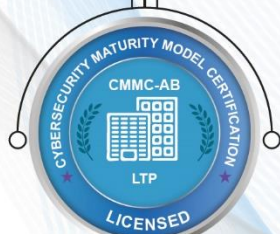
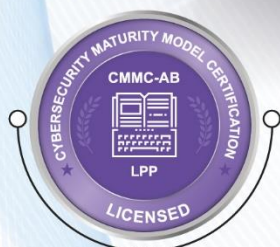




**HITRUST**  
Authorized External Assessor

**HIPAA &  
HITECH**



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

**PCI DSS**

**PCI DSS**

**CHP** Certified HIPAA  
Professional  
HIPAA Academy

**BIA & DRP**

**ISO 27001**

**CSCS**<sup>TM</sup>  
CERTIFIED SECURITY  
COMPLIANCE SPECIALIST

**Risk Analysis**

**GDPR**

**CCSA**<sup>SM</sup>  
Certified Cyber Security Architect

**Cybersecurity  
Assessment**

**NIST**

**CCP**

**Penetration  
Testing**

**CMMC**

**CCA**

**Virtual ISO &  
IT Staffing**

**On-Demand  
Consulting**

**ecfirst**  
Academy

**Biomed**  
Med Device Cybersecurity  
 Culinda

**Managed  
Compliance**

## Table of Contents

About ecfirst.....	3
TRACER <sup>SM</sup> .....	4
Online Learning.....	12
<b>Compliance Services</b>	
HIPAA & HITECH .....	15
PCI DSS .....	16
ISO 27001 .....	18
GDPR .....	20
<b>Cybersecurity Services</b>	
NIST .....	21
CMMC .....	22
On-Demand Consulting .....	23
Managed Cybersecurity Services Program (MCSP) .....	24
BIA & IT Disaster Recovery Plan.....	25
Risk Analysis .....	26
Cybersecurity Assessment & Penetration Testing .....	27
Virtual ISO & Infosec Staffing Program .....	43
Biomed & IoT .....	44
<b>Certification Training</b>	
CHP .....	46
CSCS <sup>TM</sup> .....	47
CCSA <sup>SM</sup> .....	48
CCP .....	49
CCA .....	49
About Uday Ali Pabrai .....	56



## Consulting Practice



## Certification Training



Reimagining Cyber Defense



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



## TRACER<sup>SM</sup> Features



## Compliance

### NIST SP 800-171

### CMMC

### HIPAA

### Vendor (BA) Management

### Asset Risk Management

### Policy Portal



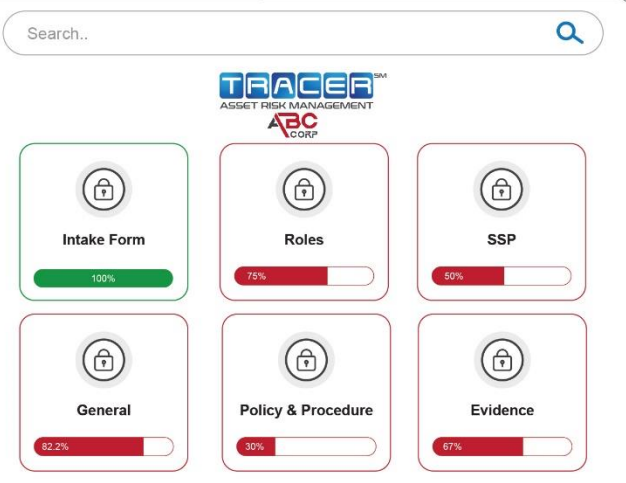
# TRACER<sup>SM</sup>

ASSET RISK MANAGEMENT

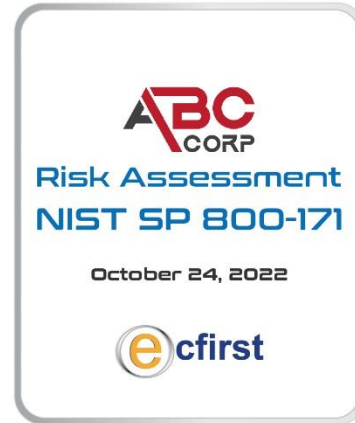


## NIST SP 800-171

### Phase 1 Planning



### Sample Report



## Cyber Readiness



## CMMC Portal

Search..

**CMMC Level 1** Back

Home / Assessment / CMMC Level 1 Self Assessment

**Self-Assessment**

<p>Phase 1</p> <p>Planning</p>	<p>Phase 2</p> <p>Self-Assessment</p>	<p>Phase 3</p> <p>Confirmation</p>	<p>Phase 4</p> <p>Generate Report</p>	<p>Phase 5</p> <p>POA&amp;M</p>
--------------------------------	---------------------------------------	------------------------------------	---------------------------------------	---------------------------------

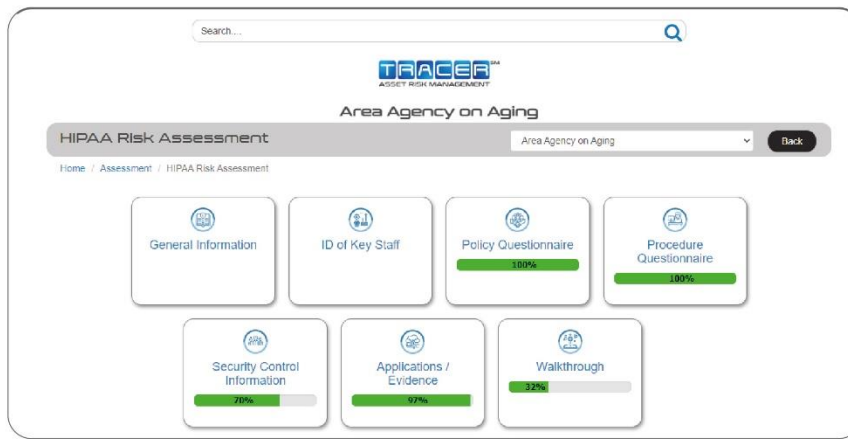
Reference Dashboard

# TRACER<sup>SM</sup>

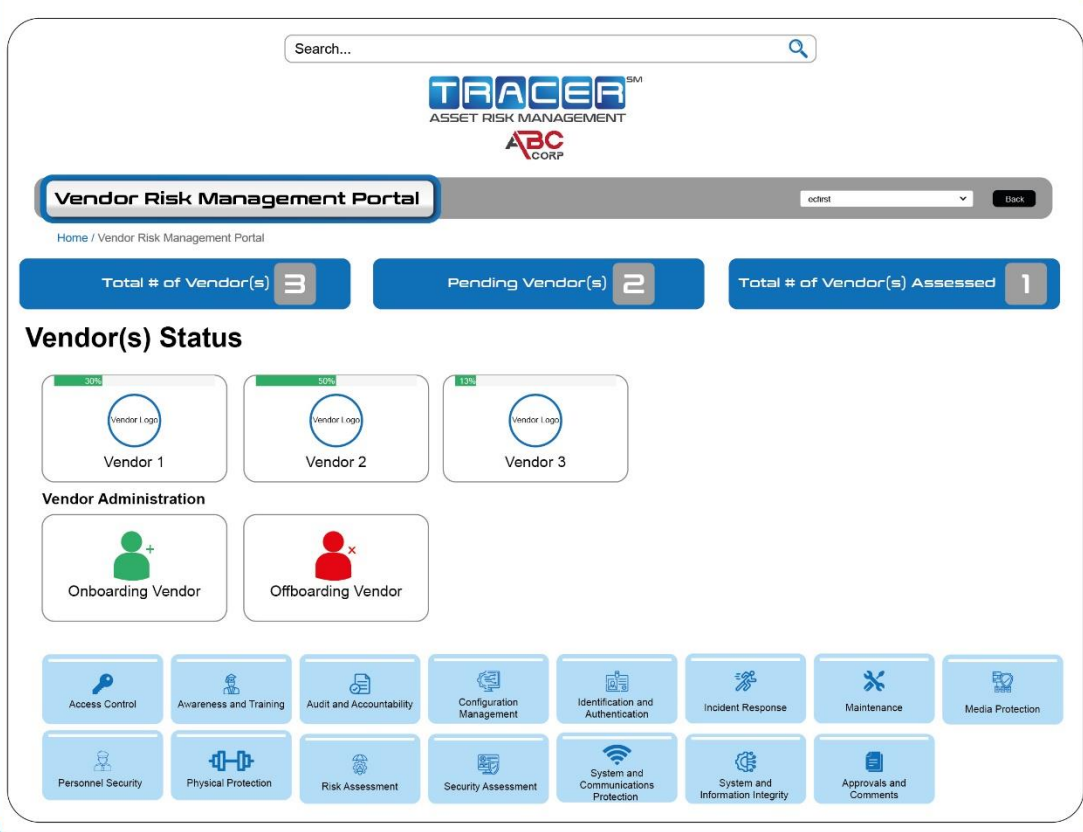
ASSET RISK MANAGEMENT



## HIPAA Portal



## Vendor Risk Management Portal





## Asset Risk Assessment

Asset Risk Management

ecfirst

Dark

Home / Asset Risk Management

Total # of Asset(s) **10**

Pending Asset(s) **3**

Total # of Asset(s) Assessed **0**

### Asset List

[Export to Excel](#)

APPLICATION NAME	↑↓ USER NAME	↑↓ EMAIL	↑↓ ROLE	↑↓ POC IT	↑↓ DATE	↑↓ ACTION
3M Clean Trace	Mary Johnson	maryjohnson@dib.org	POC IT	maryjohnson@assettracer.com	Dec 28, 2021	<a href="#">✎</a> <a href="#">🗑</a>
3M Clean Trace	John Smith	johnsmith@ventures.org	POC IT	johnsmith@assettracer.com	Dec 30, 2021	<a href="#">✎</a> <a href="#">🗑</a>

### Asset Risk Administration

[Department Master](#)

[Vendor Master](#)

[Application Master](#)

[User Master](#)

[Interview Schedule](#)

## Ransomware Readiness

Disaster Recovery Plan

10.0%

Instructions

In-scope Locations 100.0%

Roles and Responsibilities 0.0%

Data Center Operations 0.0%

BIA

38.8%

BIA-Data Collection Form 55.3%

BIA IT-Data Collection Form 22.2%

IT Disaster Recovery Plan

Data Center Operations

Item	Primary Data Center	SECONDARY Data Center - 0
Building Structure / Environment		
Building Location, Floor Number	<input type="text"/>	<input type="text"/>
Sq. Footage of Data Center	<input type="text"/>	<input type="text"/>
Structure Type	<input type="text"/>	<input type="text"/>
Type of Building / Other Risk		





## Policy Portal

### Policy Dashboard



#### Dashboard

[Back](#)[Home](#) / [Policy](#) / [Dashboard](#)

#### Security Policy Library

[Upload](#)[Create](#)[Index](#)Search: Show more 3 

File Name	File Type	File Size	Action
Implement Subnetworks Policy	PDF	1.5 MB	<a href="#">View</a> <a href="#">Download</a> <a href="#">Delete</a>
Limit System Access to Types of Transaction Policy	DOCX	257.4 KB	<a href="#">View</a> <a href="#">Download</a> <a href="#">Delete</a>
Escort and Monitor Visitors Policy	DOCX	150 KB	<a href="#">View</a> <a href="#">Download</a> <a href="#">Delete</a>

#### Privacy Policy Library

[Upload](#)[Create](#)[Index](#)

#### Other Policy Library

[Upload](#)[Create](#)[Index](#)

## Create New Policy

Policy Library

Policy Set

List of CMMC (Level 1) Policies

[View Policy Format](#)

Edit ecfirst Sample Policy Content?

CMMC Level 1 Control Physical Access Policy Yes 

Mandatory Policy Information

Policy Title

Control Physical Access Policy

Policy #

CMMC-0001-POL

Effective Date

January 1, 2022

Last Revised

January 1, 2022

Approved by

John Smith

Version #

2.0

Reference

Manage Physical Access (PE.L1-3.10.5)

Policy #

Domain 101: Physical Protection (PE)

[Save](#)

# TRACER<sup>SM</sup>

## ASSET RISK MANAGEMENT



### Procedure Portal

#### Procedure Dashboard



#### Dashboard

[Back](#)
[Home](#) / [Procedure](#) / [Dashboard](#)

#### Security Procedure Library

[Upload](#)
[Create](#)
[Index](#)
Search Show more 3 [v](#)

File Name	File Type	File Size	Action
Limit System Access to Types of Transaction Procedure	PDF	1.5 MB	<a href="#">View</a> <a href="#">Download</a> <a href="#">Delete</a>
Firewall Configuration Procedure	DOCX	257.4 KB	<a href="#">View</a> <a href="#">Download</a> <a href="#">Delete</a>
Sanitize Information System Media Procedure	DOCX	150 KB	<a href="#">View</a> <a href="#">Download</a> <a href="#">Delete</a>

#### Privacy Procedure Library

[Upload](#)
[Create](#)
[Index](#)

#### Other Procedure Library

[Upload](#)
[Create](#)
[Index](#)

### Evidence Portal



#### Evidence Dashboard

[Back](#)
[Home](#) / [Evidence](#) / [Evidence Dashboard](#)


#### HIPAA

100%

15 Files 10 GB



#### NIST SP 800-171

52.7%

10 Files 7 GB



#### CMMC L1

80%

25 Files 18 GB



#### CMMC L2

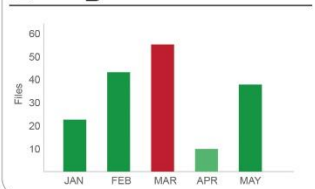
30%

9 Files 8 GB

#### Favourites

Limit System Access to Types.pdf	1.5 MB
Jun 29, 2022   CMMC L1   AC.L1-3.1.1	
Firewall Configuration Evidence.docx	257.4 KB
Jun 29, 2022   NIST SP 800-171	
Sanitize Information System.docx	150 KB
May 5, 2022   CMMC L1   IA.L1-3.5.1	

#### Usage Stats



#### Recently Uploaded

- 5 Minutes ago  
Limit System Access.pdf  
Jun 29, 2022 | CMMC L1 | AC.L1-3.1.1
- 3 Weeks ago  
Firewall Configuration Evidence.docx  
Jun 29, 2022 | NIST SP 800-171
- 1 Month ago  
Sanitize Information System.docx  
May 5, 2022 | CMMC L1 | IA.L1-3.5.1

## Evidence Portal

Search...



### HIPAA Evidence

Back

Home / Evidence / HIPAA Dashboard / HIPAA Evidence

#	HIPAA Standards & Implementation Specifications	Evidence List	Document Description	Evidence Description	Evidence Date
Security					
Administrative Safeguards					
1	§ 164.308(a)(1)(i) Security Management Process STD	Network Diagrams			<input type="checkbox"/> Evidence less than 90 days old <input type="checkbox"/> Evidence grater than 90 days old
2	§ 164.308(a)(1)(ii)(A) Risk Analysis (R) SPEC	Copies of previous assessment			
Organizational Safeguards					
1	§ 164.314(a)(1) Business Associate Contracts or Other Arrangements STD	List of BAA and other contracts			
2	§ 164.308(a)(1)(ii)(A) Risk Analysis (R) SPEC	Copies of previous assessment			









Search...



### CMMC L1

Back

Home / Evidence / Evidence Dashboard / CMMC L1

#	Practice ID	Sample Evidences	Evidence Artifact	Evidence Description	Evidence Date
DOMAIN 1: Access Control (AC)					
1	AC.L1-3.1.1 Authorized Access control	▪ SSP	Choose File Upload 	Please describe the evidence Multiple evidences may be uploaded for any requirement	
		▪ System design documentation	Choose File Upload 	Please describe the evidence description...	
2	AC.L1-3.1.2 Transaction & Function Control	▪ Restricts access only to specific transactions and functions, SSP	Choose File Upload 	Please describe the evidence description...	
DOMAIN 5: Identification & Authentication (IA)					
3	IA.L1-3.5.1 Identification	▪ Identify information system users, SSP	Choose File Upload 	Please describe the evidence description...	

Save





## Cybermapper

**Cybermapper View**

[Home](#) > [Cybermapper View](#)

What would you like to see the mapping table for?

HIPAA to ISO 27001:2013	
HIPAA Implementation Specification	ISO 27001:2013 Annex A, Control Objectives
164.308(a)(1)(i) Security Management Process	
164.308(a)(1)(i) Security Management Process STD	A.6.1.5 Information Security in Project Management
164.308(a)(1)(i)(A) Risk Analysis (R) SPEC	A.14.1.1 Information security requirements analysis and specification
	A.16.2.1 Independent review of information security

## Executive Dashboard

### Executive Dashboard

**Reports**

Title	Updated on	View
RA Report	-	<input type="button" value="View"/>
CA Report	-	N/A
RA CAP	-	N/A

**Policy Status**

Title	View
Privacy Policy	N/A
Security Policy	N/A

**Quick Links**

- [Remediation Portal](#)
- [Cybersecurity Readiness Assessment](#)
- [Cyber Mapper](#)

**Risk Assessment Status**

Title	Updated on	Status	View
DCF	-		
DCAF	-		
Compliance	-	N/A	

**Cybersecurity Assessment Status**

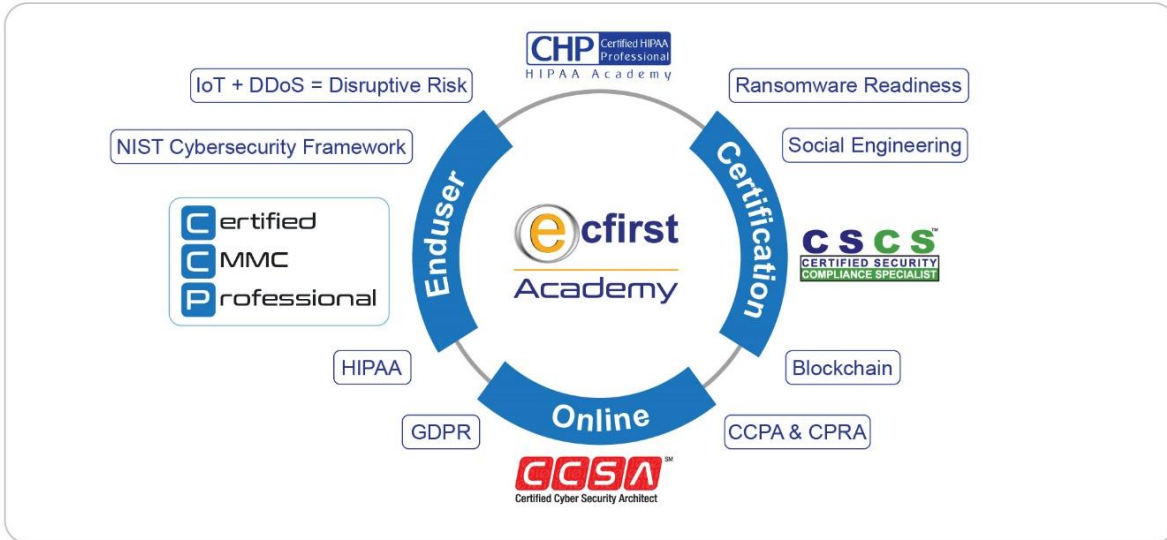
Title	Updated on	Status	View
DCF	-		
Compliance Status	-	N/A	

**Business Associates**

Title	View



## Online Learning Portal



## ecfirst Academy Features and Capabilities

- 1 Automated online software system
- 2 Content organized as various modules for each course
- 3 Each course includes an online quiz to validate content covered
- 4 Online certificate generated based on successfully completing course quiz
- 5 Easy to navigate and use the e-learning application
- 6 Audio capability is supported for course content
- 7 Supports reporting and data analysis
- 8 Tracks online learner progress
- 9 Monitors internal activity
- 10 Integrated use of pictures, images and graphics to help explain ideas, concepts, or statements
- 11 Supports a diversity of devices (responsive design)
- 12 Corporate logins available, with multiple users embed as teams, including tracking each user's progress by the administrator
- 13 Scalability, supports hectic submission process
- 14 Smart email notifications
- 15 Facility on re-allocation of quiz
- 16 Customizable real-time reports
- 17 Social learning features
- 18 ADA 508 compliant – Flexible Zoom options



## Online Learning Portal



### Logging In



The ecfirst CMMC Ecosystem

The ecfirst HIPAA Ecosystem

Welcome

Enter Your Username

Enter Your Password

Forgot My Password

Sign In

### CMMC Certification Training



Welcome: Validity Expires April 25, 2023 Home Manage MFA Logout

## Certified CMMC Professional



Updated for CMMC 2.0

Evaluation Form

CCP Pretest

Classroom

Research

Quiz

Assessor Toolkit

CMMC Practices

CMMC Readiness

Final Practice Exam

#### Quick Reference

User Guide  
CMMC Infographics  
Roles & Responsibilities  
CMMC Source Documents  
CCP Presentation Slides  
NIST Reference Documents  
CMMC Flashcard  
CMMC Flashcard Quiz  
CCP Practice Quiz  
CMMC Glossary  
CMMC Acronyms  
Controlled Unclassified Information (CUI)  
Instruction, Restricted





## Online Learning Portal



### Enduser Training

Welcome User Home Logout

### Complimentary Training

Ransomware Readiness	NIST Cybersecurity Framework	CCPA & CPRA
Social Engineering	Phishing	IoT + DDoS = Disruptive Risk
Blockchain	GDPR	HIPAA

ecfirst  
Copyright © ecfirst 1999 - 2021. All rights reserved.



CHP Certified HIPAA Professional  
HIPAA Academy

Course Categories

<b>Overview</b> What's in it For Me? (WIIFM) ▲ 9% Completed	<b>Module 1</b> HIPAA /HITECH Act/Final Rule/Safe Harbor ✖ Not Yet Started	<b>Module 2</b> Privacy Rule ✖ Not Yet Started
<b>Module 3</b> Transactions, Code Sets & Identifiers ✖ Not Yet Started	<b>Module 4</b> Security Rule ✖ Not Yet Started	
Quiz		
<b>Quiz</b> CHP Privacy Rule Quiz	<b>Quiz</b> CHP HIPAA /HITECH Act/Final Rule overview Quiz	<b>Quiz</b> CHP Transactions, Code Sets and Identifiers Quiz
<b>Quiz</b> CHP Security Rule Quiz		

Copyright © ecfirst 1999 - 2021. All rights reserved.

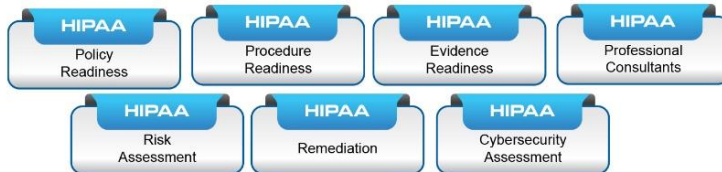
## HIPAA & HITECH



ecfirst was the first organization in the United States to deliver HIPAA training, consulting and certification services. The HIPAA Academy is the gold standard in the healthcare industry. ecfirst "delivers everything HIPAA". Talk to ecfirst and discuss your HIPAA and HITECH compliance challenges and requirements. ecfirst will create a tailored solution for your organization. Ask about the ecfirst Managed Compliance Program to maintain your HIPAA compliance program.

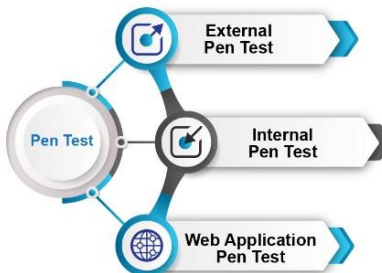
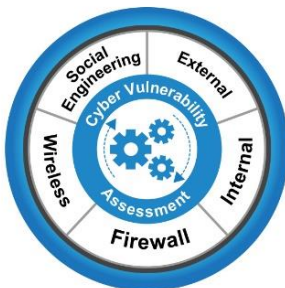
- Perform a comprehensive and thorough HIPAA Risk Assessment.
- Conduct a Cybersecurity Assessment to identify gaps.
- Develop tailored suite of policies and procedures.
- Deliver certification training providing in-depth coverage of HIPAA.
- Remediate cybersecurity and compliance gaps.
- Create customized incident response, cybersecurity, and disaster recovery plans.

### HIPAA Services



### Trust ecfirst with HIPAA

### HIPAA Compliance Lifecycle



The industry's first and most comprehensive HIPAA training and certification program.

- 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.



# PCI DSS Services



## PCI DSS: An Important Security Standard

The Payment Card Industry (PCI) Data Security Standard (DSS) is a global information security standard for protecting cardholder data. The PCI DSS requirements apply to merchants and other organizations that store, process, or transmit cardholder data. PCI DSS is a compilation of best practices for securing data throughout the information lifecycle. The PCI standard identifies several processes and procedures required to protect cardholder data. With unmatched laser beam focus on regulatory compliance and information security, ecfirst has the services your organization needs to prepare for and deliver on PCI compliance today.

### PCI DSS Goals

Secure payment card applications

Monitor & control access to systems

Remove sensitive authentication data & limit data retention

Protect the perimeter, internal, & wireless networks

Protect stored cardholder data

Finalize remaining compliance efforts, & ensure all controls are appropriately implemented

## The ecfirst PCI Readiness Assessment

This assessment enables organizations to understand the current PCI standard compliance posture and includes a Corrective Action Plan (CAP). This assessment is a remediation roadmap that the organization should complete prior to undergoing a formal PCI audit.



## ecfirst Brings Deep Experience & Expertise with PCI DSS

The ecfirst PCI DSS Readiness Assessment is a methodical examination and review of the state of PCI compliance with the defined control objectives and associated requirements of version 3.2 of the Standard. This ecfirst exercise results in an actionable & comprehensive PCI DSS Readiness Assessment Report that summarizes findings and provides details on areas in which the organization does not comply. A prioritized list of activities and recommended timetable are included, as is an executive presentation of the assessment findings.



# PCI DSS Services



1 Day

## PCI DSS Cybersecurity Workshop

### Learning Objectives

The focus of this one-day ecfirst PCI DSS cybersecurity workshop is to:

- ✦ Step through control objectives and associated requirements
- ✦ Examine guidance for defined requirements
- ✦ Review policies to address PCI DSS mandates
- ✦ Walk through requirements for risk assessment, vulnerability assessment and penetration testing
- ✦ Learn about best practices to address PCI DSS and other security standards

### Private On-Site Workshop



### Target Audience

Compliance Professionals & Managers

Information Security Officers

Security Practitioners

Privacy Officers

Internal Compliance Auditors

Senior IT Professionals

Walk through sample PCI DSS policies in-class!



## ISO 27001 Services

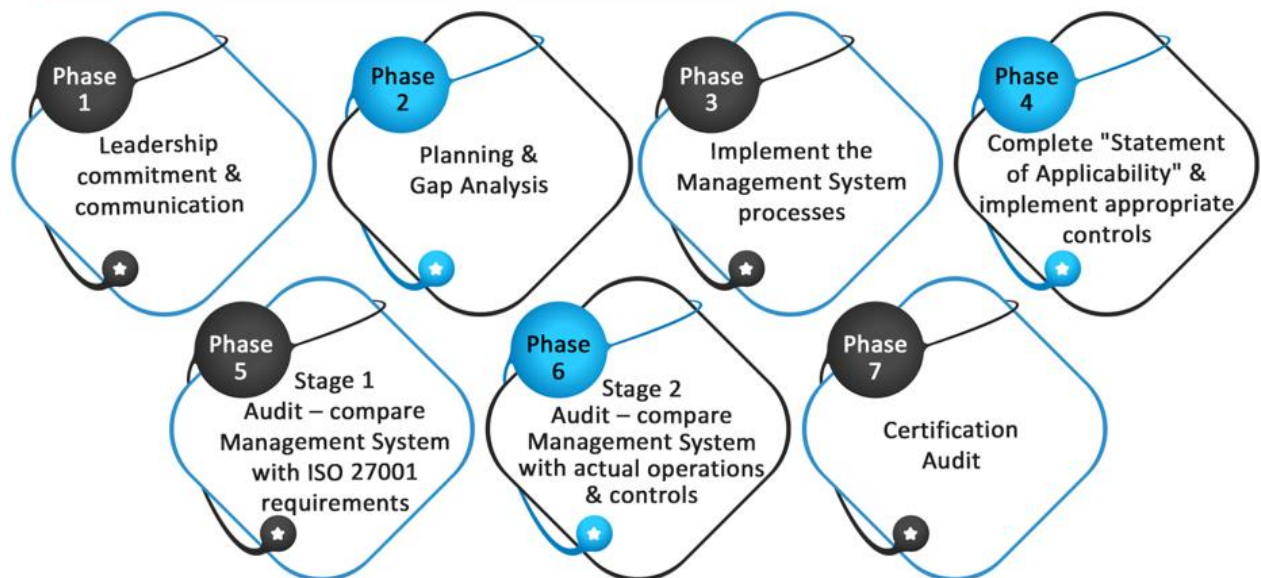


Organizations are increasingly considering applying the family of ISO 27001 international security standards to comply with various U.S. Federal and state regulations such as HIPAA, HITECH, as well as standards such as the PCI DSS. The ISO 27001 is a global standard that provides a comprehensive framework organizations can adopt to address compliance requirements and establish a resilient information infrastructure.

ecfirst Brings Deep Experience & Expertise with ISO 27001

ecfirst's fast-paced, one-day private training workshop on ISO 27001, its policy templates, quick reference cards, and deep consulting expertise embodied in its signature methodology, *bizSHIELD™*, are enabling organizations to easily adopt the ISO standard.

### A Phased Approach to Adopt ISO 27001



## ISO 27001 Services



### ISO 27001 & 27799 A 1-Day Workshop



Examine the core requirements of the ISO 27001 standard.

Understand the core elements of an Information Security Management System (ISMS).

Walk through several sample security policy templates an organization may use to address regulatory requirements.

Examine the clauses, categories, and controls defined in the ISO 27002 standard.

Examine the objective and core requirements of the ISO 27799 standard.

### ISO 27001 & ISO 27799 Services

#### ISO 27001 Training

A fast paced, instructor-led, one-day Getting Started with the ISO 27001 training delivered at your site.

#### Managed Compliance

Managed Cybersecurity Services Program (MCSP) for ISO 27001 that enables your organization to leverage deep ecfirst ISO expertise and yet pay a fixed monthly fee for a 36-month period and access a range of services at a fixed price.

#### CSCS™ Program

A two-day in-depth certification program, Certified Security Compliance Specialist™ (CSCS™) that addresses ISO 27001, PCI DSS, HIPAA, HITECH, FISMA and a lot more.

#### ISO 27001 Webcast

ISO 27001 Webcast – Applying the ISO 27001 Standard to Address Federal and State Regulations.

#### ISO 27001 Policy

ISO 27001 Security Policy Templates that can easily be tailored to enable your organization to establish a comprehensive library of policies.



# GDPR Services



The General Data Protection Regulation (GDPR) unifies the regulations within the European Union (EU). Discuss GDPR with ecfirst. ecfirst offers a complete range of GDPR compliance solutions, including:

- ▶ On-Demand Consulting (ODC) Advisory Services to establish a credible GDPR compliance Program
- ▶ Managed Cybersecurity Services Program (MCSP) to monitor and maintain a GDPR compliance program
- ▶ Comprehensive risk assessment to identify GDPR compliance gaps
- ▶ Cybersecurity vulnerability assessment to determine security vulnerabilities
- ▶ Policy review and update to address GDPR requirements
- ▶ Development of tailored GDPR security procedures

## GDPR Services

GDPR  
Policy  
Readiness

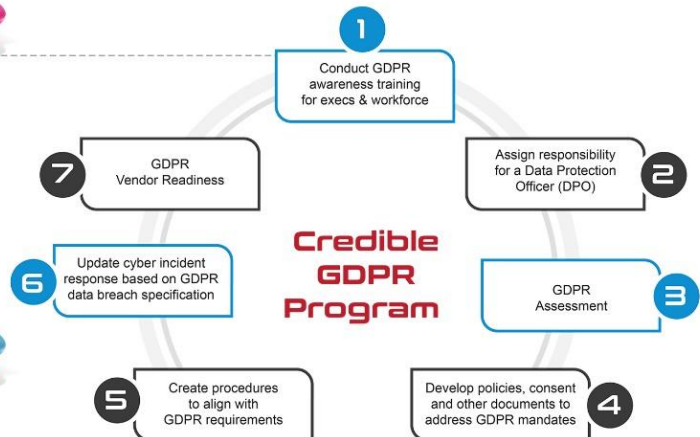
GDPR  
Procedure  
Readiness

GDPR  
Evidence  
Readiness

GDPR  
Professional  
Consultants

Trust ecfirst with GDPR

**GDPR Private Webinar:  
Complimentary!**



## GDPR Policy & Procedure

Update your policies to align with GDPR. Talk to ecfirst about creating customized policies and procedures.

**Act Now for GDPR Compliance!**

Perform a comprehensive GDPR Risk assessment

# NIST Cybersecurity Framework Services



ecfirst delivers a comprehensive suite of end-to-end NIST Cybersecurity Framework Services. Align your compliance program with the NIST Cybersecurity Framework. Ask about a complimentary seat in the industry leading cybersecurity certification training program, **CSCS** CERTIFIED SECURITY COMPLIANCE SPECIALIST

- Perform a comprehensive and thorough NIST Assessment.
- Conduct a Cybersecurity Assessment to identify gaps.
- Develop tailored suite of policies and procedures.
- Deliver certification training providing in-depth coverage of NIST.
- Remediate cybersecurity and compliance gaps.
- Create customized incident response, cybersecurity, and disaster recovery plans.

## NIST Cybersecurity Framework



## NIST Cybersecurity Framework Policy & Procedure!

Templates



Custom Updates

## NIST Cybersecurity Framework Services



Trust ecfirst with NIST Cybersecurity



The Industry's first program focused on cybersecurity compliance mandates.

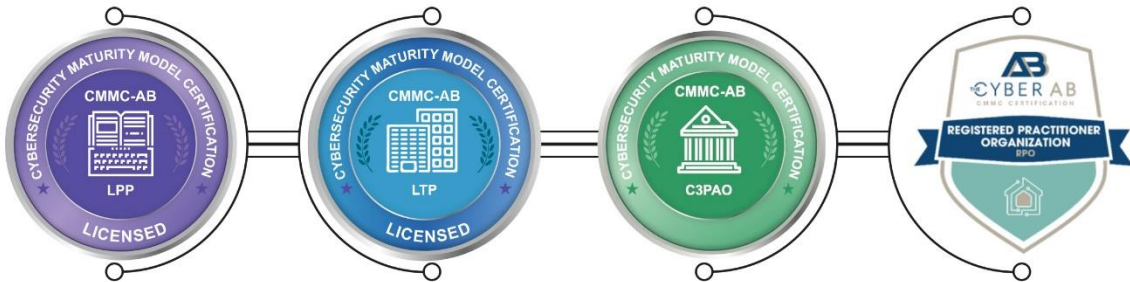
- Step through industry standards such as PCI DSS, GDPR, CCPA, ISO 27001, HIPAA, and FISMA.
- Evaluate America's standard for compliance: NIST guidance and special publications.
- Understand U.S. state government information security mandates (e.g. Texas, California, New York and others).
- Explore best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





# CMMC Consulting Services

## Cybersecurity Maturity Model Certification



### CMMC Readiness Services!



### CMMC Signature Methodology!



### CMMC Readiness

- Readiness Assessment
- Gap Remediation Guidance
- Policy Development
- System Security Plan (SSP) Development
- Procedure Guidance
- Evidence Guidance

### Certified CMMC Professional (CCP)

Virtual | Private | Online



“Solid content and flexible delivery”

“Highly informative”

“Best course ever experienced”

“ecfirst courseware is AMAZING!”

## On-Demand Consulting (ODC)

On-site | Virtual



### A Flexible Consulting Service Tailored to Your Needs

We at ecfirst refer to this consulting model as “you can do it, we can help.” ecfirst resources may be applied to work along with your IT and compliance personnel to help:

- Create and update cybersecurity policies
- Technical procedures
- Processes
- Forms
- Supporting documentation
- Other required tasks

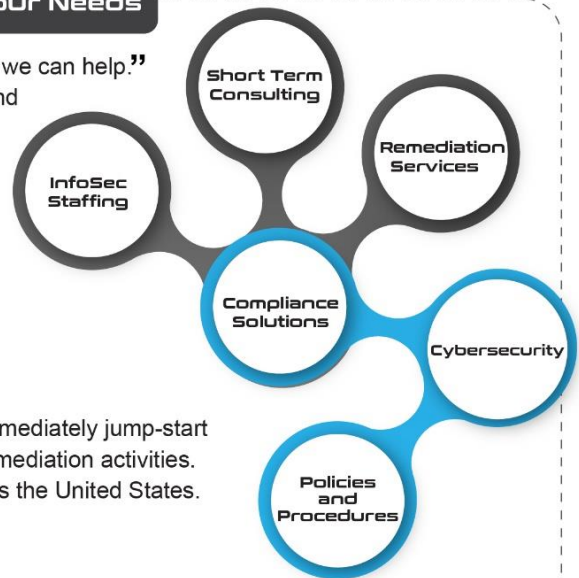
The ecfirst On-Demand Consulting (ODC) service you can immediately jump-start cybersecurity and compliance projects, as well as address remediation activities. The ODC services can be delivered on-site, or virtually, across the United States.

- Minimum 10-hour blocks of consulting time
- Fixed-rate
- No long-term commitment
- Expert compliance and cybersecurity resources to use for your initiatives

The ecfirst Team can lead and support projects in the areas of HIPAA, HITECH, ISO 27001, NIST, CMMC, GDPR, CCPA, 23 NYCRR 500 and others.

Thinking about HITRUST CSF® certification? Talk to ecfirst about aligning your policies and procedures with the NIST cybersecurity framework and the HITRUST CSF.

*On-Demand compliance solutions from ecfirst provide your organization with access to specialized compliance and security resources with no short or long-term commitment. Get started today!*



### Client Reference

“We found that ecfirst provided exceptional value for the work they delivered. The staff members were easy to work with. Their insight and guidance has enabled our organization to be better positioned to address compliance requirements. We highly recommend ecfirst and look forward to working with them again in the near future.”

**Kristi Schmidt**

*Michiana Health Information Network (MHIN)*

## Managed Cybersecurity Services Program (MCSP)

Fixed Monthly Fee. Flexible. Scalable



### MCSP for HIPAA Compliance

Does your organization need to comply with regulations & standards such as the HITECH Act, State Regulations, HIPAA Privacy & HIPAA Security? *Are your internal resources stretched to capacity & you lack the necessary expertise to identify all cybersecurity gaps & vulnerabilities?*

More than ever before, businesses today need to comply with cybersecurity & regulatory requirements to protect sensitive information about their customers, who may be consumers or patients. The penalties associated with not meeting cybersecurity requirements are not insignificant. Further, organizations have to extend precious internal resources to gain cybersecurity expertise & then manage regulatory requirements for privacy & information on a recurring basis.

This can be challenging to most organizations. ecfirst can help with its MCSP – the first program of its type in the industry, worldwide.

ecfirst delivers complete end-to-end solutions for cybersecurity. With over thousands of clients across all States in the USA, ecfirst tailors its work to closely align with your requirements & culture. Whether your requirements include a resource to implement security controls & technologies, develop policies & procedures, or comply with HIPAA, HITECH, PCI DSS, ISO 27001, ecfirst is flexible to address your workforce needs.

#### On a regular schedule, organizations must by law:

- Assign responsibility to the security officer who is responsible for coordinating cybersecurity initiatives
- Conduct a comprehensive & thorough cybersecurity assessment
- Complete a Business Impact Analysis (BIA) for contingency planning & disaster recovery
- Develop & update security policies & procedures
- Train all members of the workforce

#### MCSP Benefits

MCSP is designed to assist organizations, including business associates manage cybersecurity requirements, security & core components of the infrastructure. ecfirst's MCSP is designed to address critical regulatory requirements. Key benefits of the managed cybersecurity program include:

- Clearly defined deliverables to achieve secured organization
- Expert advisor assigned – serves as interim Information Security Advisor (one call; one email)
- Risk analysis & cybersecurity assessment conducted on a regular schedule
- Policies maintained on a continual basis
- Easily tailored to your organizational requirements - highly flexible
- Very scalable program – can monitor & audit as required
- Skilled resource pool with expert domain knowledge
- Fixed monthly fee, no interest

### Client Reference

*“ Prime Healthcare and its network of 40+ hospitals are excited to have exclusively selected ecfirst, home of the HIPAA Academy, to address HIPAA and HITECH regulatory compliance mandates. The engagement is based on the ecfirst MCSP which is a complete end-to-end comprehensive compliance solution that addresses risk analysis, technical vulnerability assessment, policy development, social engineering, business impact analysis, creation of a disaster recovery plan, as well as on-demand remediation services for risk management (corrective action plan). Prime Healthcare is excited to have partnered with an organization – ecfirst – that is recognized in the healthcare industry and with business associates internationally, as a leader devoted to enabling health systems to continually meet information privacy and security regulatory requirements. ”*

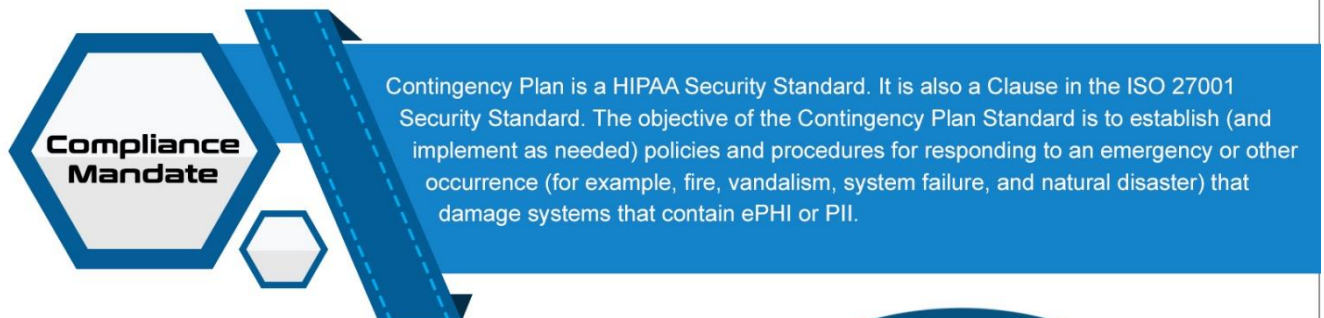
**Prime Healthcare**



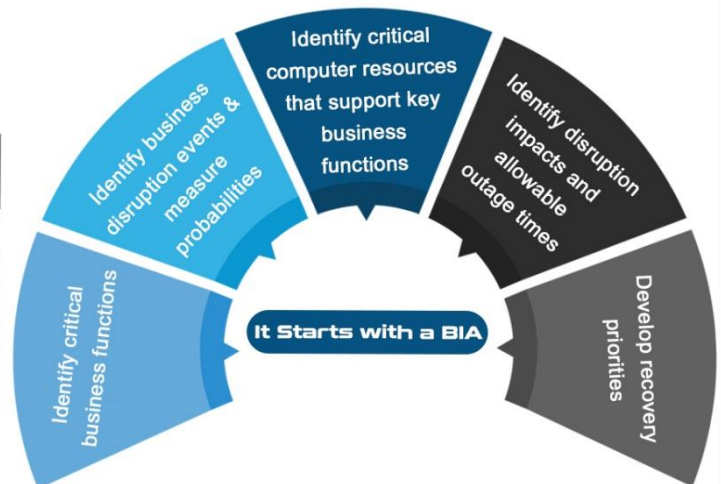
## BIA & IT Disaster Recovery Plan Prepared for a Cyber Event?



Contingency planning, also referred to as Business Continuity Planning (BCP), is a coordinated strategy that involves plans, procedures and technical measures to enable the recovery of systems, operations, and data after a disruption. A Business Impact Analysis (BIA) is the foundation for building Contingency Plans. Once the BIA is completed, Contingency Plans can be developed using the information identified in the BIA. Typically, two types of Contingency Plans will need to be developed: Emergency Mode Operations Plan for business unit recovery and IT Disaster Recovery Plan (IT DRP) for Information Technology (IT) systems and infrastructure.



Standard	Implementation Specifications
Contingency Plan	Data Backup Plan Disaster Recovery Plan Emergency Mode Operation Plan Testing and Revision Procedure Applications and Data Criticality Analysis



### Ransomware. Prepared?

Organization must perform a Business Impact Analysis & Develop IT Disaster Recovery Plan.

### Client Deliverables

1

Business Impact Analysis Report

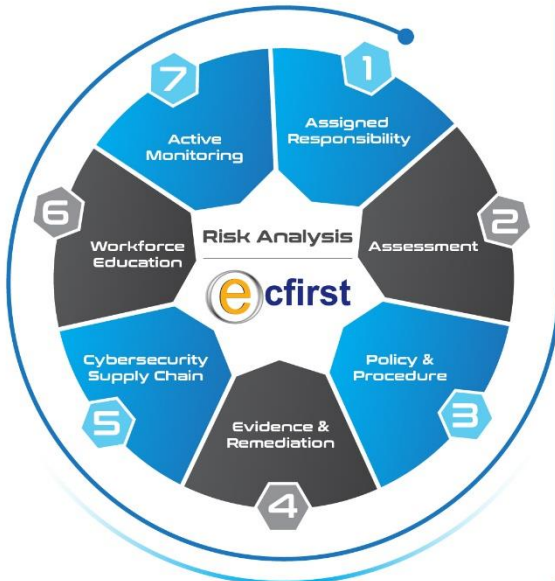
2

An IT Disaster Recovery Plan

# Risk & Cyber Assessment



## Signature Methodology



## Risk Analysis

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

Risk Analysis	Platinum	Gold
Kick-Off/Launch Meeting	Virtual	✗
Personalized Interviews	Virtual	✗
Administrative Safeguards	✓	✓
Physical Safeguards	✓	✓
Technical Safeguards	✓	✓
Privacy Assessment	✓	✓
Supply Chain Assessment	✓	✓
Policy Gap Assessment	✓	✓
Breach Assessment	✓	✓
Guided Facility Walkthrough	✓	✗
Guided Data Center Assessment	✓	✗
Executive Brief	Virtual	✗
Corrective Action Plan (CAP)	✓	✓



TRACER is a platform to manage your compliance and cybersecurity program.





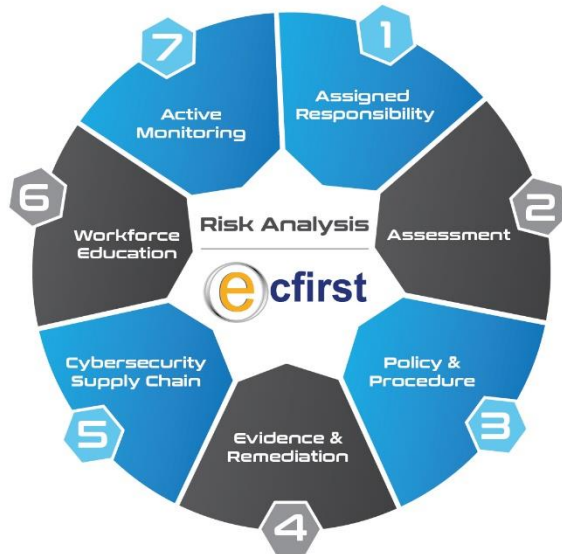
## Risk & Cyber Assessment

Performed Remotely!



### Signature Methodology

Page 3



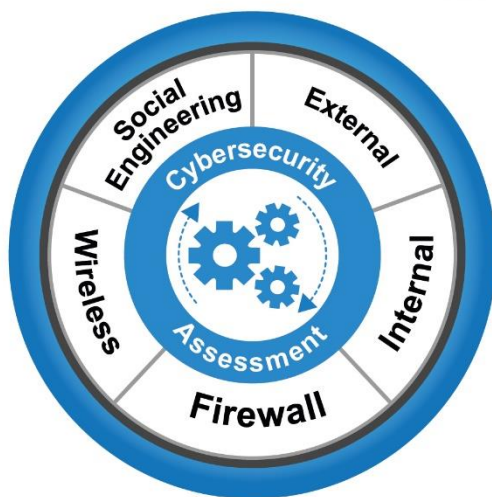
### Social Engineering

Page 4



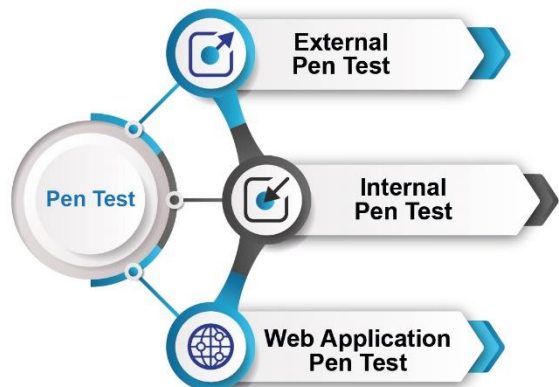
### Cybersecurity Assessment

Page 3



### Pen Test

Page 10



## Risk & Cyber Assessment

Performed Remotely!

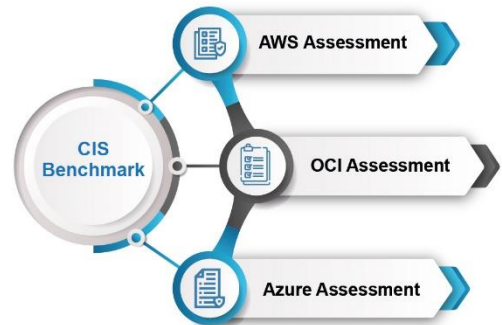
### Asset Risk Management

Page 3



### CIS Benchmark

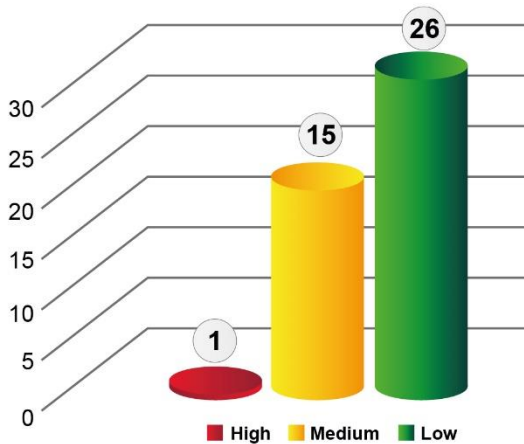
Page 13



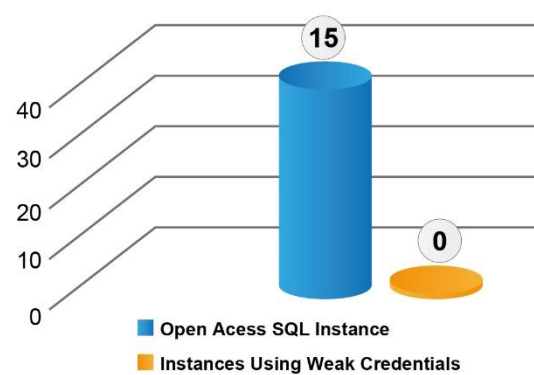
### Deep Database Assessment

Page 13

Database Vulnerability Totals



SQL Database Instances



# Cybersecurity Assessment

Performed Remotely!

Every organization must conduct a thorough and comprehensive assessment of the potential risks and vulnerabilities to the Confidentiality, Integrity, and Availability (CIA) of all sensitive, confidential information.

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	✓	✓	✗	✗	✗

## Executive Dashboard

### Significant Findings



### Risk Summary

- An overall Security Grade: **B**
- An overall Security Risk: **Medium**



### Cyber Risk Status

#### External System Vulnerability Totals



#### Web App Vulnerability Totals



#### Internal Vulnerability Totals



#### Firewall Configuration Vulnerability Totals





## Cybersecurity Assessment

Performed Remotely!

### Titanium

#### Titanium Level is organized into four (4) distinct areas.

You must be able to deploy a Virtual Machine image (in OVF format) supporting our defined specifications, such as an ESX server or VMWare Workstation installation. If you are unable to deploy our Virtual Machine image, we will send you a hardware device at an additional cost.

#### External Assessment

- ✦ Externally accessible IP addresses (up to 256) scanned for vulnerabilities; all identified vulnerabilities validated to the extent possible
- ✦ Up to four (4) external domains tested for:
  - » Google Hacking Database entries
  - » Domain Name Server misconfigurations
  - » Metadata in publicly accessible documents
- ✦ Up to two (2) websites/applications crawled/scanned for vulnerabilities under one (1) user role
- ✦ Scope does not include Biomedical Device Cybersecurity Assessment or other specialized devices and equipment

#### Wireless Assessment

- ✦ We will send a handheld device (along with instructions) that someone in your organization will utilize to assist us in this portion of the assessment
- Assessment of one (1) physical building to identify:
  - » Potentially rogue Access Points/SSIDs
  - » Open wireless access segmentation review, including testing of segmentation
  - » Insecure authentication/encryption configurations including testing of Pre-Shared Key strength

#### Firewall Assessment

- ✦ Review of up to four (4) supported firewall configurations to identify Operating System related vulnerabilities and best practice adherence
  - » Includes review of firewall rules on a single (1) firewall to assist with business justification documentation and configuration according to the principle of least privilege

#### Cybersecurity Assessment Scope

#### Titanium

External Assessment	✓ Customized
Internal Assessment	✓ Customized
Firewall Assessment	✓ Customized
Wireless Assessment	✓ Customized
Detailed Analysis	✓
Corrective Action Plan (CAP)	✓
Detailed Remediation Steps	✓
Executive Brief	✓

#### Internal Assessment

- ✦ Internal IP addresses (up to 4096) scanned for vulnerabilities; all identified vulnerabilities validated to the extent possible
- ✦ Up to 16 Class C network ranges scanned for:
  - » Devices responding to "default" SNMP Community Strings
  - » Systems running up to three (3) database server types (i.e. MSSQL, MySQL, Oracle, etc.) that allow open access
  - » Identified systems also tested for "default" credentials
- ✦ Up to three (3) Active Directory domains tested for:
  - » Identity and Access Management best practice adherence
  - » Password Policy best practice adherence
  - » User account password strength
  - » USB device enumeration of systems registered in Active Directory
  - » Identification of currently connected devices

# Cybersecurity Assessment

Performed Remotely!

## Platinum

**Platinum Level is divided into four (4) distinct areas.**

*You must be able to deploy a Virtual Machine image (in OVF format) supporting our defined specifications, such as an ESX server or VMWare Workstation installation. If you are unable to deploy our Virtual Machine image, we will send you a hardware device at an additional cost.*

### External Assessment

- ❖ Up to sixteen (16) externally accessible IP addresses scanned for vulnerabilities; all identified vulnerabilities validated to the extent possible
- ❖ Up to three (3) external domains tested for:
  - » Google Hacking Database entries
  - » Domain Name Server misconfigurations
  - » Metadata in publicly accessible documents
- ❖ Up to two (2) websites/applications crawled/scanned for vulnerabilities under one (1) user role

### Wireless Assessment

- ❖ *We will send you a handheld device (along with instructions) that someone in your organization will utilize to assist us in this portion of the assessment*
- ❖ Assessment of one (1) physical building to identify:
  - » Potentially rogue Access Points/SSIDs
  - » Open wireless access segmentation review, including testing of segmentation
  - » Insecure authentication/encryption configurations including determination of Pre-Shared Key strength

### Firewall Assessment

- ❖ Review of up to two (2) supported firewall configurations to identify Operating System related vulnerabilities and best practice adherence

### Cybersecurity Assessment Scope

## Platinum

External Assessment	✓
Internal Assessment	✓
Firewall Assessment	✓
Wireless Assessment	✓
Detailed Analysis	✓
Corrective Action Plan (CAP)	✓
Detailed Remediation Steps	✓
Executive Brief	✓

### Internal Assessment

- ❖ Up to sixteen (16) internal IP addresses scanned for vulnerabilities
  - » All identified vulnerabilities validated to the extent possible
- ❖ Up to three (3) class C network ranges scanned for:
  - » Devices responding to "default" SNMP Community Strings
  - » Systems running up to three (3) database server types (i.e. MSSQL, MySQL, Oracle, etc.) that allow open access
  - » Identified systems are also tested for "default" credentials
- ❖ Up to two (2) Active Directory domains tested for:
  - » Identity and Access Management (IAM) best practice adherence
  - » Password Policy best practice adherence
  - » User account password strength
  - » USB device enumeration of systems registered in Active Directory (AD)
  - » Identification of currently connected devices



## Cybersecurity Assessment

Performed Remotely!

### Gold

Gold level is organized into three (3) distinct areas.

You must be able to deploy a Virtual Machine image (in OVF format) supporting our defined specifications, such as an ESX server or VMWare Workstation installation. If you are unable to deploy our Virtual Machine image, we will send you a hardware device at an additional cost.

### External Assessment

- ❖ Up to eight (8) externally accessible IP addresses scanned for vulnerabilities
- ❖ One (1) external domains tested for:
  - » Google Hacking Database entries
  - » Domain Name Server misconfigurations
  - » Metadata in publicly accessible documents
- ❖ One (1) websites/applications anonymously crawled/scanned for vulnerabilities

### Firewall Assessment

Review of one (1) supported firewall configuration to identify Operating System related vulnerabilities and best practice adherence

### Cybersecurity Assessment Scope

Gold

External Assessment	✓
Internal Assessment	✓
Firewall Assessment	✓
Wireless Assessment	✗
Detailed Analysis	✓
Corrective Action Plan (CAP)	✓
Detailed Remediation Steps	✓
Executive Brief	✗

### Internal Assessment

- ❖ Up to eight (8) internal IP addresses scanned for vulnerabilities
- ❖ One (1) class C network ranges scanned for:
  - » Devices responding to "default" SNMP Community Strings
  - » Systems running one (1) database server type (i.e. MSSQL, MySQL, etc.) that allows open access
  - » Systems also tested for "default" credentials
- ❖ One (1) Active Directory domains tested for:
  - » Identity and Access Management best practice adherence
  - » Password Policy best practice adherence
  - » User account password strength
  - » USB device enumeration of systems registered in Active Directory

# Cybersecurity Assessment

Performed Remotely!

## Silver

Silver level is divided into two (2) distinct areas.

Please note that the Cybersecurity Assessment – Silver would most likely not be considered a comprehensive cybersecurity assessment, as critical areas related to the internal network/system management are not included in the testing.

### External Assessment

- ❖ Up to eight (8) externally accessible IP addresses scanned for vulnerabilities
- ❖ One (1) external domains tested for:
  - » Google Hacking Database entries
  - » Domain Name Server misconfigurations
  - » Metadata in publicly accessible documents
- ❖ One (1) websites/applications anonymously crawled/scanned for vulnerabilities

### Firewall Assessment

Review of one (1) supported firewall configuration to identify Operating System related vulnerabilities

### Cybersecurity Assessment Scope

Silver

External Assessment	✓
Internal Assessment	✗
Firewall Assessment	✓
Wireless Assessment	✗
Detailed Analysis	✓
Corrective Action Plan (CAP)	✗
Detailed Remediation Steps	✗
Executive Brief	✗

## Periodic Cybersecurity Scanning

Performed Remotely!

- ❖ Periodic external cybersecurity scans (performed remotely)
  - » Up to thirty-two (32) externally accessible IP addresses scanned quarterly for vulnerabilities
- ❖ Report containing:
  - » Detailed cybersecurity findings
  - » Corrective Action Plan
  - » Detailed remediation information
- ❖ Periodic internal cybersecurity scans (performed remotely)
  - » Up to thirty-two (32) internal IP addresses scanned quarterly for vulnerabilities
- ❖ Report containing:
  - » Detailed cybersecurity findings
  - » Corrective Action Plan
  - » Detailed remediation information

# Cybersecurity Assessment

Performed Remotely!

## Web Application Cybersecurity Assessment

✖ The scope of a Web Application Cybersecurity Assessment includes the following specific items:

- » One (1) Web Application
- » One (1) user role type to be utilized for testing
  - "Client" user account type
  - Anonymous access will also be tested

### General Goal(s)

- » Identify vulnerabilities related to the OWASP Top 10
- » Identify deviations from best practice

### Out-of-scope

- » Underlying System vulnerability testing
- » Web Application Firewall (WAF) and/or IDS/IPS evasion

## Web Application Cybersecurity Assessment Methodology

### Mapping

- » Analyzing HTTPS Support
- » Analyze Software Configuration
- » Crawl the site/application
- » Application flow charting
- » Relationship analysis
- » Session analysis

### Discovery

- » Automated Vulnerability Scanning
- » Information Leakage & Directory Browsing Discovery
- » Username Harvesting & Password Guessing
- » Command Injection Discovery
- » Directory Traversal & File Inclusion Discovery
- » SQL Injection Discovery
- » Cross-site Scripting (XSS) Discovery
- » Cross-site Request Forgery (CSRF) Discovery
- » Session Flaw Discovery
- » Insecure Redirects & Forwards Discovery

Upon completion of the penetration test and receiving the initial report, there will be 60 days to remediate. After that time, ecfirst will review the remediation and retest as necessary and will provide a new updated report.

# Pen Test

Performed Remotely!

## External Penetration Test

- ❖ External Penetration Test is “pre-scoped” to the following general criteria:
  - » A “grey box” test provides the following:
    - IP address ranges owned/operated
    - All domains owned/associated with up to sixteen (16) external systems
  - » Testing takes place across 5 business days, primarily during business hours

### Primary Goal

- ❖ Primary goal is to gain unauthorized elevated access to an externally accessible system
- » A secondary goal is to gain unauthorized access to other systems utilizing the primary goal system

### Out-of-Scope

- ❖ Denial of Service attacks

- ❖ The External Penetration Test methodology is described below:

### Reconnaissance

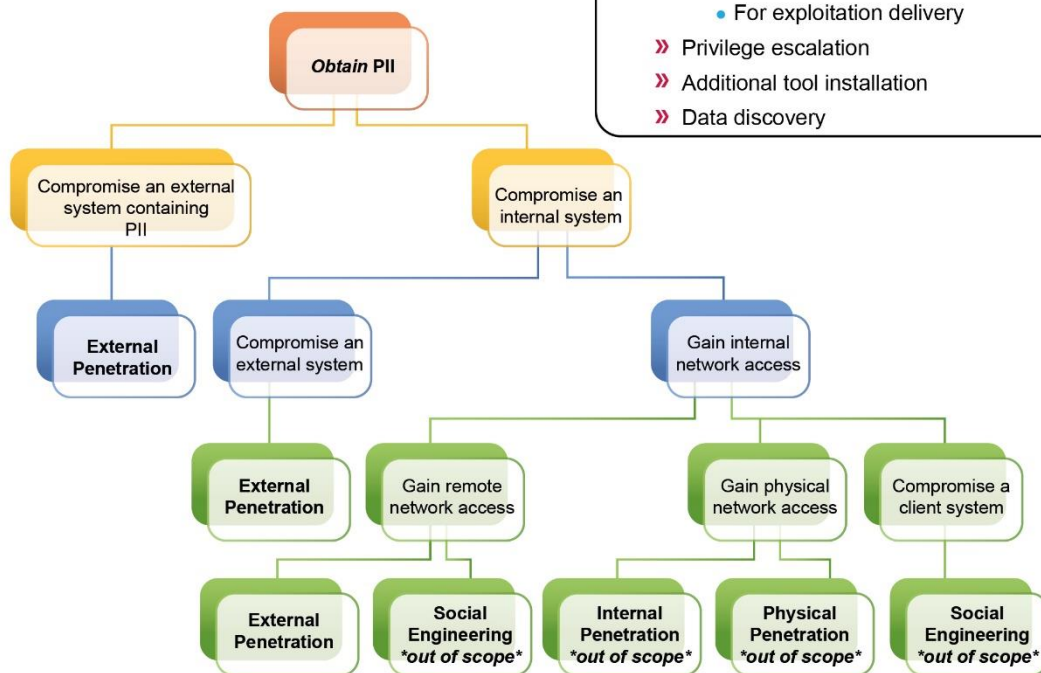
- » Client personnel and cultural information
- » Client business terminology
- » Technical infrastructure information

### Scanning

- » Network discovery
- » Network port and service identification
- » Cybersecurity identification
- » Enumeration

### Exploitation

- » Password cracking
- » Discovered credential usage
- » Manual and automated cybersecurity validation
- » Phishing attempts
  - For credential gathering
  - For exploitation delivery
- » Privilege escalation
- » Additional tool installation
- » Data discovery





# Pen Test

Performed Remotely!

## Internal Penetration Test

❖ Internal Penetration Test is “pre-scoped” to the following general criteria:

» A “grey box” test provides the following:

- Domain User account configured as a “regular” employee
- Remote access to the internal network via a virtual machine or physical device provided by us

» Not all vulnerabilities identified will be validated and/or exploited

- Only those deemed most likely to assist in reaching the defined Goal will be further validated and exploited

### Primary Goal

- » Primary goal is to gain Domain Administrator level access on the internal network.
- Secondary goal is to gain unauthorized access to sensitive data

### Out-of-Scope

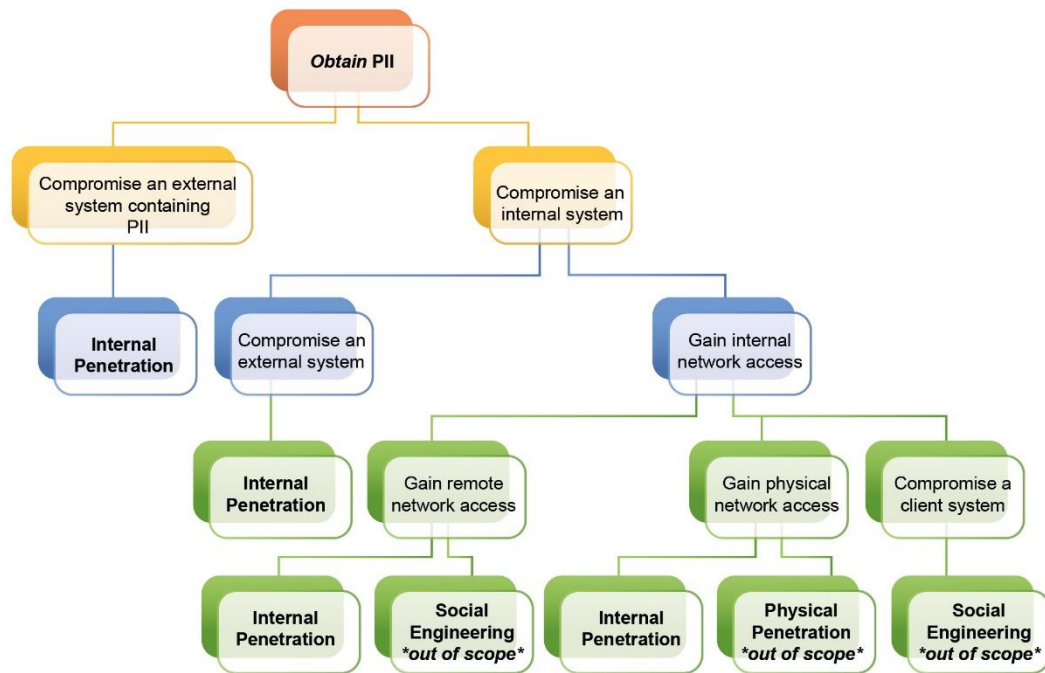
- » End-user attacks (i.e. phishing, man-in-the-middle, client-side exploitation, etc.)
- » Denial of Service attacks

### Scanning

- » Network discovery
- » Network port and service identification
- » Cybersecurity identification
- » Enumeration

### Exploitation

- » Password cracking
- » Discovered credential usage
- » Manual and automated cybersecurity validation
- » Privilege escalation
- » Additional tool installation
- » Data discovery



**Pen Test****Performed Remotely!****Web Application Penetration Test**

✦ A Web Application Penetration Test includes the following specific items:

- » One (1) Web Application
- » One (1) user role type to be utilized for testing
  - “Client” user account type
  - Anonymous access will also be tested

**General Goal(s)**

- » Gain anonymous access to authenticated sections of the application
- » Gain access to other client data within the application

**Out-of-Scope**

- » Underlying system cybersecurity exploitation
- » System account creation
- » Web Application Firewall and/or Intrusion Detection System/Intrusion Protection System evasion

The Web Application Penetration Test methodology is described below.

**Reconnaissance**

- » Technical infrastructure information

**Discovery**

- » Automated cybersecurity scanning
- » Information leakage and directory browsing discovery
- » Username harvesting and password guessing
- » Command injection discovery
- » Directory traversal and file inclusion discovery
- » SQL injection discovery
- » Cross-site scripting discovery
- » Cross-site Request Forgery discovery
- » Session flaw discovery
- » Insecure redirects and forwards discovery

**Mapping**

- » Network discovery
- » Network port and service identification
- » Analyzing HTTPS support
- » Identify virtual hosting and load balancers
- » Analyze software configuration
- » Spider the site/application
- » Application flow charting
- » Relationship analysis
- » Session analysis

**Exploitation**

- » Exploit identified enumeration flaws
- » Exploit identified bypass flaws
- » Exploit identified injection flaws
- » Exploit identified session flaws
- » Chain exploits together, pivot to other systems, data exfiltration, raid, etc.

## CIS Benchmark Assessment

Performed Remotely!

### AWS Assessment

#### Advancing Cloud Security with CIS on AWS

Increased demand for remote work capabilities continues since 2020. Customer security in the cloud remains an important part of that growth. The Center for Internet Security (CIS), in conjunction with Amazon Web Services (AWS), has worked to enhance security in the already secure AWS Cloud since 2015.

The AWS Shared Responsibility Model makes it easy to understand the role cloud consumers play in protecting their unique AWS environments. CIS security best practices can help organizations achieve cloud security from the customer's side of the responsibility model.

Best practice configuration guides include the CIS AWS Foundations Benchmark, CIS Amazon Linux 2 Benchmark, and service-based guidance like the CIS Amazon Elastic Kubernetes Service (EKS) Benchmark. Guides contain prescriptive guidance to secure configurations for a subset of AWS services and account-level settings.

#### ecfirst AWS Report includes:

- » Alignment with CIS Benchmark for AWS Foundations, Level 1 settings
- » Correctly configured settings where further action is required to achieve full security benefits
- » Review of available versus used licenses and their impact
- » Analysis of findings, including strengths and prioritized areas for improvement

#### Configuration benchmark alignment areas include:

- » Identity and access management
- » Storage
- » Logging
- » Monitoring
- » Networking

#### Readiness Assessment

The AWS Cloud Readiness Assessment is **your first step in organizational readiness for leveraging the cloud effectively**. The assessment provides analysis and planning to identify, measure, and create business value using technology services and document current business objectives for cloud enablement.

The phases for this assessment are:

- » **Initiation:** Capture the business context including the general and specific drivers for the assessment.
- » **Preliminary Analysis:** Establishes the architecture frameworks to be used and data-points to be collected. In this phase we also identify sources of information, and named points-of-contact.
- » **Discovery:** Construction of a catalogue of applications, data, technologies, processes and organisation structure, which is populated with multiple data points against each element.
- » **Analysis:** Interpretation and presentation of the assessment findings, typically expressed in terms of the fitness of each component, its sustainability and contribution to the overall risk profile.



# CIS Benchmark Assessment

Performed Remotely!

## OCI Assessment

### CIS Foundations Benchmark for Oracle Cloud

The recommendations in the new CIS Foundations Benchmark for Oracle Cloud include:

- » Encouraging the use of multi-factor authentication (MFA) for all console users
- » Restricting remote administration ports outside of the enterprise network
- » Configuring logging and notifications to aid in identifying anomalous behavior and investigate potential compromise.

The CIS Oracle Cloud Infrastructure Foundations Benchmark. Provides prescriptive guidance to securely configure an Oracle Cloud account. The step-by-step checklist includes detailed recommendations for Identity and Access Management, networking, and logging and monitoring. It's available as a free download to public and private organizations worldwide.

The CIS Oracle Cloud Infrastructure (OCI) Foundations Benchmark provides prescriptive guidance for establishing a secure baseline configuration for the OCI environment. The scope of this benchmark is to establish a base level of security for anyone utilizing the included OCI services.

While all organizations require a prudent level of cybersecurity these days, It is recommended for organizations who use OCI meet the CIS Benchmark for OCI Foundations at Level 1.

- » Review of compliance with each "Level 1" item contained in the Benchmark.
- » Report detailing each item contained in the assessment along with your Compliant/Non-Compliant status.

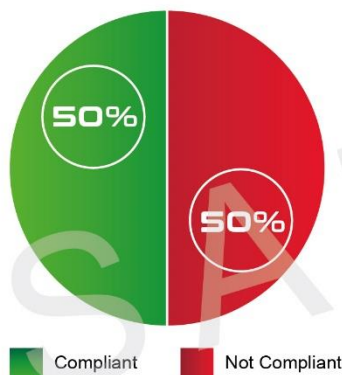
#### ecfirst OCI Report includes:

- » Alignment with CIS Benchmark for OCI Foundations, Level 1 settings
- » Correctly configured settings where further action is required to achieve full security benefits
- » Review of available versus used licenses and their impact
- » Analysis of findings, including strengths and prioritized areas for improvement

#### Configuration benchmark alignment areas include:

- » Identity and access management
- » Network configurations
- » Log management
- » Object storage
- » Asset management

### Executive Dashboard



Area	Total # of CAP Items	Not-Compliant CAP Items	Compliant
IAM	12	3	9
Networking	5	2	3
LogMon	17	12	5
Object Storage	2	1	1
Asset Management	2	1	1
<b>Total</b>	<b>38</b>	<b>19</b>	<b>19</b>

# CIS Benchmark Assessment

Performed Remotely!

## Azure Assessment

### CIS Microsoft Azure Foundations Benchmark v1.3.0 Highlights

The CIS Foundations Benchmarks provide prescriptive guidance for various areas including: Identity and Access Management (IAM), database services, logging and monitoring, networking, virtual machines, and Azure's Security Center and Storage Accounts. Key changes to this new release include:

- » Reference links in multiple recommendations to the CIS Azure Security Benchmark v2
- » Multiple recommendations for the change of Advanced Data Security to Azure Defender. New recommendations for additional Azure Defender bundles
- » Multiple activity log alert console remediation steps
- » Removal of multiple recommendations for features that have been deprecated

### Azure Virtual VM Assessment

The ecfirst An Azure VM Assessment describes:

- » **Azure Readiness:** Whether servers are suitable for migration to Azure.
- » **Monthly Cost Estimation:** The estimated monthly compute and storage costs for running the VMs in Azure.
- » **Monthly Storage Cost Estimation:** Estimated costs for disk storage after migration.

#### ecfirst Azure Report includes:

- » Alignment with CIS Benchmark for Azure Foundations, Level 1 settings
- » Correctly configured settings where further action is required to achieve full security benefits
- » Review of available versus used licenses and their impact
- » Analysis of findings, including strengths and prioritized areas for improvement

#### Configuration benchmark alignment areas include:

- » Identity and access management
- » Data storage
- » Logging functions
- » System monitoring
- » System networking

### Executive Dashboard

#### Compliance Progress



Compliant Not Compliant NA

Area	Compliant	Non-Compliant	N/A
IAM	1	1	0
SecCenter	11	8	0
StorageAccounts	2	1	0
Database	2	9	8
Log-Monitor	9	7	0
Networking	3	2	0
VM	1	2	0
Other	1	2	1
AppService	2	3	0

## Deep Database Assessment

Performed Remotely!

The ecfirst Deep Database Instance Assessment checks for and reports on:

- » Known vulnerabilities on the database instance.
- » Configuration issues based on standards such as NIST, Center for Internet Security (CIS) & Defense Information Systems Agency (DISA) - Security Technical Implementation Guide (STIG).
- » Identification and Access Control issues.
- » Combinations of settings that could lead to escalation of privilege attacks, data leakage, Denial-of-Service (DoS), or the unauthorized medication of data.

### Executive Dashboard

Overall Risk: **High**

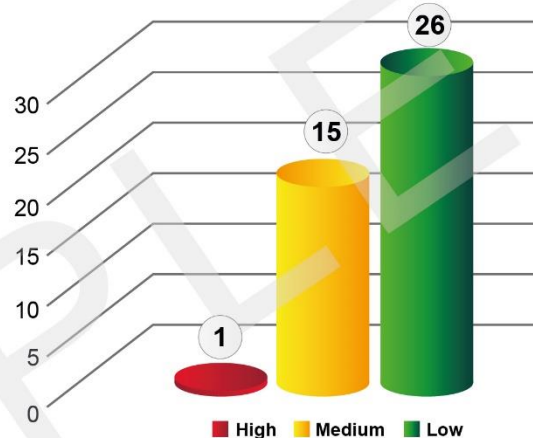
ecfirst scanned specific subnets to identify systems running MSSQL databases that allow open access; by open access we mean access to the login prompt. ecfirst was able to identify 37 database instances that allow open access. This allows an attacker the opportunity to attempt unauthorized logins to the database, as well as attempt to exploit any vulnerabilities associated with the SQL instance.

ecfirst also attempted to login to the identified SQL servers with default or easy to guess credentials. No database instances were discovered using default or easy to guess credentials.

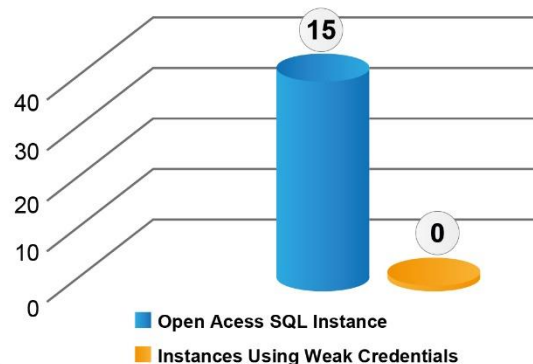
A select database instance was further scanned for known vulnerabilities and misconfiguration issues. During this assessment, ecfirst identified a total of 42 vulnerabilities on the in-scope systems. Within this total number of vulnerabilities, 42 unique vulnerabilities were identified; 16 of these unique vulnerabilities are rated as a **High** or **Medium** risk.

Issue	Impact
Permission on registry extended proc	If not configured properly, the registry extended stored procedures can be used to read or write sensitive information from the registry.

### Database Vulnerability Totals



### SQL Database Instances





## Social Engineering

Performed Remotely!

- ❖ 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

## Virtual ISO & Infosec Staffing Program



### Virtual ISO

As a Virtual ISO (VISO), ecfirst will provide the following services during the engagement:

- Consultation and advice to leadership with respect to the strategic management of the information security program.
- Guidance and counsel to the CEO and key members of the leadership team in defining objectives for information security.
- Work with leadership to oversee the formation and operations of a company-wide information security organization that is organized toward a common goal in information security and compliance.
- Develop and oversee remediation efforts to facilitate compliance with security regulations.
- Manage institution-wide information security governance processes and facilitate the establishment of an information security program and project priorities.
- Coordinate and review incident response procedures.
- Establish annual and long-range security and compliance goals, define security strategies, reporting mechanisms and program services; and create a roadmap for continual program improvements.
- Stay abreast of information security issues and regulatory changes at the state and national level and communicate to leadership on a regular basis about those topics.
- Facilitate development, design, and implementation of proposed updates, enhancements, and new functionality to the information systems so that privacy and security is maintained.
- Identify emerging privacy and security practices and technologies to be assimilated, integrated, and introduced within the organization.
- Support the establishment of company infrastructure to support and guide individual divisions/departments/sites in IT efforts.
- Assess new security threats and vulnerabilities and make recommendations on appropriate avoidance and mitigation strategies.

### InfoSec Service Staffing Program

The InfoSec Service Staffing Program provides our customers with options for short term or long term information security or compliance professionals, including:

- Security Analyst
- Security Professional
- Compliance Professional
- Senior Compliance Analyst
- Senior Cybersecurity Professional

Duration of contract can range from one month, to three months or longer.

Discuss your InfoSec Staff augmentation requirements with ecfirst.  
We will create a cost effective solution to address your priorities.

## Biomed & Internet of Things (IoT) Cybersecurity Readiness



### Biomed Facts: FBI

- The number of internet-connected medical devices is projected to grow from 20 billion in 2018 to 50 billion in 2020.
- Deficient security capabilities, legacy operating systems, difficulties in patching vulnerabilities and a lack of security awareness are significant risks to both medical devices themselves and the networks to which they connect.
- Unsecure or poorly secured medical devices can leave networks open to Distributed Denial of Service (DDoS) attacks.

Source: FBI Alert I-101717a-PSA

Myth	Fact
The FDA is the only federal government agency responsible for the cybersecurity of medical devices.	The FDA works closely with other federal government agencies, such as the U.S. Department of Homeland Security (DHS), but also works with members of the private sector, medical device manufacturers, health care delivery organizations, security researchers, and end users to increase the security of critical cyber infrastructure.
Medical device manufacturers can't update medical devices for cybersecurity.	Medical device manufacturers can always update a medical device for cybersecurity. In fact, the FDA does not typically need to review medical device updates implemented solely to strengthen cybersecurity.
The FDA tests medical devices for cybersecurity.	The FDA does not conduct premarket testing for medical products. Testing is the responsibility of the medical product manufacturer.

### ecfirst Biomed & IoT Cybersecurity Services

- Biomed Risk Assessment (HIPAA, HITRUST®, NIST Cybersecurity Framework)
- Biomed Cybersecurity Assessment
- Biomed Policy and Procedure
- Biomed Cybersecurity Remediation
- Complimentary seat in industry leading Certified Cyber Security Architect<sup>SM</sup> (CCSA<sup>SM</sup>) program
- Knowledge transfer throughout the biomed cybersecurity assessment
- Unconditional Guarantee. No Questions! ecfirst will not consider an engagement complete unless client is 100% satisfied

### Biomed Business Risks

- Disruption of patient care
- Loss of Protected Health Information (PHI) and Personally Identifiable Information (PII)

### Biomed & IoT Cybersecurity Readiness

The ecfirst Biomed and IoT Cybersecurity Report includes an Asset Inventory, which identifies specific biomed device information such as:

- IP Address
- Hostname (if resolvable or successfully authenticated)
- Operating System (if discoverable or successfully authenticated)
- Open Ports
  - Potentially Active Services
- Installed Software



## Biomed & Internet of Things (IoT) Cybersecurity Readiness



### Securing IoT & Biomed Devices

- Equipment Management
- Patch Management
- Staff Security Training
- Vulnerability Scanning
- Risk Management
- RFP Language to Include Security Features
- Device Integration Test Lab

### Biomed Devices

- Pacemakers
- Personal Fitness Devices
- Drug Pumps
- Medical Ventilators
- Mobile Medical Systems
- Medical Monitors
- In-Home Monitors
- Medical Imaging Machines

### Training & Certification



- Examine how to establish a cybersecurity program based on the NIST Cybersecurity Framework.
- Step through key areas that must be addressed in a credible incident response plan.
- Walk through core components, organization and CMMC Maturity Levels. Examine CMMC domains and CMMC capabilities required for organizations.

### ecfirst Biomed Cybersecurity Checklist

- ☒ **Cybersecurity Framework** Determine the cybersecurity framework that will establish the foundation for your security program requirements for medical IoT devices.
- ☒ **Policy** Develop a cybersecurity policy specific to medical IoT devices. Ensure the policy is reviewed by associated and impacted departments/business units, approved by senior leadership, and communicated to the workforce.
- ☒ **Security Risk Assessment** Ensure medical IoT devices are within the scope of enterprise cybersecurity risk assessment exercises. Perform a vulnerability assessment to determine medical IoT device security gaps. Examine the security architecture and identify opportunities to possibly segregate medical IoT devices (i.e. determine application of segregation for medical IoT devices).
- ☒ **Business Associate Agreements (BAA)** Review third-party vendors (business associates) and their security practices to ensure HIPAA, FDA, and other mandates are appropriately addressed.
- ☒ **Configuration Management** Ensure each type of medical IoT device is configured consistently, and addresses the appropriate security capabilities to secure PHI and PII.
- ☒ **Encryption** Examine options to encrypt PHI and PII stored, processed or transmitted by medical IoT devices.
- ☒ **Risk Management** Based on the findings of the risk assessment, establish a plan for risk management of medical IoT devices. Ensure formal remediation is performed on a regular schedule (e.g. monthly).

## First HIPAA Program in the U.S. Healthcare Industry!

Virtual | On-site | Public Schedule



### Learn HIPAA. Know HIPAA!

The Health Insurance Portability and Accountability Act (HIPAA) is about insurance portability, fraud, and administrative simplification.

This Certified HIPAA Professional (CHP) certification training helps you better understand HIPAA's Administrative Simplification Act as well as how to create a framework for initiating and working towards a blueprint for HIPAA compliance.



### Learning Objectives

- Analyze the latest updates in HIPAA Privacy, HIPAA Security and HITECH Breach mandates.
- Understand the OCR Audit Protocol, an important guidance for HIPAA compliance.
- Examine recent OCR HIPAA settlements, including required corrective action plans.
- Review HIPAA compliance best practices for covered entities and business associates.
- Step through relevant NIST standards and HITRUST® Certification for HIPAA compliance.



### Target Audience

CHP training class program targets:

- Compliance Officers
- Privacy and Security Officials
- Healthcare Executives
- Senior Clinicians
- Chief Information Officers (CIOs)
- Legal Professionals
- IT Professionals

### Program Testimonials

"This HIPAA Academy CHP course is definitely an essential training aid for anyone working in the areas of Privacy & Security. I'd definitely recommend the course to all healthcare facilities and covered entities who must comply with HIPAA. The course provided outstanding detailed information to us."

**Felicia Burks | United States Army**

"Highly detailed specific information. The CHP Course was extensive and course handbook looks to be a good reference for future use."

**Mike Fuller | State of Mississippi Dept. of Health**

## The World's First Program Focused on Compliance & Cybersecurity

Virtual | On-site | Public Schedule



### Distinguish Yourself in the Marketplace

Get the CSCS™ Credential! Just having a background in IT or information security is not sufficient anymore for the challenges of business today. Employers are looking for individuals who not only have IT skills but also understand compliance regulations that impact their industry and business – because these are priorities that must be met.



### Learning Objectives

- Step through industry standards such as PCI DSS, GDPR, ISO 27001, HIPAA, and FISMA.
- 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.



### Target Audience

The CSCS™ program is of value to compliance professionals and managers, information security officers, security practitioners, privacy officers, internal compliance auditors and senior IT professionals.

### Modules

- Module 1: State of Cybersecurity
- Module 2: Critical Issues of Today
- Module 3: Regulations and Frameworks: Getting Started
- Module 4: ISO/IEC 27K Series
- Module 5: PCI DSS
- Module 6: Healthcare Information Security Regulations
- Module 7: U.S. Federal Regulations
- Module 8: NIST Frameworks and Guidance
- Module 9: U.S. State Regulations
- Module 10: GDPR
- Module 11: Incident Response Plan (IRP)
- Module 12: Business Continuity Plan (BCP)

### Program Testimonials

"Instructor was very enthusiastic and made the class more interesting. It was a great overall discussion of all the standards and regulations including certifications that businesses have to comply with. Rating of CSCS™ course: 10. Rating of instructor: 10."

**Michael Carr | Beacon Health Options**

"The CSCS™ Program covered several information security areas including ISO 27000, HIPAA, PCI DSS, FISMA and others. I really liked the way the whole program was delivered by instructor. Covered the landscape of global information security and compliance. This program brings a lot of energy and passion towards the subject and a good sense of humor while delivering these complex topics. Would highly recommend others to take this certification program."

**V. Ashok Kumar | episource India Pvt. Ltd**



## An Executive Cyber Security Program

Virtual | On-site | Public Schedule



### Step through U.S. DoD Cybersecurity Mandate: CMMC

CCSA<sup>SM</sup> is an instructor-led 1-day program. The program validates knowledge and skill sets in cybersecurity with focus on the NIST Cybersecurity Framework, and the U.S. DoD cybersecurity mandate, CMMC. Core topics emphasized include establishing a credible, evidence-based enterprise cybersecurity program and developing a comprehensive incident response plan.



### Learning Objectives

- Examine how to establish a cybersecurity program based on the NIST Cybersecurity Framework.
- Step through key areas that must be addressed in a credible incident response plan.
- Walk through core components, organization and CMMC Levels.
- Review encryption implementation across the enterprise to mitigate business risk.



### Target Audience

- Information Security Officers
- Security Practitioners
- Privacy Officers
- Senior IT Professionals
- Compliance Professionals & Managers

### Program Testimonials

“Clearly educates the students to know NIST Cybersecurity Framework and how to use it in the real-world cybersecurity field. The instructor is very knowledgeable with solid experience from cybersecurity consulting engagements. So, the students can learn the practical cybersecurity assessment and risk management skills. I strongly recommend this course for NIST Cybersecurity Framework training and awareness education. Overall Rating of Course: 10. Overall Rating of the Instructor: 10.”

**Bin Du | McAfee**

“Long-time expertise of the instructor and a very logical layout of the course material were strengths of the CCSA<sup>SM</sup> Program. For a non-IT HIPAA professional like myself, this course gave a comprehensive, but easy-to-understand structure for integrating privacy and security requirements. Overall rating of Course: 10. Overall rating of Instructor: 10.”

**Brett Shrader, Privacy Officer | Beacon Health Options**



## Training Program



### Summary

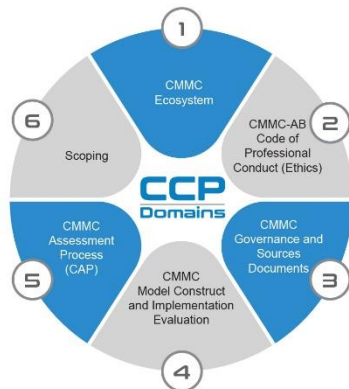
This Certified CMMC Professional (CCP) exam will verify a candidate's knowledge of the Cybersecurity Maturity Model Certification (CMMC), relevant supporting materials, and applicable legal and regulatory requirements to protect Federal Contract Information (FCI) and Controlled Unclassified Information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

### Authoritative Source

The Department of Defense (DoD) is the authoritative source for CMMC documentation.

<https://dodcio.defense.gov/CMMC/>

### Certified CMMC Professional (CCP)



### 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 CompTIAA+ or equivalent knowledge/experience.
  - ◆ Complete CCP Class offered by a Licensed Training Provider (LTP).
  - ◆ Pass DoD CUI Awareness Training no earlier than three (3) months prior to the exam.
- ◆ <https://securityhub.usalearning.gov/index.html>

### All Content is Digital



### 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
- ◆ Candidate CMMC Assessment Team Members

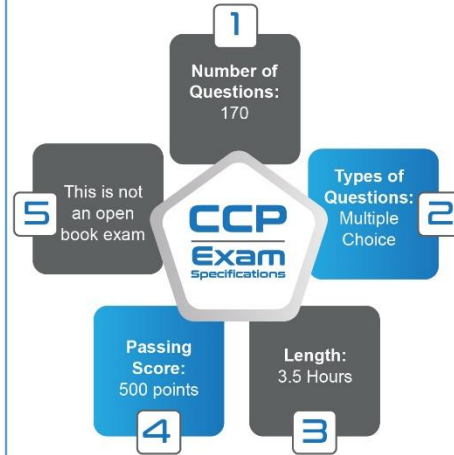


## Training Program



#	Domain	Exam Weight	CCP Program	36 Hours
1	CCP Pre Program Prep			2 Hours
2	CMMC Ecosystem	5%	Domain 1, 2 & 3 Tuesday, Day 1 8:30 am - 4:30 pm Offline Prep: 2 Hours	10 Hours
3	The Cyber-AB Code of Professional Conduct (Ethics)	5%		
4	CMMC Governance and Sources Documents	15%		
5	CMMC Model Construct and Implementation Evaluation	35%	Domain 4 Wednesday, Day 2 8:30 am - 4:30 pm Offline Prep: 2 Hours	10 Hours
6	CMMC Assessment Process (CAP)	25%	Domain 5 Thursday, Day 3 8:30 am - 4:30 pm Offline Prep: 2 Hours	10 Hours
7	Scoping	15%	Domain 6 & Review Friday, Day 4 8:00 am - 12:00 pm	4 Hours
8	Practice Exam & Review			

### CCP Exam Specifications



<https://academy.ecfirst.com>



Welcome  
Validity expires April 15, 2024

Home Manage MFA Logout

## Certified CMMC Professional



Updated for CMMC 2.0

Evaluation Form

CCP Pretest

Classroom

Research

Quiz

Assessor Toolkit

CMMC Practices

CMMC Readiness

Final Practice Exam

### Quick Reference

User Guide  
CMMC Infographics  
Roles & Responsibilities  
CMMC Source Documents  
CCP Presentation Slides  
NIST Reference Documents  
CMMC Handbook  
CMMC Placeholder Quiz  
CCP Practice Quiz  
CMMC Glossary  
CMMC Acronyms  
Controlled Unclassified Information (CUI)  
Instructor, Restricted





**Training  
Program**



## Day 1 | Tuesday

8:30 am to 4:30 pm | Lunch Duration: 30 Mins.  
Offline Prep: 2 Hours

10  
Hours

Content Presentation | Domain Review | Quiz

CCP Pre Program Prep

2  
Hours

### Introduction

#### Domain 1: CMMC Ecosystem

Task 1 Identify and compare roles/responsibilities/requirements of authorities across the CMMC Ecosystem.

#### Domain 2: The Cyber-AB Code of Professional Conduct (Ethics)

Task 1 Identify and apply your knowledge of the Guiding Principles and Practices of the Cyber-AB Code of Professional Conduct (CoPC)/ISO/IEC/DoD requirements.

#### Domain 3: CMMC Governance and Sources Documents

Task 1 Demonstrate your understanding of FCI and CUI in non-federal unclassified networks.

Task 2 Determine the appropriate roles/responsibilities/authority for FCI and CUI.

Task 3 Demonstrate your understanding of the CMMC Source and Supplementary documents.

## Day 2 | Wednesday

8:30 am to 4:30 pm | Lunch Duration: 30 Mins.  
Offline Prep: 2 Hours

10  
Hours

Content Presentation | Domain Review | Quiz

#### Domain 4: CMMC Model Construct and Implementation Evaluation

Task 1 Given a scenario, apply the appropriate CMMC Source Documents as an aid to evaluate the implementation/review of CMMC practices.

Task 2 Apply your knowledge of the CMMC Assessment Criteria and Methodology, to the appropriate CMMC practices.

Task 3 Analyze the adequacy/sufficiency around the location/collection/quality/usage of Evidence.



# Training Program



## Day 3 | Thursday

8:30 am to 4:30 pm | Lunch Duration: 30 Mins.  
Offline Prep: 2 Hours



Content Presentation | Domain Review | Quiz

### Domain 5: CMMC Assessment Process

Task 1	Choose the appropriate roles of the CCP in the CMMC Assessment Process when developing the assessment plan (Phase 1 – Plan and Prepare Assessment).
Task 2	Apply CMMC Assessment Process requirements pertaining to the role of the CCP as an assessment team member while conducting a CMMC assessment (Phase 2 – Conduct Assessment).
Task 3	Demonstrate your comprehension of the CCP role in the preparation of assessment report (Phase 3 – Report Assessment Results).
Task 4	Demonstrate your comprehension of the CCP role in the process of evaluating outstanding assessment issues on Plan of Action and Milestones (POA&M) (Phase 4 – Evaluation of Outstanding Assessment POA&M Items).
Task 5	Given a scenario, determine the appropriate phases/steps to assist in the preparation/conducting/reporting on a CMMC Level 2 Assessment.

## Day 4 | Friday

8:00 am to 12:00 pm



Content Presentation | Domain Review | Quiz

### Domain 6: Scoping

Task 1	Understand CMMC High-Level Scoping as described in the CMMC Assessment Process.
Task 2	Given a Scenario, analyze the organization environment to generate an appropriate scope for FCI Assets.



Practice Exam



Review



## Training Program



### Summary

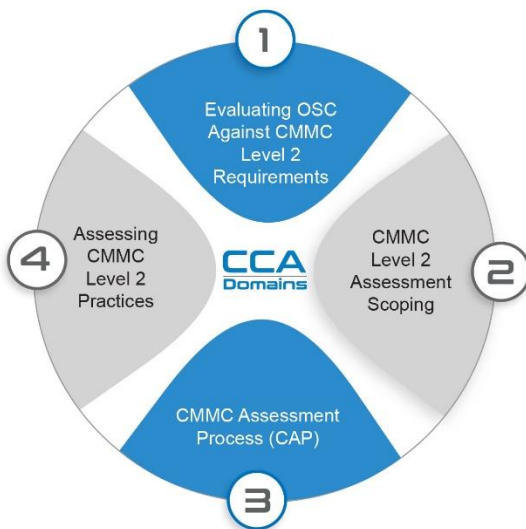
This Certified CMMC Assessor (CCA) exam will verify a candidate's readiness to perform as an effective Certified Assessor of Organizations Seeking Certification (OSC) at CMMC Level 2. A passing score on this CCA exam is a prerequisite to a CMMC Lead Assessor designation.

### Authoritative Source

The Department of Defense (DoD) is the authoritative source for CMMC documentation.

<https://dodcio.defense.gov/CMMC/>

### Certified CMMC Assessor (CCA)



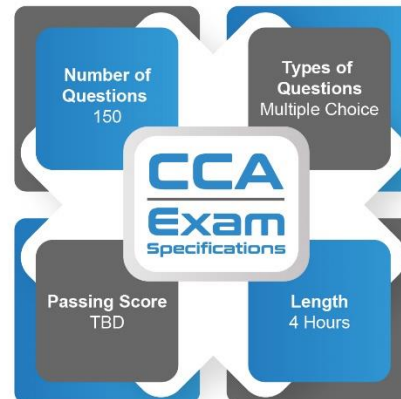
### Intended Audience

- ◆ CCP seeking to advance to CCA.
- ◆ Certified CMMC Instructors who wish to teach the CCA course.

### All Content is Digital



### CCA Exam Specifications





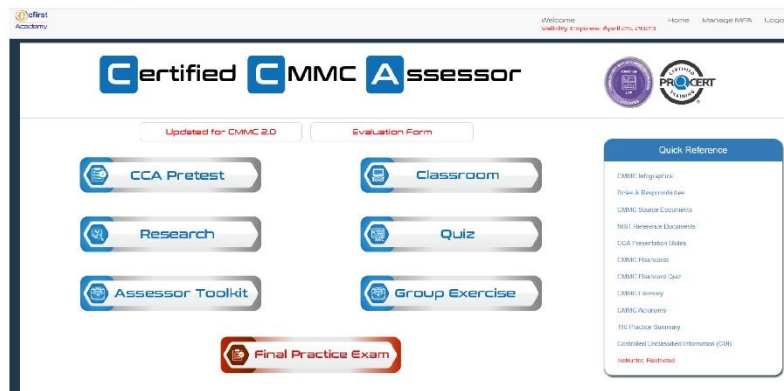


# Training Program



#	Domain	Exam Weight	CCA Program	36 Hours
1	CCA Pre Program Prep			2 Hours
2	Welcome Introductions, About the Portal and Pre-Quiz			
	Introduction			
	Evaluating OSC Against CMMC Level 2 Requirements	15%		
3	CMMC Level 2 Assessment Scoping	20%		
4	CMMC Assessment Process (CAP)	25%		
5	Assessing CMMC Level 2 Practices	40%		
6	Practice Exam & Review			

<https://academy.ecfirst.com>





# Training Program



## Day 1 | Tuesday

8:30 am to 4:30 pm | Lunch Duration: 30 Mins.  
Offline Prep: 2 Hours

10  
Hours

Content Presentation | Domain Review | Quiz

### CCA Pre Program Prep

2  
Hours

Welcome Introductions, About the Portal and Pre-Quiz

### Introduction

#### Domain 1: Evaluating OSC Against CMMC Level 2 Requirements

Task 1 Assess the various environmental considerations of OSCs against CMMC L2 practices.

#### Domain 2: CMMC Level 2 Assessment Scoping

Task 1 Analyze the CMMC Assessment Scope of Controlled Unclassified Information (CUI) Assets as they pertain to a CMMC assessment using the five categories of CUI assets as defined in the CMMC Level 2 Assessment Scoping Guide.

Task 2 Given a scenario, analyze the CMMC Assessment Scope based on the predetermine CUI categories within the CMMC Level 2 Assessment Scoping Guide.

Task 3 Evaluate CMMC assessment scope considerations based on the CMMC Level 2 Assessment Scoping Guide.

## Day 2 | Wednesday

8:30 am to 4:30 pm | Lunch Duration: 30 Mins.  
Offline Prep: 2 Hours

Content Presentation | Domain Review | Quiz

### Domain 3: CMMC Assessment Process (CAP)

Task 1 Given a scenario, apply the appropriate phases and steps to plan, prepare, conduct, and report on a CMMC Level 2 Assessment.

## Day 3 | Thursday

8:30 am to 4:30 pm | Lunch Duration: 30 Mins.  
Offline Prep: 2 Hours

10  
Hours

Content Presentation | Domain Review | Quiz

### Domain 4: Assessing CMMC Level 2 Practices

Task 1 Identify evidence verification/validation methods and objects for Practices based on the CMMC Level 2 Assessment Guide and CAP documentation.

## Day 4 | Friday

8:00 am to 12:00 pm

4  
Hours



Practice Exam



Review

Ali Pabrai



U.S. Department of Defense  
CMMC Program



## Global Cyber Defense Thought Leader

MSEE | CISSP (ISSAP | ISSMP) | CMMC (CCA, CCP, PA, PI, RPA, RP) | HITRUST® CCSFP | Security+



Mr. Ali Pabrai, a global cybersecurity & compliance expert, is the chairman & chief executive of ecfirst. A highly sought after professional, he has successfully delivered solutions to U.S. government agencies, IT firms, healthcare systems, legal & other organizations worldwide. His career was launched with the U.S. Department of Energy's nuclear research facility, Fermi National Accelerator Laboratory. He has served as vice chairman and in several senior officer positions with NASDAQ-based firms.

Mr. Pabrai has led numerous engagements worldwide for ISO 27001, PCI DSS, NIST, CMMC, GDPR, CCPA, FERPA, HITRUST CSF and HIPAA/HITECH. Mr. Pabrai served as an Interim CISO for a health system with 40+ locations.

Mr. Pabrai has presented passionate briefs to tens of thousands globally, including the USA, United Kingdom, France, Taiwan, Singapore, Canada, India, UAE, Saudi Arabia, Philippines, Japan, Ireland, Bahrain, Jordan, South Africa, Egypt, Ghana and other countries.

He is a globally renowned speaker who has been featured as a keynote as well as moderated cybersecurity conferences. Mr. Pabrai is the author of several published works. Clients that Mr. Pabrai has delivered to have included the U.S. Defense Intelligence Agency (DIA), and the U.S. Naval Surface Warfare Center.

Mr. Pabrai was appointed and served (2017) as a member of the select HITRUST CSF Assessor Council. Mr. Pabrai is a proud member of the InfraGard (FBI).

"We have had the true pleasure of working with Ali Pabrai at conferences all over the world during the past few years – with one unanimous word that keeps resounding among audiences and staff alike – **AWESOME!**"

Michael Mach | Conference Program Manager | ISACA



## FBI Conference



"Pabrai's presentation style is engaging, and he encourages questions and discussions. I would recommend him for future presentations and trainings."

Josh More | Cyber Sector Chief | Iowa FBI InfraGard

"On behalf of the Idaho InfraGard (FBI), I would like to thank Pabrai for presenting at our conference. Pabrai is the kind of speaker you want to bring to executives and staff. He says it in a simple, no nonsense way, in a manner that everyone can understand."

Rachel Zahn | President | InfraGard (FBI) | Idaho Alliance

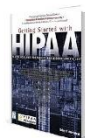
"You delivered a fantastic presentation and we all felt your passion for cyber security."

James E Lamadrid | Supervisory Special Agent | Federal Bureau of Investigation (FBI) | Cyber Task Force

"Thank you Pabrai. Your enthusiasm and relevance for the Information Security material you presented at our combined InfraGard (FBI) conference in Idaho Falls was very well received and pertinent to both our chapter as an organization and the constituents in attendance."

"As a government employee, I appreciated the simplified insight of highlighting the importance of compliance and funding compared to information security success beyond qualitative metrics. I heard many times over that your specific information with measurable results made your material directly relevant to individuals, businesses and organizations. Thanks again and I hope you are able to join us again in the future."

Clark Harshbarger | FBI



Getting Started with HIPAA

First published book on HIPAA



UNIX Internetworking

First book on UNIX & Networks



Internet & TCP/IP Network Security

First book on TCP/IP security

The ecfirst DoD CMMC Ecosystem



Achieve CMMC Certification







**Corporate Office**

295 NE Venture Drive  
Waukee, IA 50263  
United States

**Kris Laidley**

Team Lead, Business Development &  
Certification Program

Email: [Kris.Laidley@ecfirst.com](mailto:Kris.Laidley@ecfirst.com)

