











# ecfirst

AI Defense, *Beyond Cyber*

## Table of Contents

About 	3
 ASSET RISK MANAGEMENT	4
Online Learning	14
<b>Compliance Services</b>	
HIPAA & HITECH	20
PCI DSS	21
ISO 27001	22
GDPR	24
 Authorized External Assessor	25
<b>Cybersecurity Services</b>	
NIST	26
On-Demand Consulting	27
Managed Cybersecurity Services Program (MCSP)	28
BIA & IT Disaster Recovery Plan	29
Risk Analysis	30
Cybersecurity Assessment & Penetration Testing	31
Virtual ISO& Infosec Staffing Program	50
Biomed & IoT	51
<b>Certification Training</b>	
 HIPAA Assessor	53
 CERTIFIED SECURITY	54
 Certified Cyber Security Architect	55
CMMC	56
 Certified Chief Information Professional	57
 Certified CMMC Assessor	59
About Uday Ali Pabrai	61



### Consulting Practice



### Certification Training



AI Defense, Beyond Cyber



Cyber Defense Platform



### Cyber Defense Platform

02 Compliance Portals

07 Remediation Portal  
Cybermapper

03 Assessment Portal  
Policy Portal

08 Vendor Management  
Asset Management

04 Procedure Portal  
Evidence Portal

09 Incident, Breach &  
Ransomware Portal

05 HIPAA Portal  
GDPR Portal

06 NIST Cyber Portal  
NIST 171 Portal

10 Executive Dashboard







Cyber Defense Platform



### Assessment Portal

Search...



Cybersecurity

Back

Home / Cybersecurity

Data Collection Form

### Policy Portal

Search...



Dashboard

Back

Home / Policy / Dashboard

Security Policy Library

Upload Create Refresh

Search:

Show more 3

File Name	File Type	File Size	Action
Implement Subnetworks Policy	PDF	1.2 MB	
Limit System Access to Types of Transaction Policy	DOCX	297.4 KB	
Escort and Monitor Visitors Policy	DOCX	150 KB	

Privacy Policy Library

Upload Create Refresh

Other Policy Library

Upload Create Refresh



Cyber Defense Platform



## Procedure Portal

Search...

**TRACER**  
ASSET RISK MANAGEMENT  
ABC CORP

**Dashboard** Back

Home / Procedure / Dashboard

**Security Procedure Library** Upload Create Index

Search  Show more 3

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

**Privacy Procedure Library** Upload Create Index

**Other Procedure Library** Upload Create Index

## Evidence Portal

Search...

**TRACER**  
ASSET RISK MANAGEMENT  
ABC CORP

**Evidence Portal** Back

Home / Evidence Documents

Upload Your Files here  Notify Client

Upload

Search:  Show 10 entries

File Name	Created On	Action	Select All <input type="checkbox"/>
HIPAA Awareness.pdf	Jul 26, 2023 07:12:36 AM	<a href="#">Download</a> <a href="#">Delete</a>	<input type="checkbox"/>
NIST CSF Risk Assessment Report.doc	Jul 25, 2023 07:04:59 AM	<a href="#">Download</a> <a href="#">Delete</a>	<input type="checkbox"/>
Joint Security Meeting.doc	Feb 1, 2023 04:32:40 AM	<a href="#">Download</a> <a href="#">Delete</a>	<input type="checkbox"/>

Previous 1 Next



Cyber Defense Platform



## HIPAA Portal

Search...



### HIPAA Risk Assessment

Back

Home / Data Collection Forms / HIPAA Risk Assessment

 General Information	 Interview Schedule	 Policy Analysis	 Procedure Analysis
 Security Control Analysis	 Artifacts	 Site Walkthrough	 Cloud Analysis

## GDPR Portal

Search...



### Global Data Protection Regulation (GDPR)

Back

Home / Data Collection Forms / GDPR

General Questionnaire	0%
<b>GDPR Article 5</b>	<b>0%</b>
GDPR Article 6	0%
GDPR Article 7	0%
GDPR Article 8	0%
GDPR Article 9	0%
GDPR Article 10	0%
GDPR Article 12	0%

#### GDPR Article 5

Status: 0% 1/7

##### Principles relating to processing of personal data

1. Personal data shall be:

- a. Processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency);
- b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (purpose limitation);
- c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);
- d. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy);
- e. Kept for no longer than is necessary for the purposes for which the personal data are processed (storage limitation).

[Upload Policy Documents](#) [Map Uploaded Policy Documents](#)

Uploaded Policy Files

1 (a) (DCF) How does your organization process personal data about the data subject?





Cyber Defense Platform



## NIST Cybersecurity Framework Portal

Search...

TRACER ASSET RISK MANAGEMENT  
ABC CORP

**NIST Policy** Back

Home / Data Collection Forms / NIST DCF / NIST Policy

Identify **0%** Protect **0%** Detect **0%** Respond **0%** Recover **0%**

#	QUESTION	MAP	ANSWER
1	Do you have a policy for identifying and managing data, personnel, devices, systems, and facilities?		Select
2	Do you have a policy for identifying and managing your organization's mission, objectives, stakeholders, and activities?		Select
3	Do you have a policy for identifying and managing your organization's regulatory, legal, risk, environmental, and operational requirements?		Select
4	Do you have a policy for identifying and managing your cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals?		Select

## NIST SP 800-171 Portal

Search...

TRACER ASSET RISK MANAGEMENT  
ABC CORP

**NIST SP 800-171** Back

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

**D1: Access Control** **Access Control Status 0%** 1/28

D2: Awareness and Training  
D3: Audit and Accountability  
D4: Configuration Management  
D5: Identification and Authentication  
D6: Incident Response  
D7: Maintenance  
D8: Media Protection  
D9: Personal Security  
D10: Physical Protection  
D11: Risk Assessment

**3.1.1 Does your organization limit system access to authorized users or devices?**

Yes No N/A Process only: No documentation available

Justification

1 2 3 4 5 6 7 8 9 10 ... 27 28 Next



Cyber  
Defense  
Platform



## Remediation Portal

Search...

TRACER SM  
ASSET RISK MANAGEMENT  
ABC CORP

Remediation Management Back

Home / Remediation Management

HIPAA  
CAP

Cybersecurity  
CAP

Pen Test  
CAP

## Cybermapper

Search...

TRACER SM  
ASSET RISK MANAGEMENT  
ABC CORP

Cybermapper View Back

Home / Cybermapper View

What would you like to see the mapping table for?

Show

**HIPAA to NIST SP 800-53r5 Mapping**

HIPAA	NIST SP 800-53 r5
<b>Administrative Safeguards</b>	
164.308(e)(1)(ii) Security Management Process STD	RA-1 Risk Assessment Policy and Procedures The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk



Cyber Defense Platform



## Vendor Management

Search...

**TRACER**  
ASSET RISK MANAGEMENT  
**ABC**  
CORP

Vendor Management Back

Home / Vendor Management

Total # of Vendor(s)	4	Pending Vendor(s)	4	Total # of Vendor(s) Assessed	0	Total # of Vendor(s) Permitted	4
----------------------	---	-------------------	---	-------------------------------	---	--------------------------------	---

Vendor Administration Onboarding Vendor Onboarding Vendor

Vendor(s) Status

Vendor 1	Vendor 2	Vendor 3	Vendor 4
33%			

## Asset Management

Search...

**TRACER**  
ASSET RISK MANAGEMENT  
**ABC**  
CORP

Asset Management Back

Home / Asset Management

Total # of Assets(s)	2	Pending Assets(s)	1	Total # of Assets(s) Assessed	1
----------------------	---	-------------------	---	-------------------------------	---

1	Epic	John Smith	john.smith@epic.com	john.smith@assettracer.com	Oct 24, 2023
---	------	------------	---------------------	----------------------------	--------------



Cyber  
Defense  
Platform



## Incident, Breach & Ransomware Portal

Search...

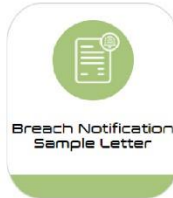
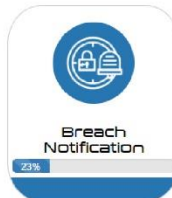


Incident, Breach & Ransomware Portal

Back

Home / Incident, Breach & Ransomware Portal / Incident Management

### Incident Management







Cyber  
Defense  
Platform



## Executive Dashboard

Search...



### Executive Dashboard

Back

Home / Executive Dashboard

#### Report Card

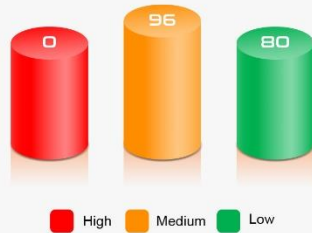
- B-** External Network
- B+** Internal Network
- C-** Wireless Network
- D-** Firewall Configuration
- C-** Overall Security Grade

#### Risk Summary

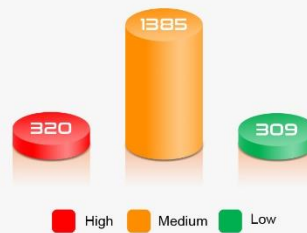


▶ An overall Security Grade: **C-** ▶ An overall Security Risk: **High**

#### External System Risk



#### Internal System Risk





## Online Learning Portal



**AI** Cyber Defense Academy Risk Management  
A One-Day Training

**CHP** Certified HIPAA Professional  
HIPAA Academy

**CSCS**  
CERTIFIED SECURITY COMPLIANCE SPECIALIST

**CISA**  
Certified Cyber Security Architect



HIPAA

Blockchain

Social Engineering

Ransomware Readiness

NIST Cybersecurity Framework

IoT + DDoS = Disruptive Risk

CCPA & CPRA

GDPR



### Features and Capabilities

Online 24x7x365

- 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 Responsive design supports a diversity of devices
- 12 Corporate logins available, with multiple users embedded as teams, including tracking each user's progress by the administrator
- 13 Smart email notifications
- 14 Customizable real-time reports
- 15 Social learning features
- 16 ADA 508 compliant – Flexible Zoom options



# Online Learning Portal



## Logging In



Welcome

Enter Your Username

Enter Your Password

Forgot My Password

Sign In

The ecfirst CMMC Ecosystem

The ecfirst HIPAA Ecosystem

© ecfirst. All Rights Reserved. 2024

## CMMC Certification Training



Certified CMMC Professional



- Updated for CMMC 2.0
- Classroom
- Quiz
- Assessor Toolkit
- CMMC Practices
- Final Practice Exam

Quick Reference

- CCP Pretest
- Research
- Assessor Toolkit
- CMMC Readiness

Certified CMMC Assessor



- Updated for CMMC 2.0
- Classroom
- Quiz
- Group Exercise
- Final Practice Exam

Quick Reference

- CCA Pretest
- Research
- Assessor Toolkit
- CMMC Readiness

Quick Reference

- CMMC 2.0 PowerBall, December 2020
- CMMC 2.0 Overview
- CMMC 2.0 Security Checklist
- NIST Behavioral Checklist
- CCM Preparation Guide
- CMMC Handbook
- CMMC Handbook Set
- CMMC Handbook
- CMMC Assessment
- 11 - Guidance Summary
- Shared Responsibility
- Customer/Supplier Information (C-2)



# Online Learning Portal



## Enduser Training

## CMMC End User Courses





# Online Learning Portal



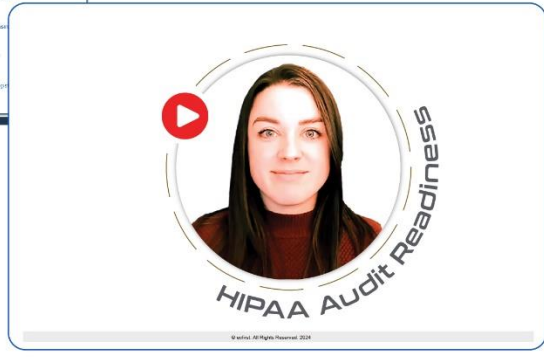
## CHP Certified HIPAA Professional HIPAA Academy



Evaluation Form

- Quick Links
- HIPAA Policy Book
  - HIPAA Security Rule
  - CSA Health Equity Vulnerability Migration Guide
  - H-IR Guidance
  - Webinars
  - HIPAA Audit Preparation
  - Bookstore
  - OCR Self-Practices
  - OCR Remedial Solutions
  - HIPAA Compliance
  - Control Profiles and Plans
  - Regulatory Updates
  - Event Management
  - Apprentice
  - GDPR/HIPAA Video Tapes
  - Advanced Learning

- CHP Manual
- CHP Quick Reference Card
- CHP Online Slides
- CHP Module Quiz
- CHP Practice Quiz
- CHP Certification Exam



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



- Quick Links
- NIST References
  - GDPR References
  - CCPA & CPRA
  - PCI DSS Reference
  - Awareness Training

- CSCS<sup>™</sup> Manual
- CSCS<sup>™</sup> Quick Reference Card
- CSCS<sup>™</sup> Online Slides
- CSCS<sup>™</sup> Module Quiz
- CSCS<sup>™</sup> Practice Quiz
- CSCS<sup>™</sup> Certification Exam



# Online Learning Portal



Evaluation Form



**Quick Links**

- NIS1 References
- CSAMC Reference
- Ransomware References
- Encryption Reference



© ecfirst. All Rights Reserved. 2024



## Risk Management

A One-Day Training

### AI Cyber Academy

Home / AI Cyber Academy

Back



**AI Cyber Exam Information**

**Quick Links**

- edRPA Resources
- RISIT References
- AI RISIT RMF Policy Index



© ecfirst. All Rights Reserved. 2024



# Online Learning Portal



## Online Certification Training





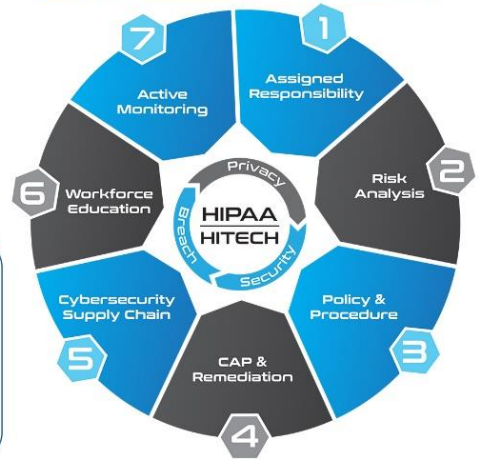
# HIPAA & HITECH



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.

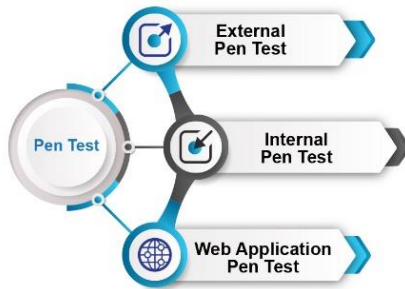
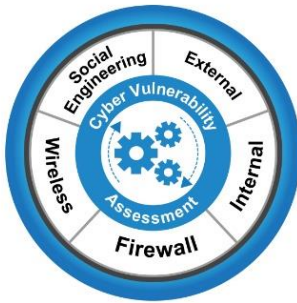
- ④ Perform a comprehensive and thorough HIPAA Risk Assessment.
- ④ Conduct a Cybersecurity Assessment to identify gaps.
- ④ Develop tailored suite of policies and procedures.
- ④ Deliver certification training providing in-depth coverage of HIPAA.
- ④ Remediate cybersecurity and compliance gaps.
- ④ Create customized incident response, cybersecurity, and disaster recovery plans.

## HIPAA Compliance Lifecycle



### HIPAA Services

### Trust ecfirst with HIPAA



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

- ④ Analyze the latest updates in HIPAA Privacy, HIPAA Security and HITECH Breach mandates.
- ④ Examine OCR HIPAA settlements to understand the bar for HIPAA compliance.
- ④ Review HIPAA compliance challenges and best practices for covered entities and business associates.





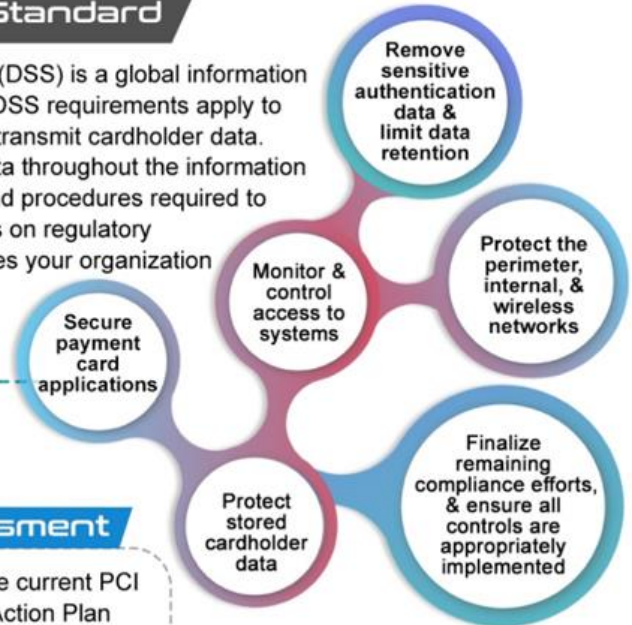
# PCI DSS Services



## 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



## 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.

# ISO 27001 Services

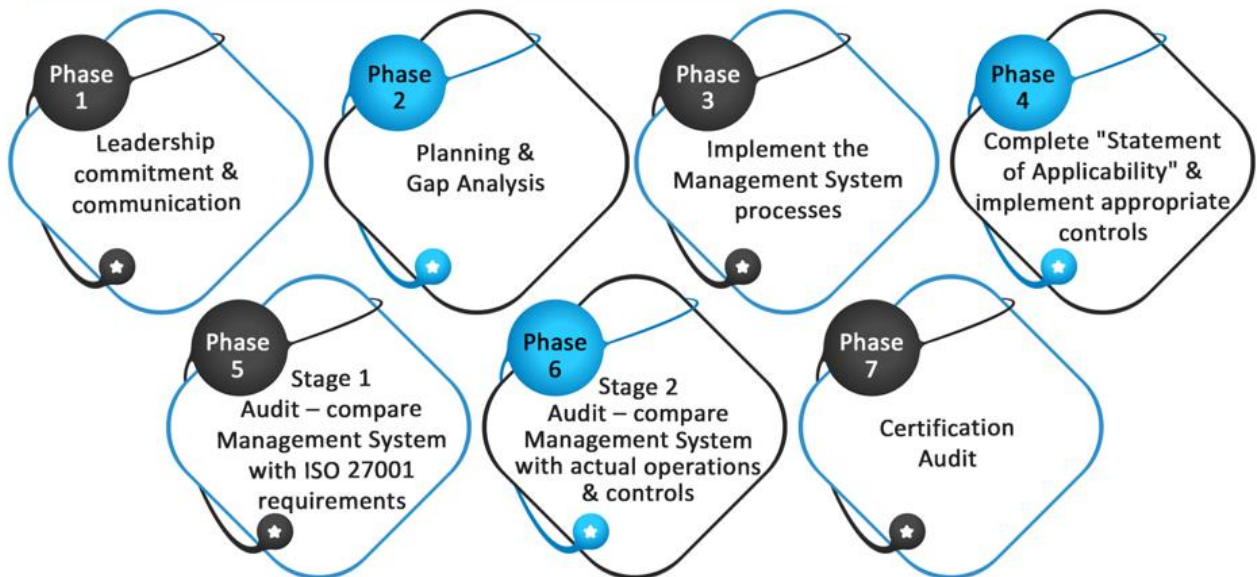


Organizations are increasingly considering applying the family of ISO 27001 international security standards to comply with various U.S. Federal and state regulations such as HIPAA, HITECH, as well as standards such as the PCI DSS. The ISO 27001 is a global standard that provides a comprehensive framework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



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.

### 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 Policy

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

### 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.

### ISO 27001 Webcast

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

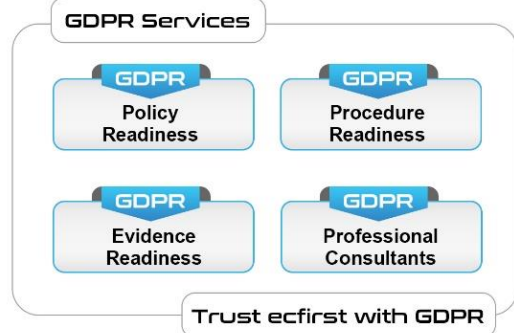


# GDPR Services

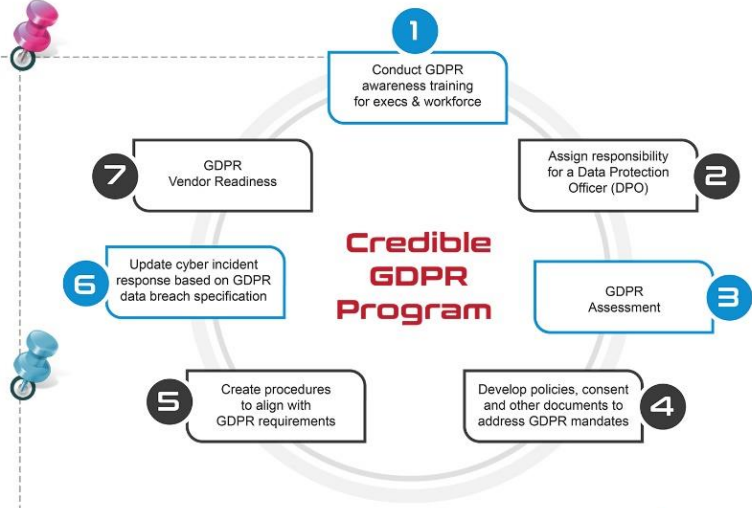


The General Data Protection Regulation (GDPR) unifies the regulations within the European Union (EU). Discuss GDPR with ecfirst. ecfirst offers a complete range of GDPR compliance solutions, including:

- ▶ 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 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

# HITRUST CSF<sup>®</sup> Services

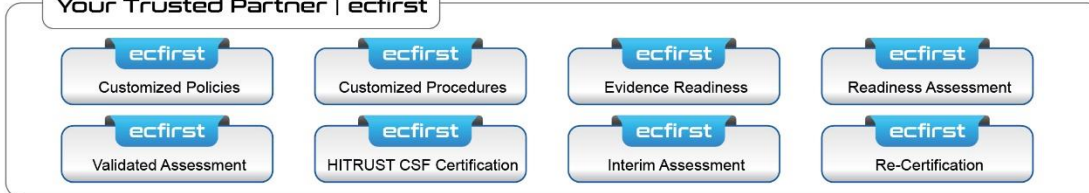


As a HITRUST Authorized External Assessor, ecfirst can assist your efforts for Readiness Assessment, Validated Assessment, HITRUST CSF Certification, Interim Assessment, and Re-certification. Talk to us about your journey to achieve HITRUST CSF Certification, and beyond. Jump-start your initiatives with ecfirst.

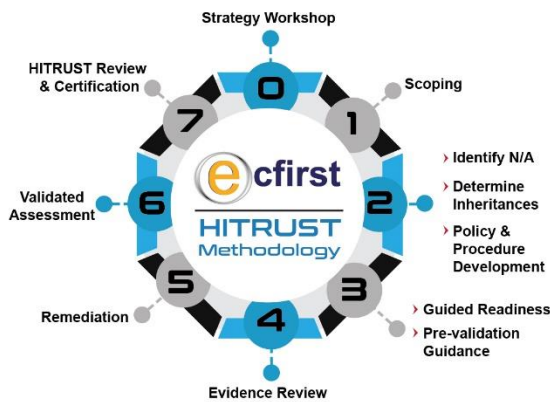
ecfirst a full suite of HITRUST services enabling your organization to achieve and manage certification, including:

- ✔ Perform a comprehensive HITRUST pre-assessment to identify compliance and cyber gaps.
- ✔ Develop a customized HITRUST policy and procedure set to meet your requirements.
- ✔ Perform a guided HITRUST Readiness Assessment.
- ✔ Guidance on the development of implementation evidence.
- ✔ Conduct a HITRUST Validated Assessment towards Certification.
- ✔ Complete a HITRUST Interim Assessment.

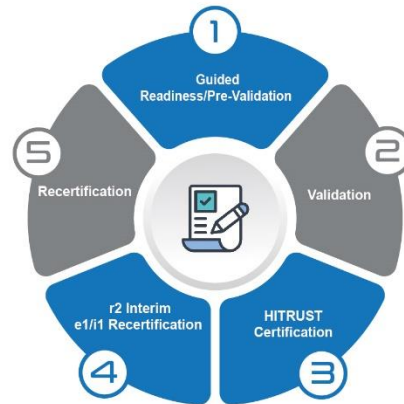
### Your Trusted Partner | ecfirst



### Signature Methodology



### Achieving Certification



### Virtual! HITRUST Cybersecurity Workshop



- ✔ Examine the fundamentals of the HITRUST CSF.
- ✔ Leveraging the HITRUST CSF to implement the NIST Cybersecurity Framework.
- ✔ Addressing regulatory mandates such as GDPR, CCPA, HIPAA, and FISMA.
- ✔ Getting organized: From Readiness Assessment, thru Validation to Certification.
- ✔ Roadmap to HITRUST and NIST certification.




Complimentary! HITRUST Exec Brief







### Achieving Certification

Ask about our free 29-minute exec brief to walk-thru the roadmap for achieving HITRUST CSF Certification. Understand key steps for readiness 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, 

-  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!







## NIST Cybersecurity Framework Services

<b>NIST Cybersecurity Framework</b> Security Assessment	<b>NIST Cybersecurity Framework</b> Policy Readiness
<b>NIST Cybersecurity Framework</b> Procedure Readiness	<b>NIST Cybersecurity Framework</b> Evidence Readiness
<b>NIST Cybersecurity Framework</b> Professional Consultants	<b>NIST Cybersecurity Framework</b> 

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.





# On-Demand Consulting (ODC)

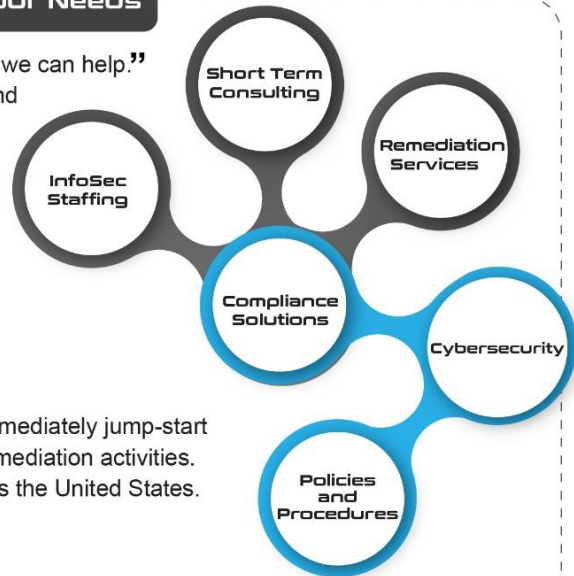


On-site | Virtual

## 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



**Manage Compliance for HIPAA, NIST and more**

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?

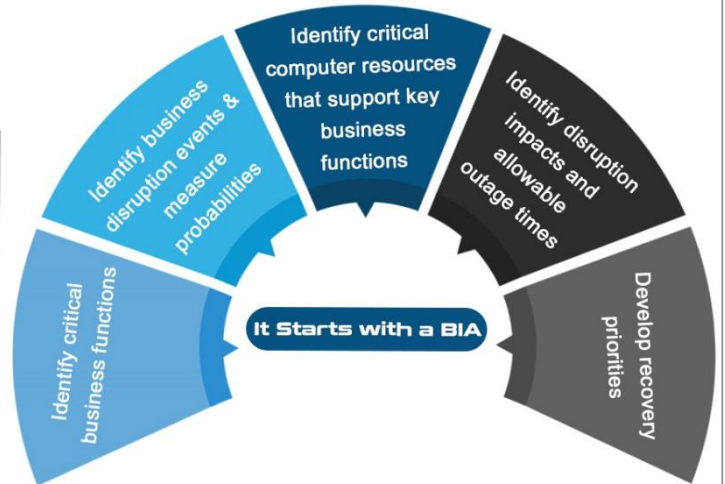


Contingency planning, also referred to as Business Continuity Planning (BCP), is a coordinated strategy that involves plans, procedures and technical measures to enable the recovery of systems, operations, and data after a disruption. A Business Impact Analysis (BIA) is the foundation for building Contingency 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.

**Compliance Mandate**

Contingency Plan is a HIPAA Security Standard. It is also a Clause in the ISO 27001 Security Standard. The objective of the Contingency Plan Standard is to establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damage systems that contain ePHI or PII.

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

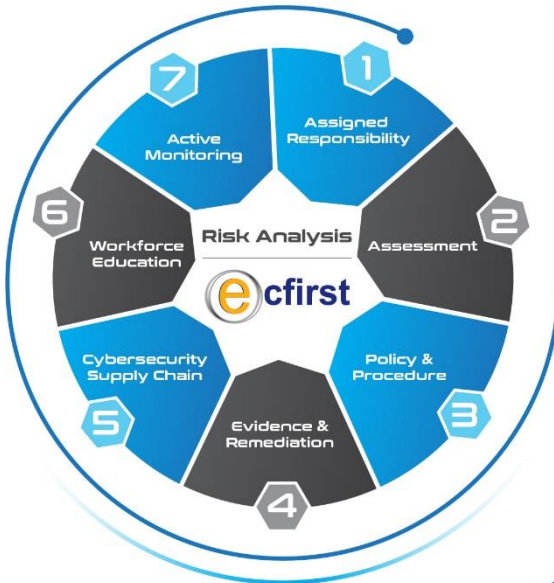
- 1 Business Impact Analysis Report
- 2 An IT Disaster Recovery Plan



# 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	X
Personalized Interviews	Virtual	X
Administrative Safeguards	✓	✓
Physical Safeguards	✓	✓
Technical Safeguards	✓	✓
Privacy Assessment	✓	✓
Supply Chain Assessment	✓	✓
Policy Gap Assessment	✓	✓
Breach Assessment	✓	✓
Guided Facility Walkthrough	✓	X
Guided Data Center Assessment	✓	X
Executive Brief	Virtual	X
Corrective Action Plan (CAP)	✓	✓



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



# Risk Assessment



HIPAA • NIST • Cyber • CloudFirst • Pen Test • CMMC • Online Tracking

## Signature Methodology

Page 3

HIPAA • NIST



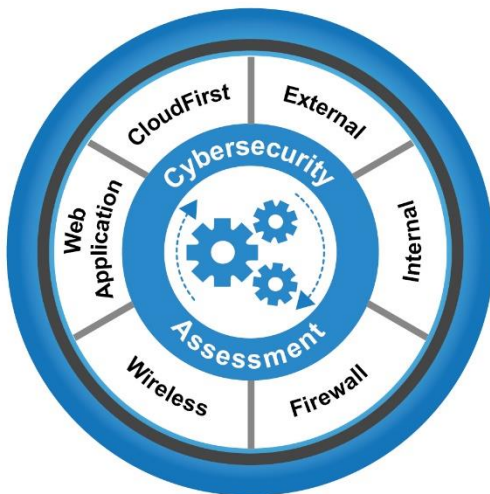
## CloudFirst

Page 10



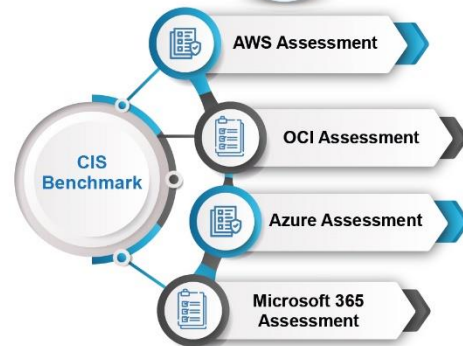
## Cybersecurity Assessment

Page 4



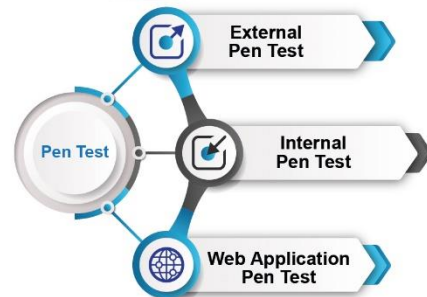
## CIS Benchmark

Page 12



## Pen Test

Page 15

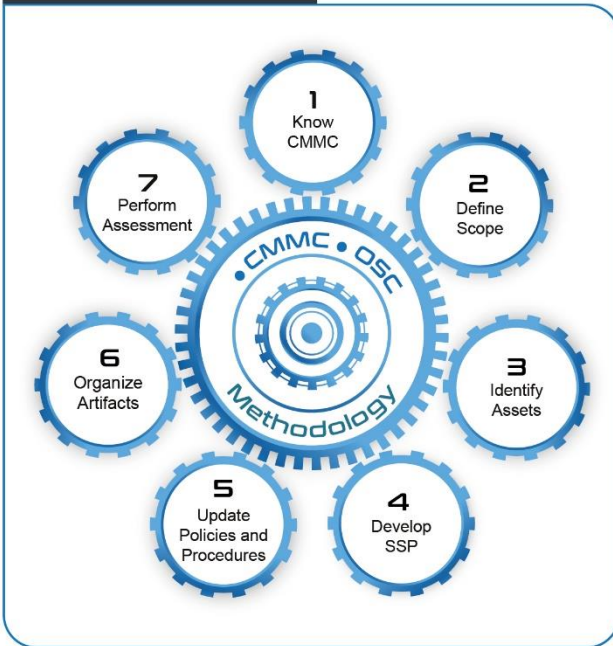


# Risk Assessment



HIPAA • NIST • Cyber • CloudFirst • Pen Test • CMMC • Online Tracking

## CMMC Readiness



## Asset Risk Management



## Social Engineering

Page 18



## Online Tracking Assessment

Page 20



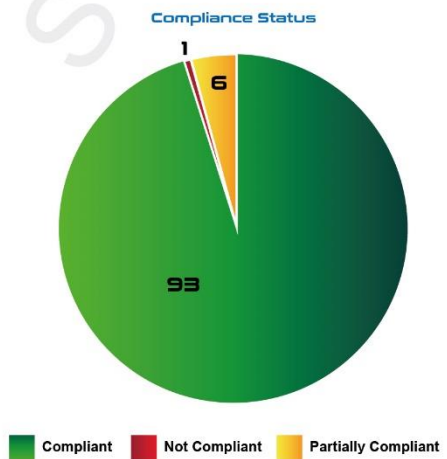
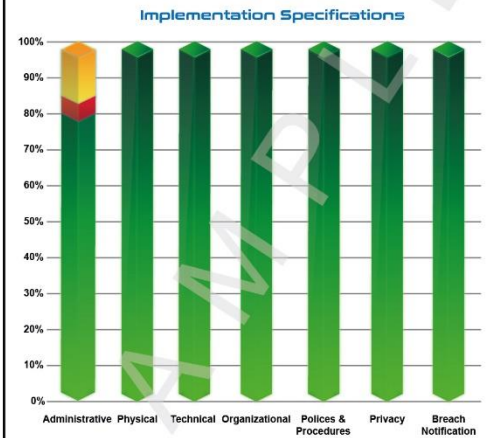
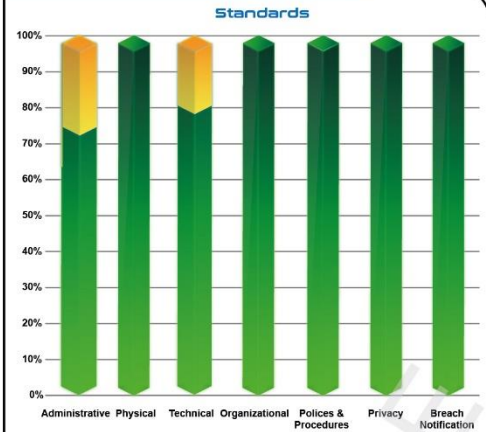


# Risk Analysis

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	X
Personalized Interviews	Virtual	X
Administrative Safeguards	✓	✓
Physical Safeguards	✓	✓
Technical Safeguards	✓	✓
Privacy Assessment	✓	✓
Supply Chain Assessment	✓	✓
Policy Gap Assessment	✓	✓
Breach Assessment	✓	✓
Guided Facility Walkthrough	✓	X
Guided Data Center Assessment	✓	X
Executive Brief	Virtual	X
Corrective Action Plan (CAP)	✓	✓

## Executive Dashboard



# Cybersecurity Assessment

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



### Cyber Risk Status



# Cybersecurity Assessment

## Titanium

The Titanium Level Assessment 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

## Platinum

The Platinum Level Assessment 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

## Gold

The Gold Level Assessment 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



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

## Silver

The Silver Level Assessment 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 contains:
    - » 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 contains:
    - » Detailed cybersecurity findings
    - » Corrective Action Plan
    - » Detailed remediation information



## Cybersecurity Assessment

### 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, you have 60 days to remediate any negative findings. After that time, ecfirst will review the remediation efforts and retest as necessary, and will provide an updated report.

# CloudFirst Cybersecurity Assessment

## CloudFirst Cybersecurity Assessment

ecfirst CloudFirst Cybersecurity Assessment Phases



Data gathered is analyzed against policies, standard best practices, and vendor security bulletins to determine potential risks and exposures to the computing environment. The results of these cybersecurity scans/tests are to be used as the basis for determining the security posture and risk to organizational systems.

## CIS Microsoft Azure Foundations Security Benchmark Assessment

With a CIS Microsoft Azure Foundations Security Benchmark Assessment, ecfirst provides prescriptive guidance for establishing a secure baseline configuration for Microsoft Azure. The scope is to establish the foundation level of security for anyone adopting Microsoft Azure Cloud. This benchmark is not a complete list of all possible security configurations and architecture.



## CIS Cloud Management Foundations Benchmark Testing

- ❖ CIS is an internationally respected community of cybersecurity experts who provide best practice analysis and guidance for each security setting available for configuration in operational and application software across over 25 vendor product families.
- ❖ Thousands of layered, defined, and inherited security configurations are set across an organization's applications, operating systems, networks, and management systems. Where is over-protection breaking required functionality and where is under-protection exposing the organization to untenable risk? Worse, what combination of settings is doing both?
- ❖ ecfirst has created benchmark testing tools and scans based on a best practice balance between low risk and high functionality.
- ❖ All ecfirst Foundations tests ensure evaluation against Level 1 CIS recommendations. The configuration review determines the overall threat of potential compromise so that the business can make adjustments based on its organizational needs and risk tolerance.
- ❖ ecfirst maintains all the tools and knowledge needed to perform testing and reporting against the latest best practice recommendations defined in the benchmark. ecfirst benchmark testing reports provide all the information required to enable risk-informed and efficient business decision-making and strengthen the organization's resistance to cyber attacks.

## CIS System Configuration Benchmark Assessment

CIS Benchmarks are best practices for the secure configuration of a target system. CIS Benchmarks are consensus-based, best practice security configuration guides developed and accepted by the government, business, industry, and academia. The ecfirst CIS System Configuration Benchmark Assessment scans the system to identify if the configuration is aligned with defined requirements.

# CloudFirst Cybersecurity Assessment

## CloudFirst Scope

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

### External Assessment

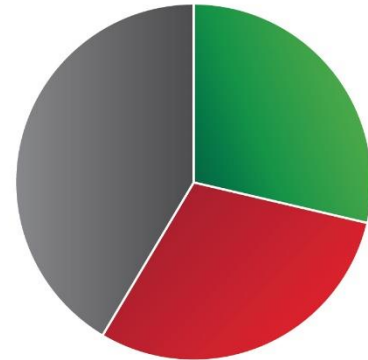
- Up to 32 IP addresses

### Internal Assessment

- An Active Directory (AD) domain is tested

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 cannot deploy our Virtual Machine image, we will have to send you a hardware device at an additional cost.

## Compliance Status Example



Compliant Not Compliant N/A

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

## CloudFirst Risk Status



## Significant Findings

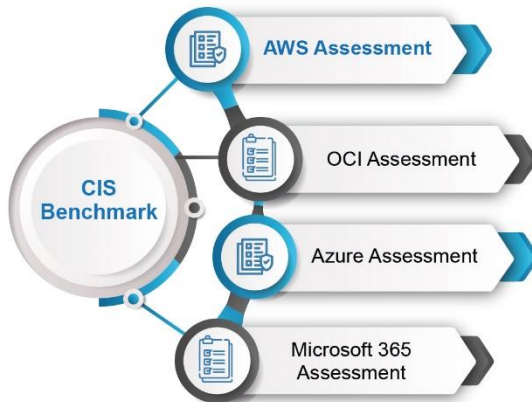




## CIS Benchmark Assessment

### 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.

#### The 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.

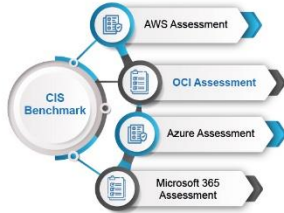
The Phases for this assessment are:

- » **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 organization 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 and its sustainability and contribution to the overall risk profile.

# CIS Benchmark Assessment

## 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

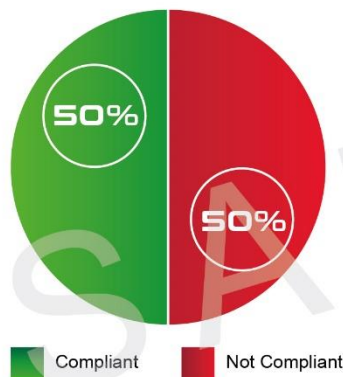
**The ecfirst OCI Report includes,**

- » 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



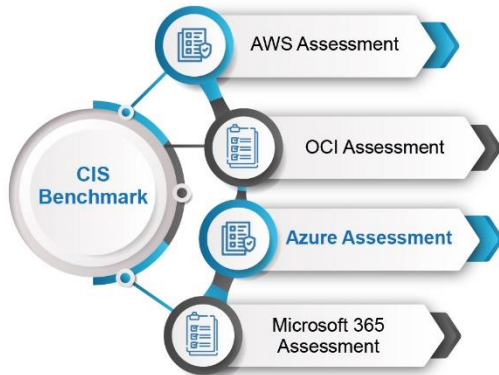
Area	Total # of CAP Items	Not-Compliant CAP Items	Compliant
IAM	12	3	9
Networking	5	2	3
LogMon	17	12	5
Object Storage	2	1	1
Asset Management	2	1	1
<b>Total</b>	<b>38</b>	<b>19</b>	<b>19</b>



# CIS Benchmark Assessment

## Azure Assessment

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



The CIS Foundations Benchmark 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 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

The ecfirst Azure Report includes,

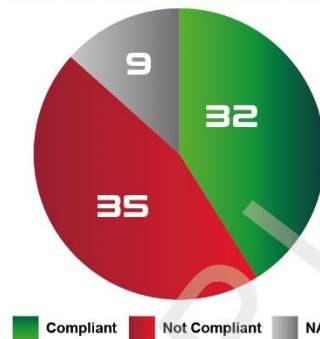
- » Alignment with CIS Benchmark for Azure Foundations, Level 1 settings
- » Correctly configured settings where further action is required to achieve full security benefits
- » Review of available versus used licenses and their impact
- » Analysis of findings, including strengths and prioritized areas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

Configuration benchmark alignment areas include,

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

### Executive Dashboard

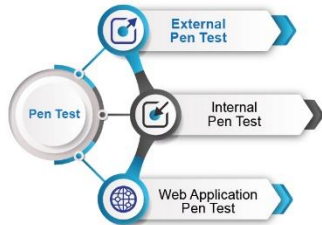
#### Compliance Progress



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

# Pen Test

## External Penetration Test



❖ The 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 organized into three (3) distinct phases:

### Reconnaissance

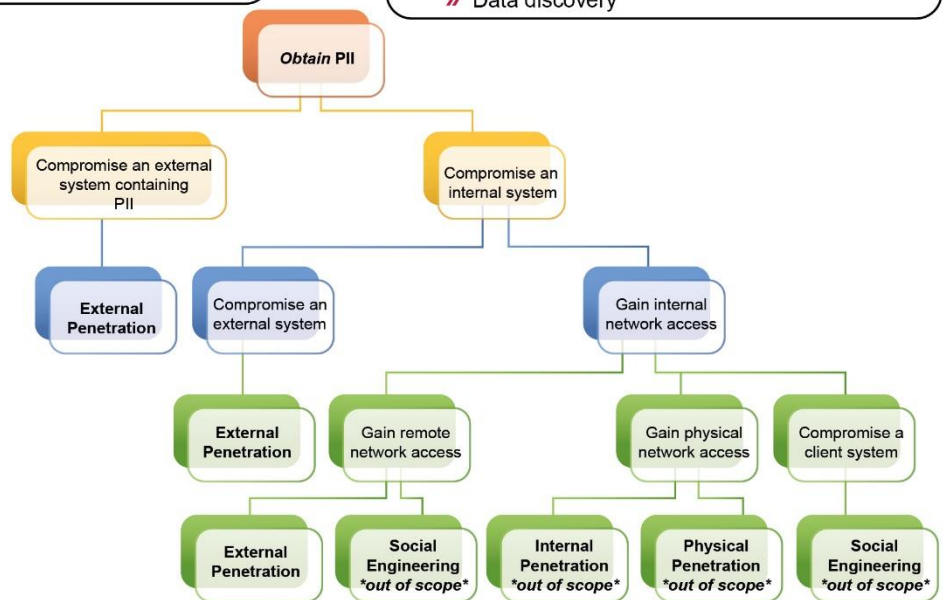
- » Client personnel and cultural information
- » Client business terminology
- » Technical infrastructure information

### Scanning

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

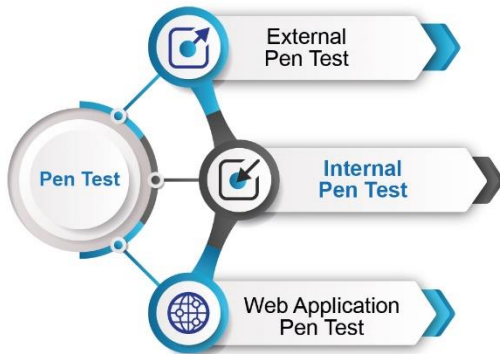
### Exploitation

- » 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

## Internal Penetration Test



❖ The 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 ecfirst
- » 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

### Scanning

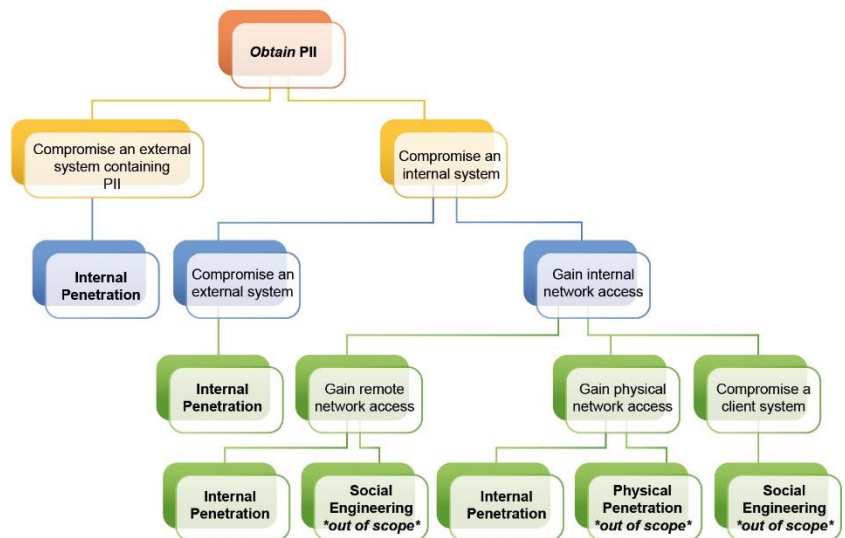
- » Network discovery
- » Network port and service identification
- » Cybersecurity identification
- » Enumeration

### Out-of-Scope

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

### Exploitation

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



## Pen Test

### 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

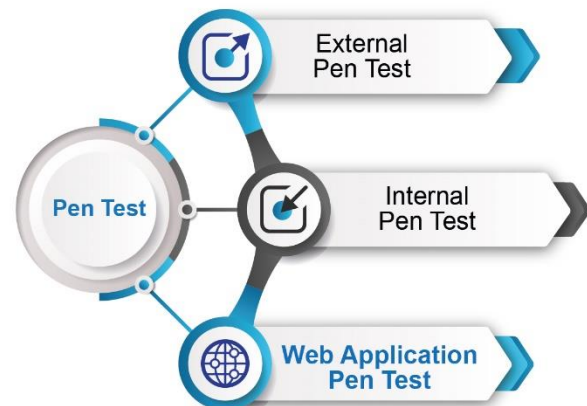
The Web Application Penetration Test methodology is organized into four (4) distinct phases,

#### 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.



## Social Engineering

- ❖ Customized phishing campaigns to identify % of phish-prone users
- ❖ Targeted end user security awareness training to reduce risk from phish-prone users
- ❖ Development of tailored phishing, vishing, pretexting, CEO Fraud 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

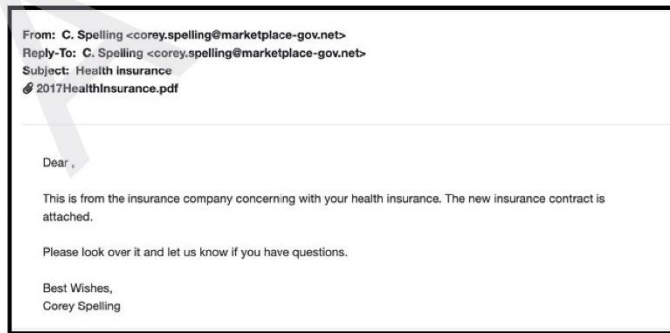
- Based on the number of users that fell victim to the phishing performed, ecfirst estimates the risk of a successful Social Engineering attack against to be a **Medium** risk.



#### 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:



## Performed an Online Tracking Assessment?

### OCR Mandate for HIPAA Compliance

#### Objectives

- ❖ Identify 3rd-party resources across websites.
- ❖ Evaluate 3rd-party resources using fingerprinting or tracking technology.
- ❖ Establish actionable recommendations.
- ❖ Ensure HIPAA compliance with OCR guidance for online tracking.



#### Online Tracking HIPAA Compliance

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.

OCR Guidance

#### Project Scope

Crawl the in-scope websites to identify calls to 3rd-party resources.

Review 3rd-party resources to identify those implementing tracking or fingerprinting technologies.

Provide report on websites employing tracking or fingerprinting technologies, including identifying the specific 3rd-party resources on each crawled page potentially providing those features.

#### The ecfirst HIPAA Ecosystem



## 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).



Virtual | On-site | Public Schedule

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

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.
- Examine OCR HIPAA settlements to understand the bar for HIPAA compliance.
- Review HIPAA compliance challenges and best practices for Covered Entities and Business Associates.
- Understand HIPAA Safe Harbour.



### Target Audience

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

### Great training!

Instructor helped at all times  
*Fast-paced, detailed, efficient*  
 Very comprehensive HIPAA program  
**The training was great**



### References

*Great speaker, great pace, kept my attention*  
**Extremely knowledgeable**  
*Great experience to reboot knowledge*  
*Refresher for various regulations*  
**Good examples**



Virtual | On-site | Public Schedule

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

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, CCPA, CPRA, 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)

**Great teachers**  
**Everything was great!**  
*Great course and instructor*  
*Lots of information given in such a short time*  
**I strongly recommend it**

### CSCS References

*He explained everything so I could understand*  
**This is a fantastic introductory course into compliance**  
*kept the class engaged*  
**Great class**





Virtual | On-site | Public Schedule

## An Executive Cyber Security Program

CCSA<sup>SM</sup> is an instructor-led 1-day program. The program validates knowledge and skill sets in cybersecurity with a 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.
- 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.



## Target Audience

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

**Clear information  
Love the pace**

*Well organized, informative and very fast*

**Very clear understand method!**

**Good compliment to the written material**

**CCSA<sup>SM</sup> References**

*Excellent presentation of valuable information*

*Very good experience and highly recommended*

**AWESOME!!!! Loved the course**

*The rate at which the materials*

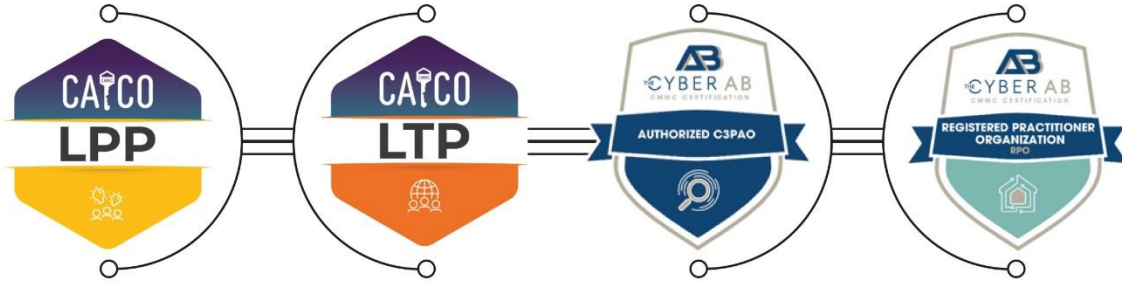
**were covered**

**Very good**



# 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)



“Solid content and flexible delivery”

“Highly informative”

“Best course ever experienced”

“ecfirst courseware is AMAZING!”



Training Program



### Summary

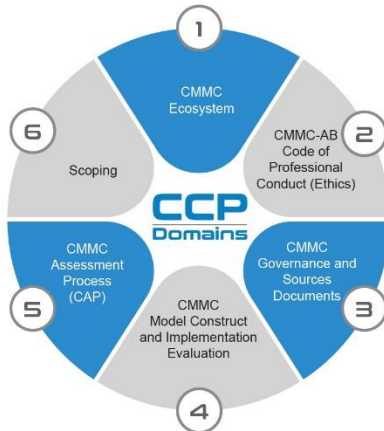
This Certified CMMC Professional (CCP) exam will verify a candidate's knowledge of the Cybersecurity Maturity Model Certification (CMMC), relevant supporting materials, and applicable legal and regulatory requirements to protect Federal Contract Information (FCI) and Controlled Unclassified Information (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)



### All Content is Digital



### Prerequisites

- ◆ College degree in a cyber or information technical field or 2+ years of related experience or education; or 2+ years of equivalent experience (including military) in a cyber, information technology, or assessment field.
  - ◆ Suggested CompTIA A+ or equivalent knowledge/experience.
  - ◆ Complete CCP Class offered by a 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>

### 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	2024 Hours
1	CCA Pre Program Prep			2 Hours
2	CMMC Ecosystem	5%	<b>Domain 1, 2 &amp; 3</b> Tuesday, Day 1 8:30 am - 4:30 pm Offline Prep: 2 Hours	10 Hours
3	Cyber-AB Code of Professional Conduct (Ethics)	5%		
4	CMMC Governance and Sources Documents	15%		
5	CMMC Model Construct and Implementation Evaluation	35%	<b>Domain 4</b> Wednesday, Day 2 8:30 am - 4:30 pm Offline Prep: 2 Hours	10 Hours
6	CMMC Assessment Process (CAP)	25%	<b>Domain 5</b> Thursday, Day 3 8:30 am - 4:30 pm Offline Prep: 2 Hours	10 Hours
7	Scoping	15%		
8	Practice Exam & Review		<b>Domain 6 &amp; Review</b> Friday, Day 4 8:30 am - 12:00 pm	3.5 Hours

### CCP Exam Specifications

- 1. Number of Questions: 170
- 2. Types of Questions: Multiple Choice
- 3. Length: 3.5 Hours
- 4. Passing Score: 500 points
- 5. This is not an open book exam

<https://academy.ecfirst.com>

- Updated for CMMC 2.0
- Evaluation Form
- Downloads

[Do you have your CPN Number?](#)
[Ready for CCP Exam?](#)
[DoD Posts CMMC Video](#)

#### Core

[Training Book](#)
[Classroom](#)

#### Additional Reference

[CMMC Domains](#)
[CCP Pretest](#)

[CMMC Practices](#)
[Quiz](#)

[Assessor Toolkit](#)
[Final Practice Exam](#)

#### Quick Links

- CMMC Proposed Rule, December 2023
- Table of Index
- 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
- Shared Responsibility
- Controlled Unclassified Information (CUI)
- Security Awareness Hub
- Instructor, Restricted





# 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

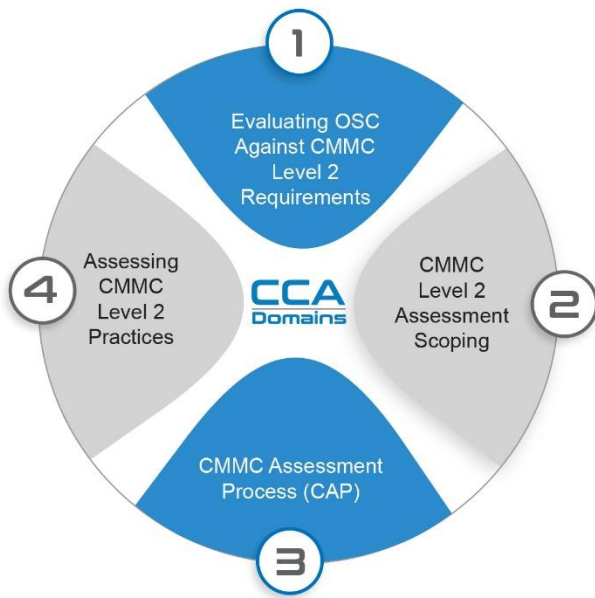
The Department of Defense (DoD) is the authoritative source for CMMC documentation.

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

## All Content is Digital



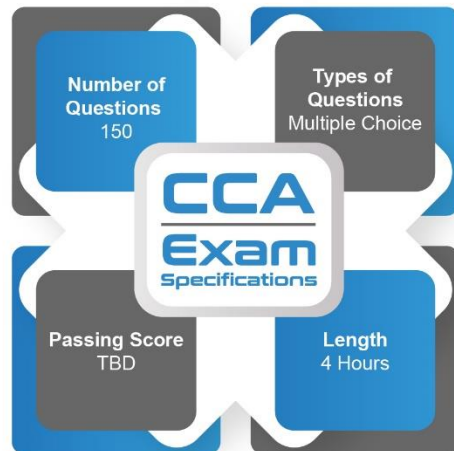
## Certified CMMC Assessor (CCA)



## Intended Audience

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

## CCA Exam Specifications







# Training Program



#	Domain	Exam Weight	CCA Program	2024 42 Hours
1	CCA Pre Program Prep			2 Hours
2	Welcome Introductions, About the Portal and Pre-Quiz		<b>Domain 0, 1, 2</b> Tuesday, Day 1 8:30 am - 4:30 pm Group Exercises: 8   40 Minutes Offline Prep: 2 Hours	10 Hours
	Introduction	15%		
3	Evaluating OSC Against CMMC Level 2 Requirements	20%		
4	CMMC Level 2 Assessment Scoping	25%	<b>Domain 3</b> Wednesday, Day 2 8:30 am - 4:30 pm Group Exercises: 7   35 Minutes Offline Prep: 2 Hours	10 Hours
5	CMMC Assessment Process (CAP)	40%	<b>Domain 4</b> Thursday, Day 3 8:30 am - 4:30 pm Group Exercises: 10   60 Minutes Offline Prep: 2 Hours	10 Hours
6	Assessing CMMC Level 2 Practices		<b>Review and Final Quiz</b> Friday, Day 4	8:30 am - 4:30 pm 10 Hours

<https://academy.ecfirst.com>

The screenshot shows the CCA Academy website interface. At the top, it says "Certified CMMC Assessor" with logos for CMMC and PRO-CERT. Below this, there are several navigation buttons: "CCA Pretest", "Classroom", "Research", "Quiz", "Assessor Toolkit", "Group Exercise", "CMMC Readiness", and "Final Practice Exam". On the right side, there is a "Quick Reference" section with a list of links including "CMMC Prepared File, Dec 2024 2024", "CMMC 2.0 Updates", "CMMC 2.0 Implementation Plan", "CMMC 2.0 Checklist", "CMMC 2.0 FAQ", "CMMC 2.0 Glossary", "CMMC 2.0 Training", "CMMC 2.0 Tools", "CMMC 2.0 Templates", "CMMC 2.0 Forms", "CMMC 2.0 Reports", "CMMC 2.0 Metrics", "CMMC 2.0 Dashboards", "CMMC 2.0 Analytics", "CMMC 2.0 Visualizations", "CMMC 2.0 Charts", "CMMC 2.0 Tables", "CMMC 2.0 Lists", "CMMC 2.0 Maps", "CMMC 2.0 Diagrams", "CMMC 2.0 Flowcharts", "CMMC 2.0 Mind Maps", "CMMC 2.0 Hierarchies", "CMMC 2.0 Networks", "CMMC 2.0 Trees", "CMMC 2.0 Grids", "CMMC 2.0 Galleries", "CMMC 2.0 Portfolios", "CMMC 2.0 Collections", "CMMC 2.0 Bundles", "CMMC 2.0 Packages", "CMMC 2.0 Suites", "CMMC 2.0 Systems", "CMMC 2.0 Frameworks", "CMMC 2.0 Methodologies", "CMMC 2.0 Approaches", "CMMC 2.0 Strategies", "CMMC 2.0 Tactics", "CMMC 2.0 Techniques", "CMMC 2.0 Procedures", "CMMC 2.0 Processes", "CMMC 2.0 Workflows", "CMMC 2.0 Pipelines", "CMMC 2.0 Cycles", "CMMC 2.0 Loops", "CMMC 2.0 Feedbacks", "CMMC 2.0 Iterations", "CMMC 2.0 Evolutions", "CMMC 2.0 Transformations", "CMMC 2.0 Innovations", "CMMC 2.0 Disruptions", "CMMC 2.0 Reconfigurations", "CMMC 2.0 Reshuffles", "CMMC 2.0 Restructurings", "CMMC 2.0 Reorganizations", "CMMC 2.0 Reimaginings", "CMMC 2.0 Reinventions", "CMMC 2.0 Revolutions", "CMMC 2.0 Paradigms", "CMMC 2.0 Frameworks", "CMMC 2.0 Methodologies", "CMMC 2.0 Approaches", "CMMC 2.0 Strategies", "CMMC 2.0 Tactics", "CMMC 2.0 Techniques", "CMMC 2.0 Procedures", "CMMC 2.0 Processes", "CMMC 2.0 Workflows", "CMMC 2.0 Pipelines", "CMMC 2.0 Cycles", "CMMC 2.0 Loops", "CMMC 2.0 Feedbacks", "CMMC 2.0 Iterations", "CMMC 2.0 Evolutions", "CMMC 2.0 Transformations", "CMMC 2.0 Innovations", "CMMC 2.0 Disruptions", "CMMC 2.0 Reconfigurations", "CMMC 2.0 Reshuffles", "CMMC 2.0 Restructurings", "CMMC 2.0 Reorganizations", "CMMC 2.0 Reimaginings", "CMMC 2.0 Reinventions", "CMMC 2.0 Revolutions", "CMMC 2.0 Paradigms".

Ali Pabrai



## Global AI Cyber Defense Thought Leader

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



Mr. Ali Pabrai, a global AI 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).

### U.S. Department of Defense CMMC Program



“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

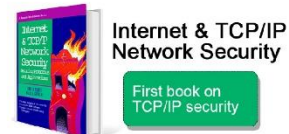
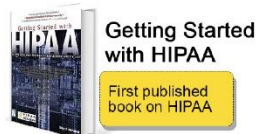
“You delivered a fantastic presentation and we all felt your passion for cyber security.”

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



### The ecfirst DoD CMMC Ecosystem





**Corporate Office**

295 NE Venture Drive  
Waukee, IA 50263  
United States

**Krystal B. Perez**

Team Lead, Business Development &  
Certification Program

Email: [Casey.Collins@ecfirst.com](mailto:Casey.Collins@ecfirst.com)

