST CSF Organization ^

Why HITRUST?

HITRUST CSF V11.6.0

Domains & Controls

Authoritative Sources

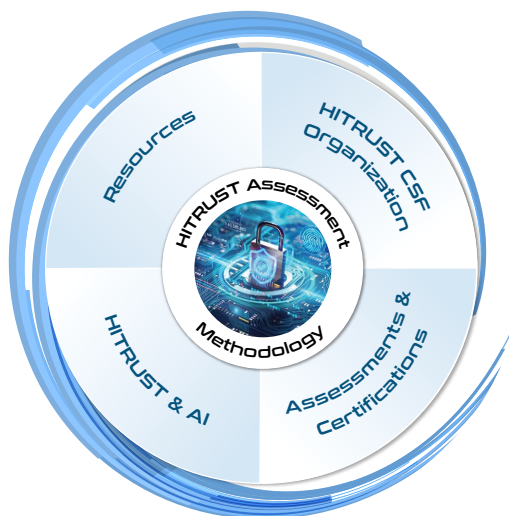
MyCSF

Assessment & Certification v

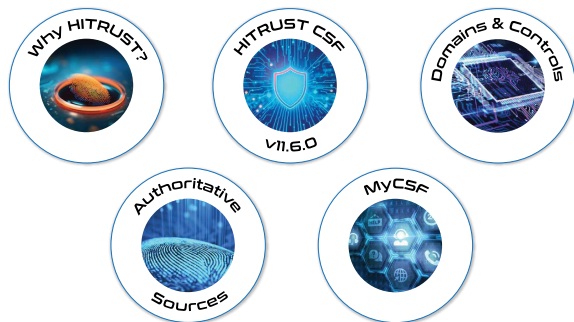
HITRUST & AI

HITRUST Resources

Why ecfirst for HITRUST?



HITRUST CSF Organization



HITRUST Resources



Assessment & Certifications



HITRUST & AI



- ✖ 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



ecfirst | SSP.ai

SSP Level 2 Template



ecfirst | SSP.ai

SSP.ai

SSP Portal

[Home](#) / [SSP Portal](#)

[Back](#)



SSP Scope



Organization Information



Security Controls



SSP Questionnaire



Dashboard



SSP Plan

Subscription

SSP Report



ecfirst | SSP.ai

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. Table of Contents	1
2. Purpose and Scope	2
3. System Identification	3
4. System Environment	4
5. System Requirements	5
6. Security Controls	6
7. Policies and Procedures	7
8. Internal Reviews	8
9. Network Diagram	9
10. System Environment	10
11. Boundary and Scope	11
12. Security Controls	12
13. Policies and Procedures	13
14. Internal Reviews	14
15. Network Diagram	15
16. System Environment	16
17. Boundary and Scope	17
18. Security Controls	18
19. Policies and Procedures	19
20. Internal Reviews	20
21. Network Diagram	21
22. System Environment	22
23. Boundary and Scope	23
24. Security Controls	24
25. Policies and Procedures	25
26. Internal Reviews	26
27. Network Diagram	27
28. System Environment	28
29. Boundary and Scope	29
30. Security Controls	30
31. Policies and Procedures	31
32. Internal Reviews	32
33. Network Diagram	33
34. System Environment	34
35. Boundary and Scope	35
36. Security Controls	36
37. Policies and Procedures	37
38. Internal Reviews	38
39. Network Diagram	39
40. System Environment	40
41. Boundary and Scope	41
42. Security Controls	42
43. Policies and Procedures	43
44. Internal Reviews	44
45. Network Diagram	45
46. System Environment	46
47. Boundary and Scope	47
48. Security Controls	48
49. Policies and Procedures	49
50. Internal Reviews	50
51. Network Diagram	51
52. System Environment	52
53. Boundary and Scope	53
54. Security Controls	54
55. Policies and Procedures	55
56. Internal Reviews	56
57. Network Diagram	57
58. System Environment	58
59. Boundary and Scope	59
60. Security Controls	60
61. Policies and Procedures	61
62. Internal Reviews	62
63. Network Diagram	63
64. System Environment	64
65. Boundary and Scope	65
66. Security Controls	66
67. Policies and Procedures	67
68. Internal Reviews	68
69. Network Diagram	69
70. System Environment	70
71. Boundary and Scope	71
72. Security Controls	72
73. Policies and Procedures	73
74. Internal Reviews	74
75. Network Diagram	75
76. System Environment	76
77. Boundary and Scope	77
78. Security Controls	78
79. Policies and Procedures	79
80. Internal Reviews	80
81. Network Diagram	81
82. System Environment	82
83. Boundary and Scope	83
84. Security Controls	84
85. Policies and Procedures	85
86. Internal Reviews	86
87. Network Diagram	87
88. System Environment	88
89. Boundary and Scope	89
90. Security Controls	90
91. Policies and Procedures	91
92. Internal Reviews	92
93. Network Diagram	93
94. System Environment	94
95. Boundary and Scope	95
96. Security Controls	96
97. Policies and Procedures	97
98. Internal Reviews	98
99. Network Diagram	99
100. System Environment	100

Training Resources



SSP Level 1



SSP Level 2



Procedures



Organization's
Security
Controls

Policies

Home



SSP Portal

Back

Select Framework

Please select the framework to proceed further

SSP Report



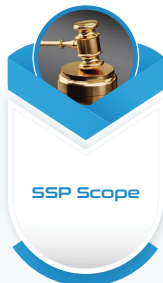
Preparation



SSP Portal

Back

Home / SSP Portal



“

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.

”

“

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.

”

“

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.

”

“

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

”

“

A crash course covering cybersecurity assessment, NIST and more.

”

“

The training was point on for the core material.

”

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!

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.**

”



“

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.

”



“

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 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.

”



“

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.

”



“ 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.

”



“ 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!

”



“ 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.

”



“

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

”



“

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

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

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

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

”

“

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.

”

“

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.

”



Get Started



#10, 8th Cross, Rainbow Nagar
Puducherry - 605011



Info@Pabrai.com



www.Pabrai.com | www.Pabrai.biz

