ecfirst | Reimagining Cyber Defense



CMMC-AB CYBERSECURITY MATURITY MODEL CERTIFICATION
LPP
LICENSED

CMMC-AB CYBERSECURITY MATURITY MODEL CERTIFICATION
LTP
LICENSED

CMMC-AB CYBERSECURITY MATURITY MODEL CERTIFICATION
C3PAO

CMMC-AB CYBERSECURITY MATURITY MODEL CERTIFICATION
RPO
REGISTERED

HITRUST®
Authorized External Assessor

HIPAA & HITECH

TRACER℠
ASSET RISK MANAGEMENT

PCI DSS

BIA & DRP

ISO 27001

HIPAA™ Academy

Risk Analysis

GDPR

CHP Certified HIPAA Professional
HIPAA Academy

Cybersecurity Assessment

NIST

CSCS™
CERTIFIED SECURITY COMPLIANCE SPECIALIST

Penetration Testing

CMMC

CCSA℠
Certified Cyber Security Architect

Virtual ISO & IT Staffing

On-Demand Consulting

ecfirst Academy

Biomed
Med Device Cybersecurity
Culinda

Managed Compliance

Table of Contents

About ecfirst 3

TRACER℠ 4

Online Learning 9

Compliance Services

HIPAA & HITECH 14

PCI DSS 15

ISO 27001 17

GDPR 19

Cybersecurity Services

NIST 20

CMMC 21

On-Demand Consulting 22

Managed Cybersecurity Services Program (MCSP) 23

BIA & IT Disaster Recovery Plan 24

Risk Analysis 25

Cybersecurity Assessment & Penetration Testing 26

Virtual ISO & Infosec Staffing Program 41

Biomed & IoT 42

Certification Training

CHP 44

CSCS™ 45

CCSA℠ 46

About Uday Ali Pabrai 47

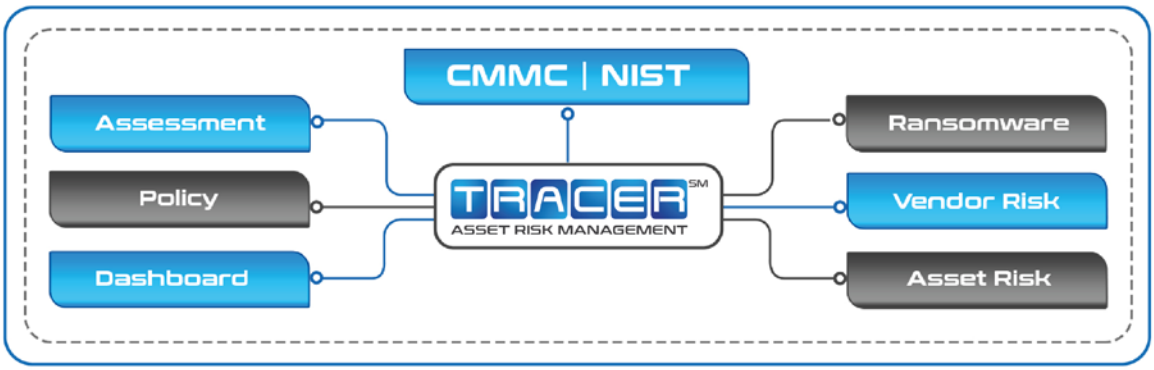
© ecfirst. All Rights Reserved. 2022



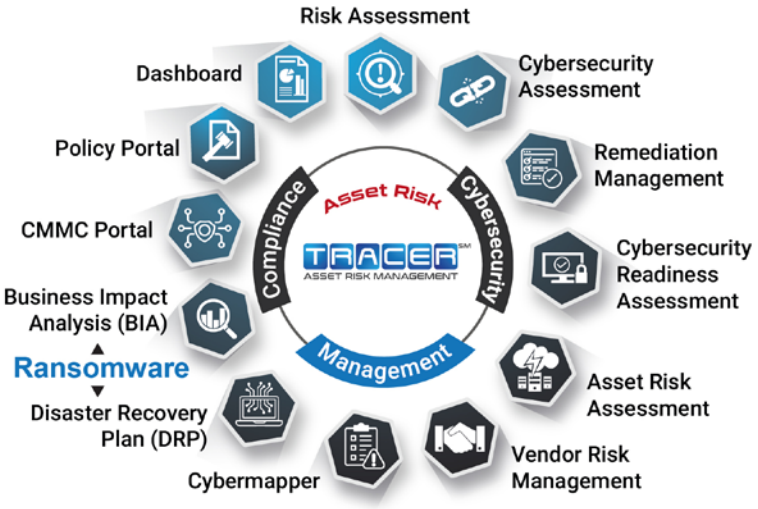
© ecfirst. All Rights Reserved. 2022

TRACER℠ ASSET RISK MANAGEMENT

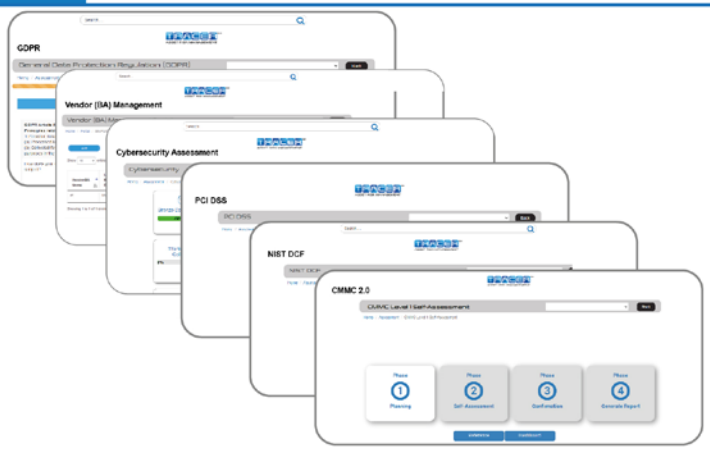
ecfirst



TRACER℠ ASSET RISK MANAGEMENT Features



Compliance



© ecfirst. All Rights Reserved. 2022

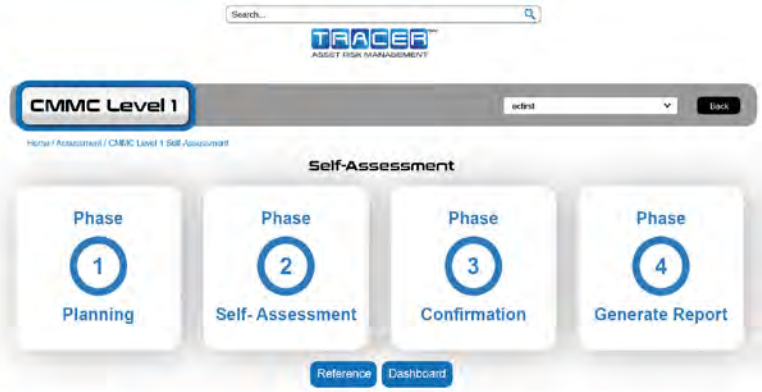
TRACER℠
ASSET RISK MANAGEMENT

ecfirst

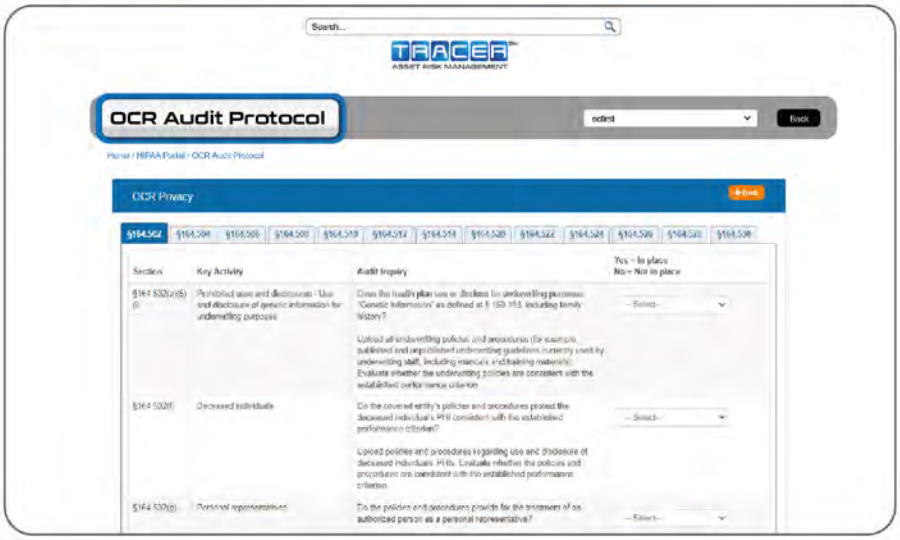
Cyber Readiness



CMMC Portal



HIPAA Portal

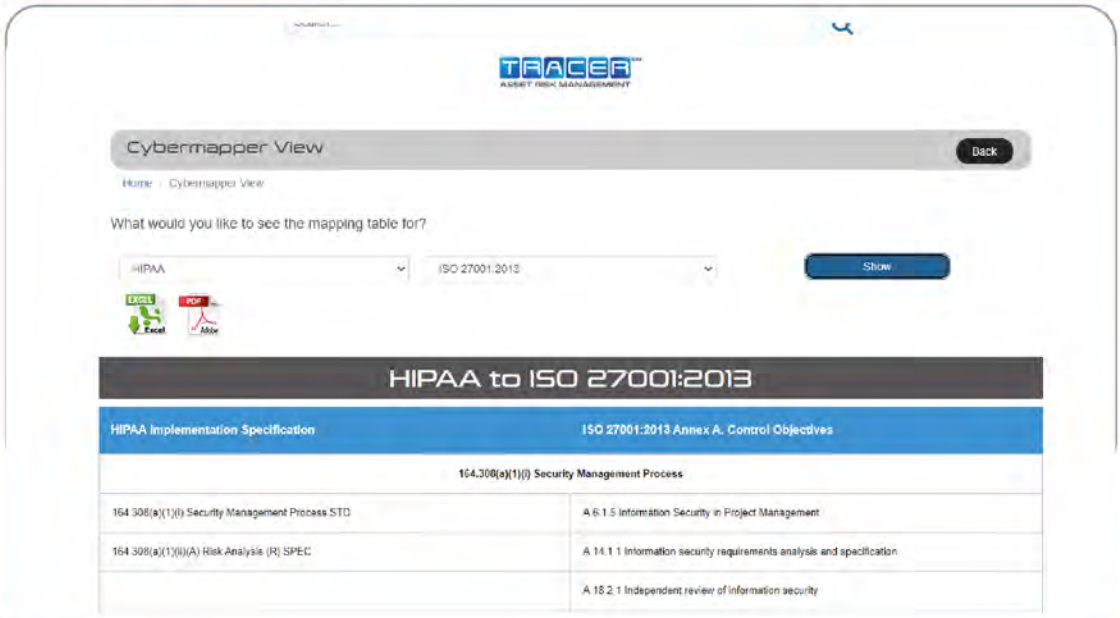


© ecfirst. All Rights Reserved. 2022

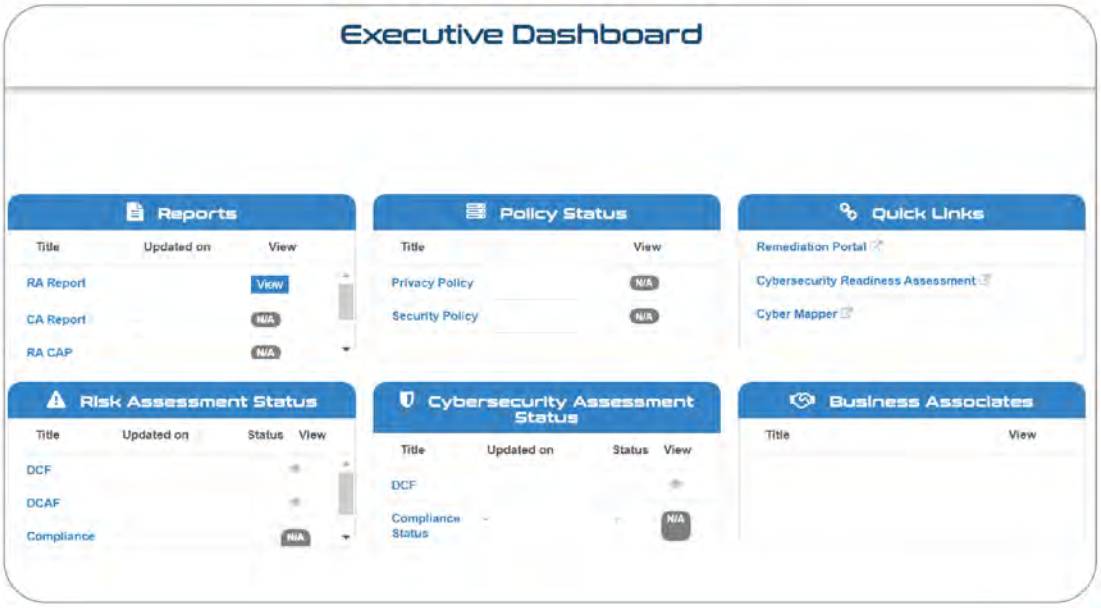
TRACER℠ ASSET RISK MANAGEMENT

ecfirst

Cybermapper



Executive Dashboard



© ecfirst. All Rights Reserved. 2022

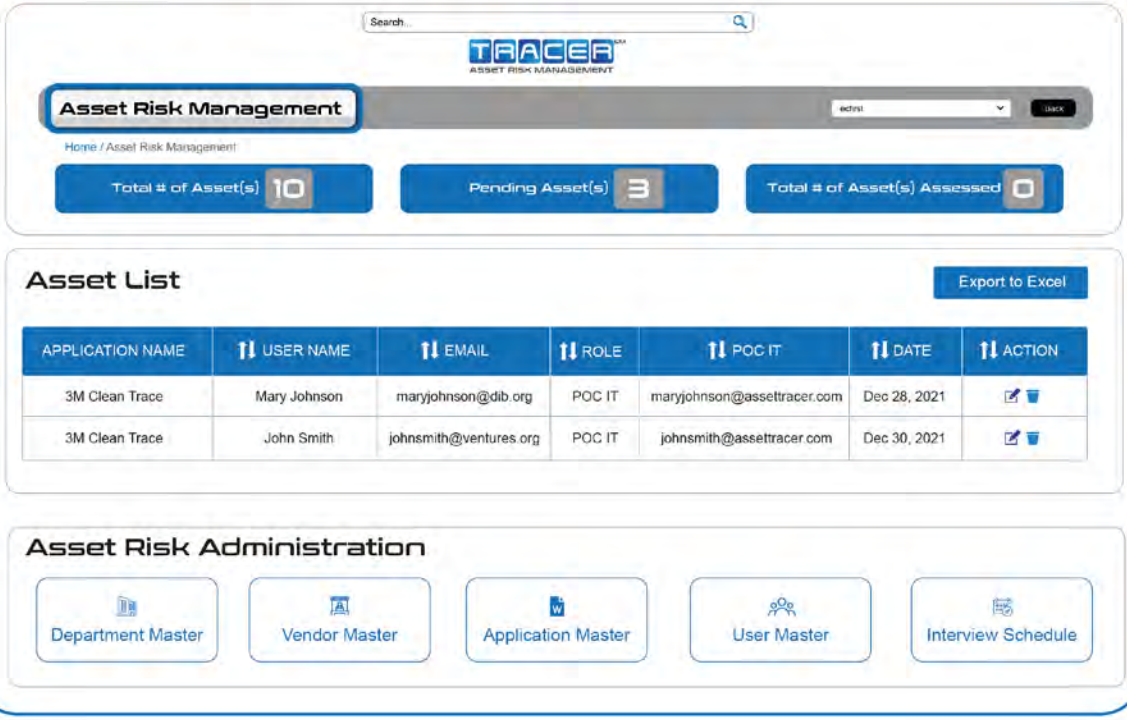
TRACER℠
ASSET RISK MANAGEMENT

ecfirst

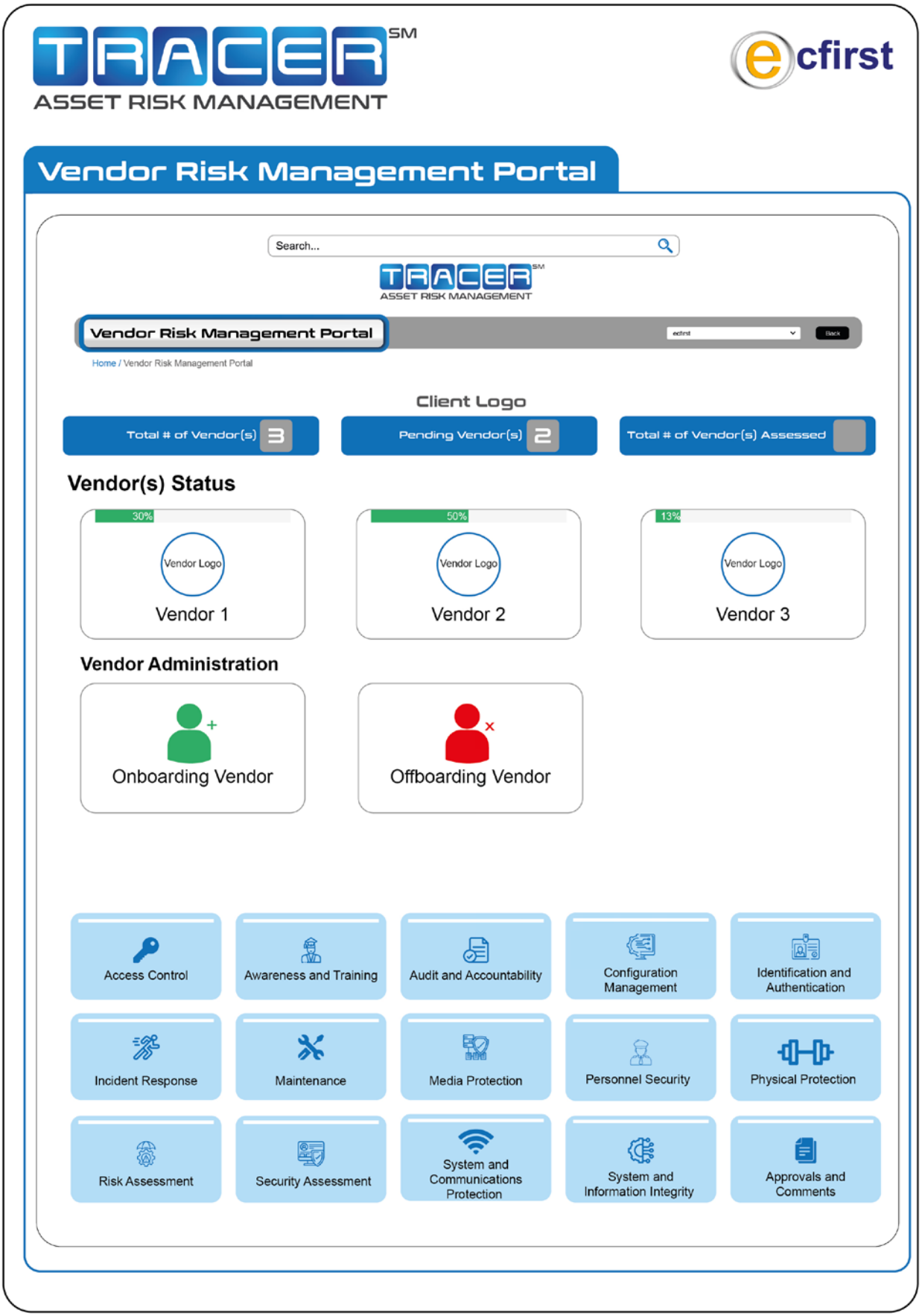
Ransomware Readiness



Asset Risk Assessment



© ecfirst. All Rights Reserved. 2022

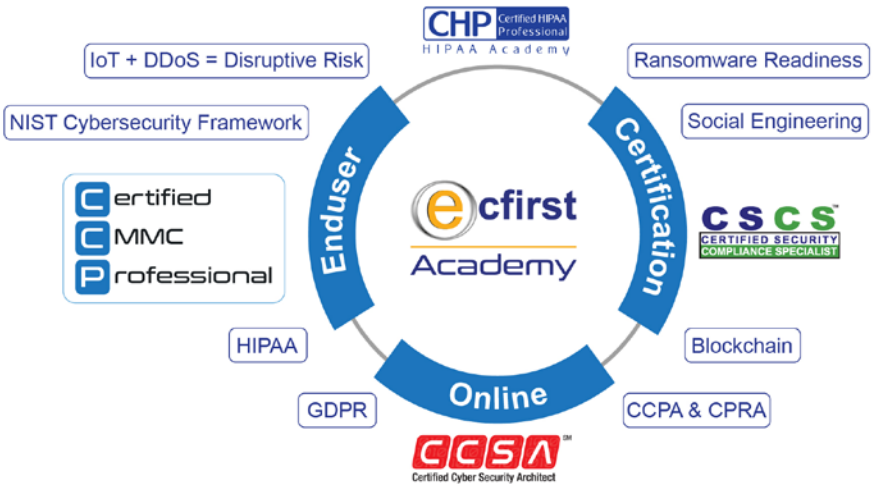


© ecfirst. All Rights Reserved. 2022

ecfirst Academy

Online Learning Portal

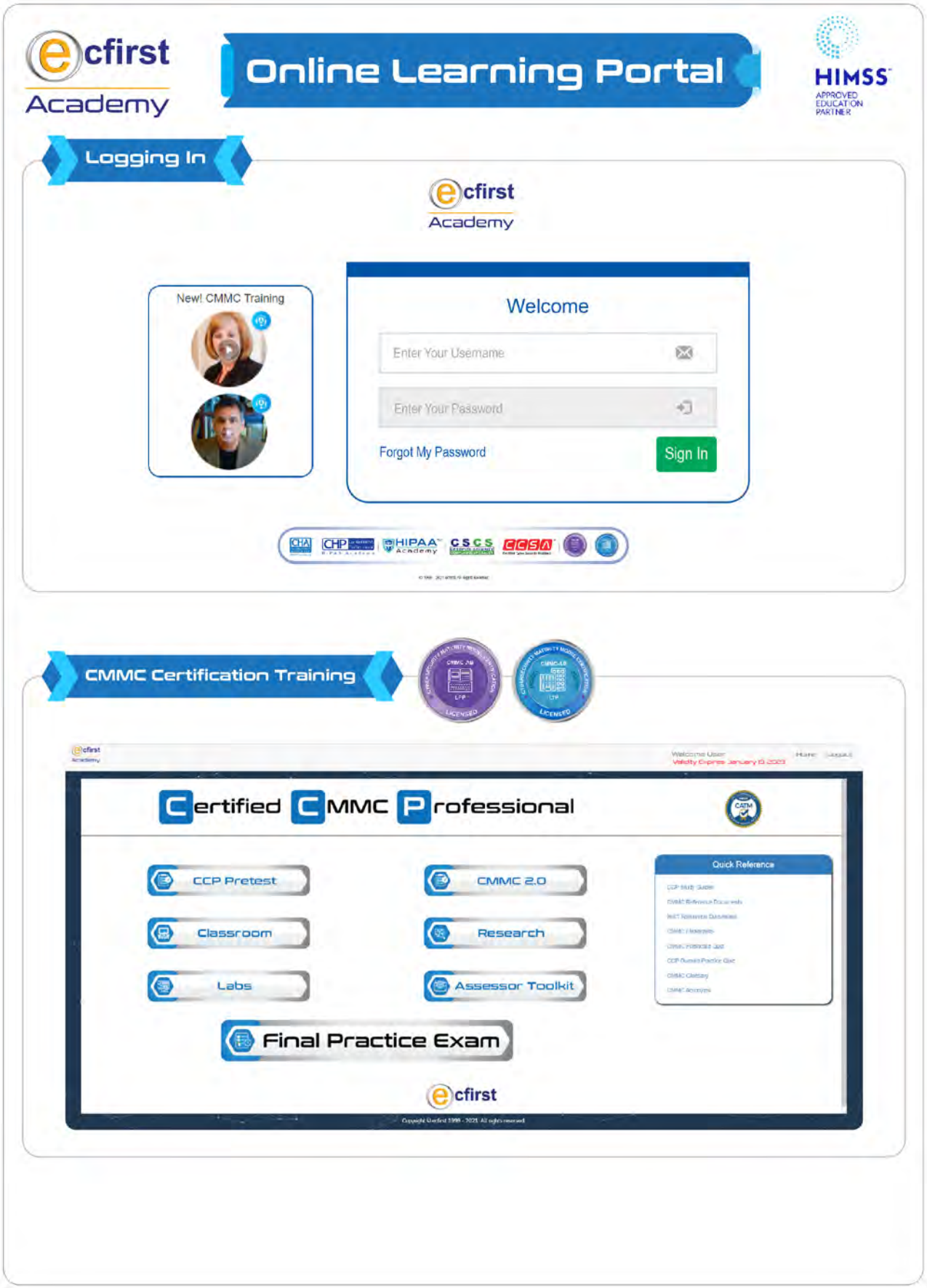
HIMSS APPROVED EDUCATION PARTNER



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

© ecfirst. All Rights Reserved. 2022


ecfirst Academy
Online Learning Portal
HIMSS APPROVED EDUCATION PARTNER
Logging In
ecfirst Academy
New! CMMC Training
Welcome
Enter Your Username
Enter Your Password
Forgot My Password
Sign In
CMMC Certification Training
Certified CMMC Professional
CCP Pretest
CMMC 2.0
Classroom
Research
Labs
Assessor Toolkit
Final Practice Exam
Quick Reference
ecfirst

ecfirst Academy

Online Learning Portal

HIMSS APPROVED EDUCATION PARTNER

Enduser Training



CHP Certified HIPAA Professional HIPAA Academy



ecfirst Academy

Online Learning Portal

HIMSS APPROVED EDUCATION PARTNER

CSCS CERTIFIED SECURITY COMPLIANCE SPECIALIST



CCSA Certified Cyber Security Architect



© ecfirst. All Rights Reserved. 2022

ecfirst Academy

Online Learning Portal

HIMSS APPROVED EDUCATION PARTNER

Online Certification Training

CHA Certified HIPAA Administrator — HIPAA Academy

CHP Certified HIPAA Professional — HIPAA Academy

CSCS Certified Security Compliance Specialist

CCSA Certified Cyber Security Architect℠





ecfirst

Recognizes

William Anto

Who has Successfully Fulfilled the Requirements for this Program

CCSA℠

Certified Cyber Security Architect

Certificate #: 401-0000881 Issued On: July 20, 2021

July 19, 2024
Expiration Date

Uday Ali Pabrai, CEO

Completion of this program may qualify for 8 hours of Continuing Education Units (CEUs). Present this certificate as needed.

© ecfirst. All Rights Reserved. 2022

HIPAA & HITECH

ecfirst | HIPAA Academy™

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.

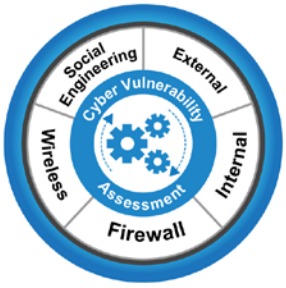
HIPAA Compliance Lifecycle

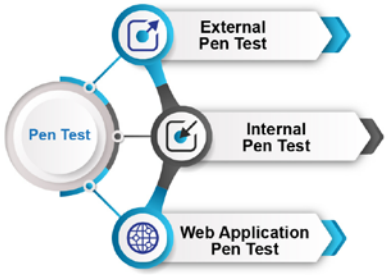


HIPAA Services

- HIPAA Policy Readiness
- HIPAA Procedure Readiness
- HIPAA Evidence Readiness
- HIPAA Professional Consultants
- HIPAA Risk Assessment
- HIPAA Remediation
- HIPAA Cybersecurity Assessment

Trust ecfirst with HIPAA







CHP Certified HIPAA Professional — HIPAA Academy

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.



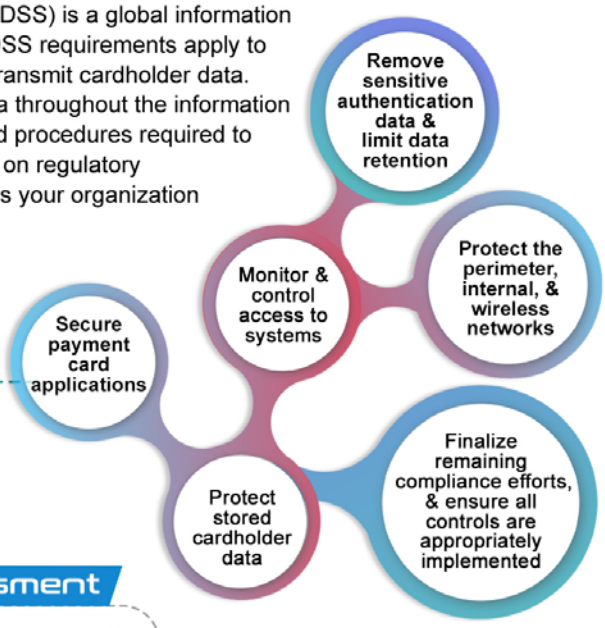
© ecfirst. All Rights Reserved. 2022

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 4.0 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.

© ecfirst. All Rights Reserved. 2022

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!

© ecfirst. All Rights Reserved. 2022

ISO 27001 Services

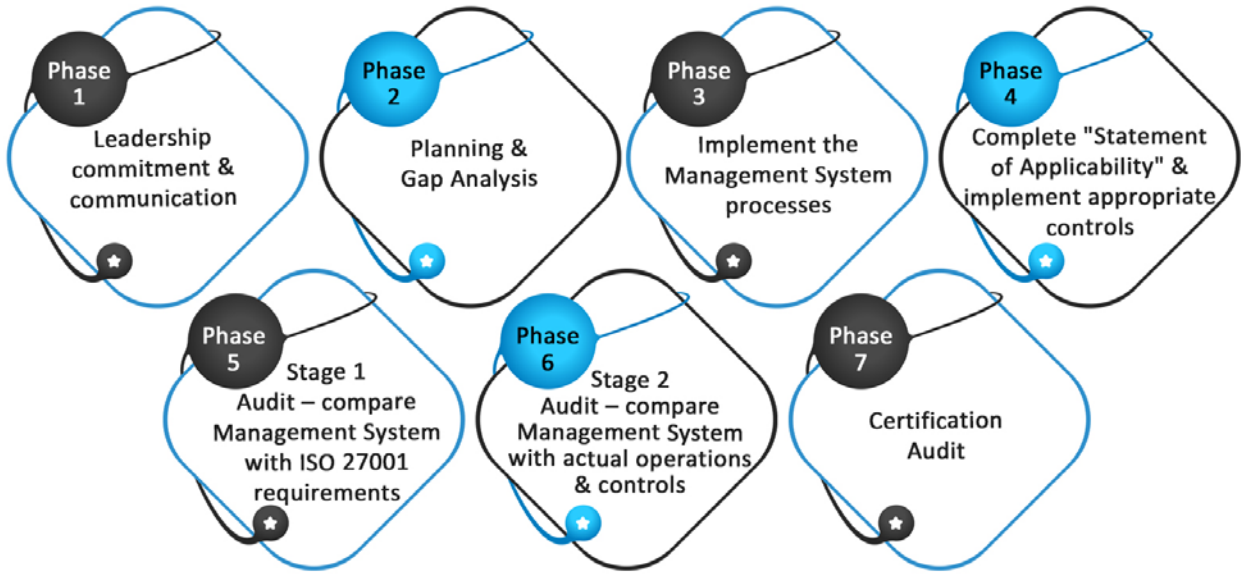
ecfirst

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, *biz*SHIELD™, are enabling organizations to easily adopt the ISO standard.

A Phased Approach to Adopt ISO 27001



© ecfirst. All Rights Reserved. 2022

ISO 27001 Services

ecfirst

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.

© ecfirst. All Rights Reserved. 2022

GDPR Services

ecfirst

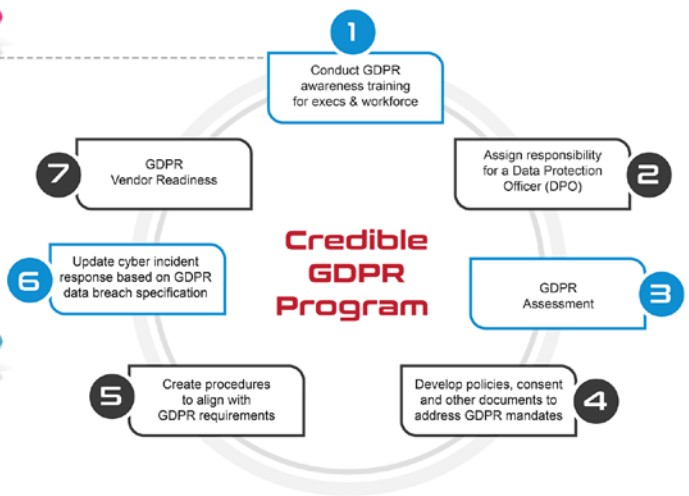
The General Data Protection Regulation (GDPR) unifies the regulations within the European Union (EU). Discuss GDPR with ecfirst. ecfirst offers a complete range of GDPR compliance solutions, including:

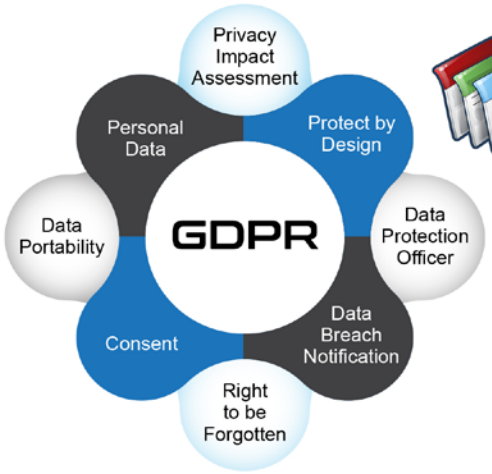
- On-Demand Consulting (ODC) Advisory Services to establish a credible GDPR compliance Program
- Managed Cybersecurity Services Program (MCSP) to monitor and maintain a GDPR compliance program
- Comprehensive risk assessment to identify GDPR compliance gaps
- Cybersecurity vulnerability assessment to 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

© ecfirst. All Rights Reserved. 2022

NIST Cybersecurity Framework Services

ecfirst

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

- 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

- NIST Cybersecurity Framework Security Assessment
- NIST Cybersecurity Framework Policy Readiness
- NIST Cybersecurity Framework Procedure Readiness
- NIST Cybersecurity Framework Evidence Readiness
- NIST Cybersecurity Framework Professional Consultants
- NIST Cybersecurity Framework CSCS

Trust ecfirst with NIST Cybersecurity



CSCS CERTIFIED SECURITY COMPLIANCE SPECIALIST

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.

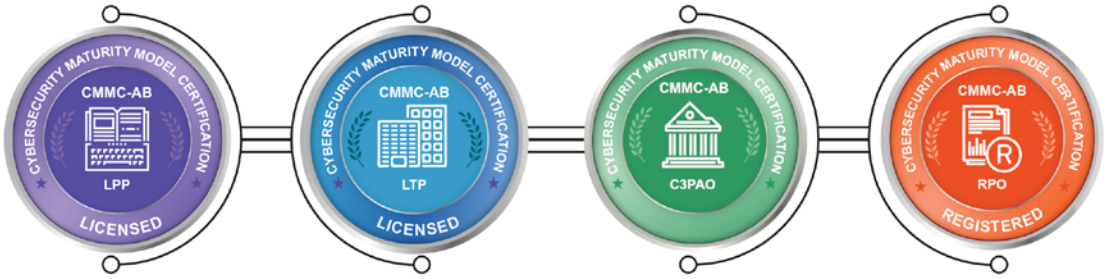


© ecfirst. All Rights Reserved. 2022

CMMC Consulting Services

Cybersecurity Maturity Model Certification

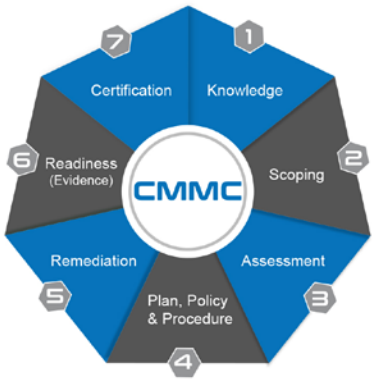
ecfirst



CMMC Readiness Services!

- CMMC Readiness Assessment
- CMMC Policy Updates
- CMMC Procedure Draft
- CMMC Evidence Guidance
- CMMC Training Program
- CMMC Remediation

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!"

© ecfirst. All Rights Reserved. 2022

On-Demand Consulting (ODC)

On-site | Virtual

ecfirst

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)

© ecfirst. All Rights Reserved. 2022

Managed Cybersecurity Services Program (MCSP)
Fixed Monthly Fee. Flexible. Scalable

ecfirst

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

© ecfirst. All Rights Reserved. 2022

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

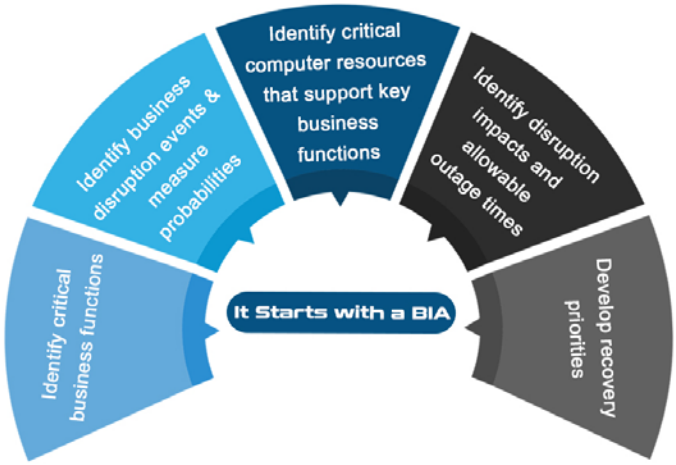
ecfirst

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

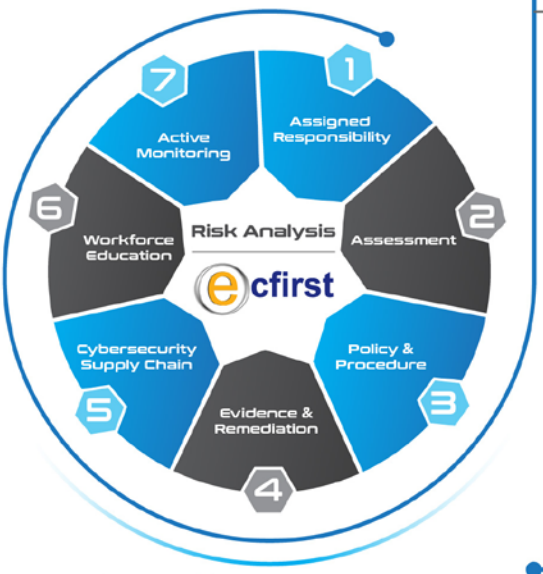
1. Business Impact Analysis Report
2. An IT Disaster Recovery Plan

© ecfirst. All Rights Reserved. 2022

Risk & Cyber Assessment

ecfirst

Signature Methodology



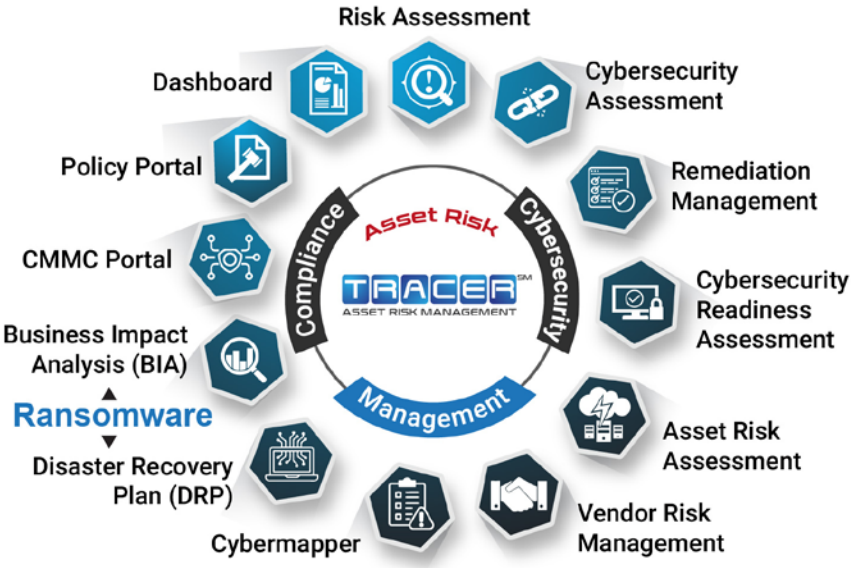
Risk Analysis

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™ ASSET RISK MANAGEMENT

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



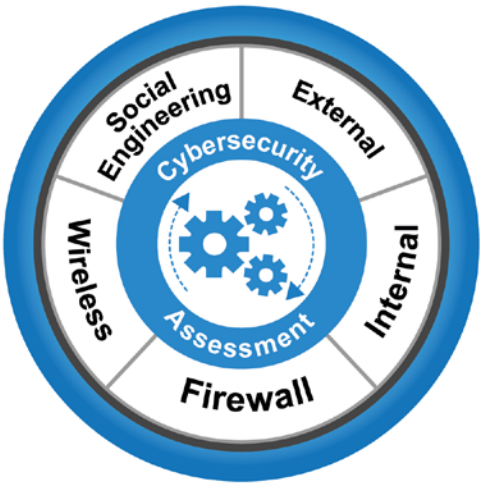
© ecfirst. All Rights Reserved. 2022

Cyber Assessments

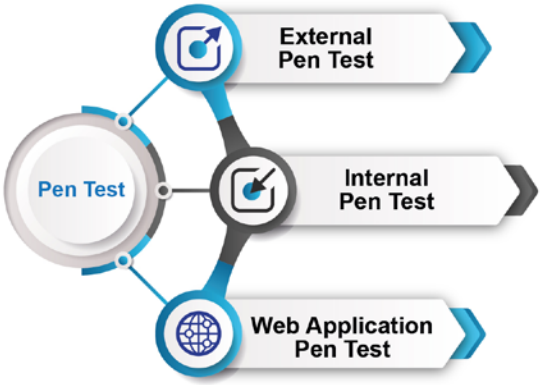
Performed Remotely!

ecfirst

Cybersecurity Assessment



Pen Test

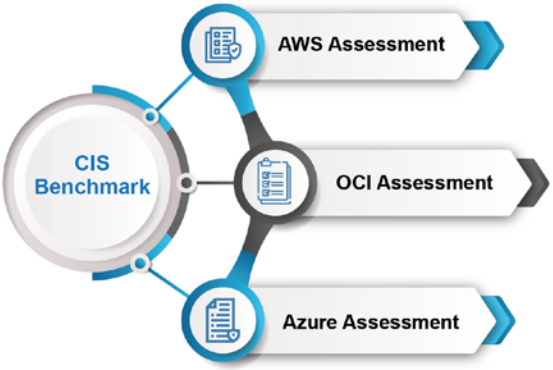


Deep Database Assessment

Social Engineering



CIS Benchmark



© ecfirst. All Rights Reserved. 2022

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

	High Risk	Medium Risk	Low Risk	Medium Risk of Successful Attack
External System Vulnerability Totals	1	27	8	
Web App Vulnerability Totals	0	1	5	Low Risk of Successful Attack
Internal Vulnerability Totals	5	105	11	Medium Risk of Successful Attack
Firewall Configuration Vulnerability Totals	0	0	0	Low Risk of Successful Attack

SAMPLE

© ecfirst. All Rights Reserved. 2022

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

SAMPLE

© ecfirst. All Rights Reserved. 2022

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

© ecfirst. All Rights Reserved. 2022

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.

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

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

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

© ecfirst. All Rights Reserved. 2022

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	X
Detailed Analysis	✓
Corrective Action Plan (CAP)	✓
Detailed Remediation Steps	✓
Executive Brief	X

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

© ecfirst. All Rights Reserved. 2022

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

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

© ecfirst. All Rights Reserved. 2022

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 (WAP) 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.

© ecfirst. All Rights Reserved. 2022

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

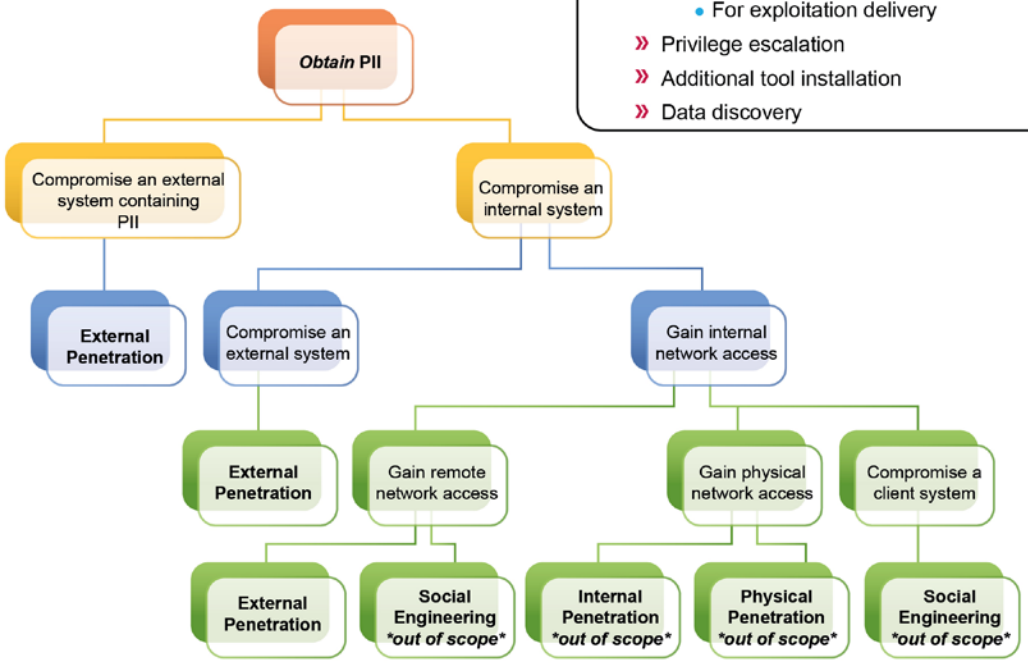
- Client personnel and cultural information
- Client business terminology
- Technical infrastructure information

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



© ecfirst. All Rights Reserved. 2022

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

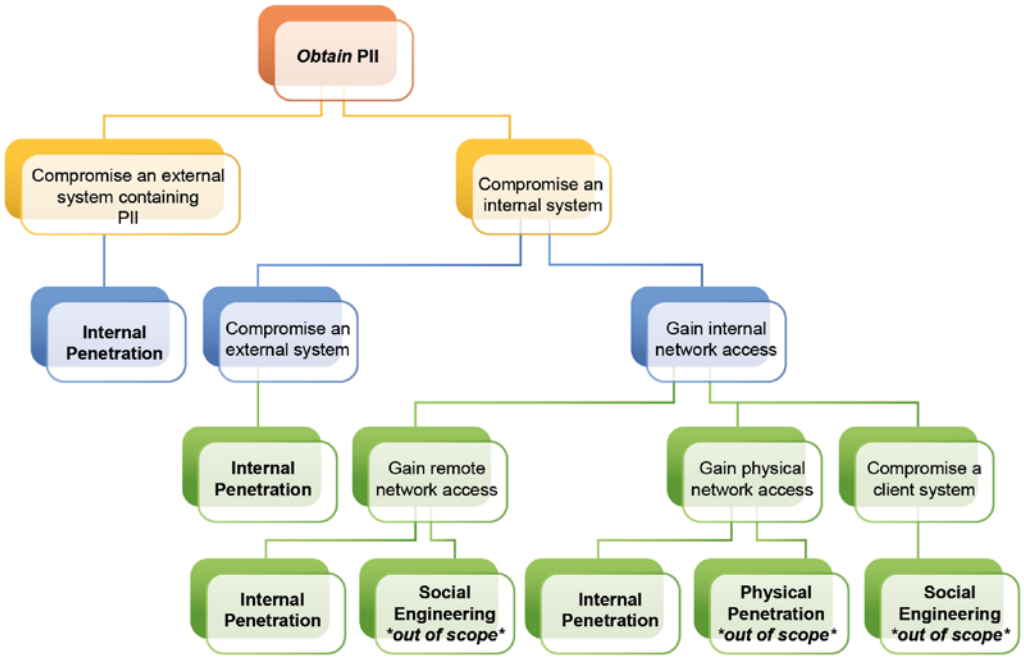
- End-user attacks (i.e. phishing, man-in-the-middle, client-side exploitation, etc.)
- Denial of Service attacks

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



© ecfirst. All Rights Reserved. 2022

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.

© ecfirst. All Rights Reserved. 2022

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

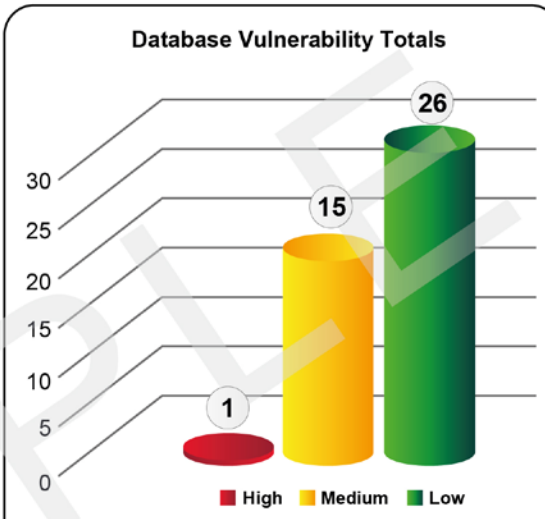
Overall Risk: **High**

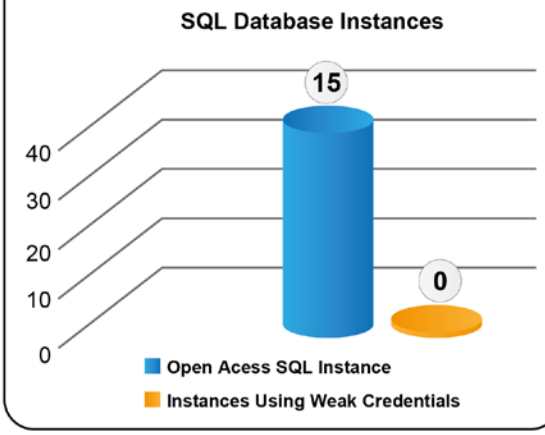
ecfirst scanned specific subnets to identify systems running MSSQL databases that allow open access; by open access we mean access to the login prompt. ecfirst was able to identify 37 database instances that allow open access. This allows an attacker the opportunity to attempt unauthorized logins to 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.





SAMPLE

© ecfirst. All Rights Reserved. 2022

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.

© ecfirst. All Rights Reserved. 2022

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
Total	**38**	**19**	**19**

SAMPLE

© ecfirst. All Rights Reserved. 2022

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:

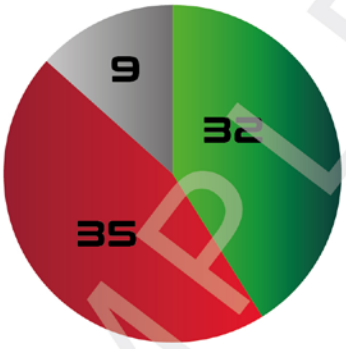
- Alignment with CIS Benchmark for Azure Foundations, Level 1 settings
- Correctly configured settings where further action is required to achieve full security benefits
- Review of available versus used licenses and their impact
- Analysis of findings, including strengths and prioritized areas for improvement

Configuration benchmark alignment areas include:

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

Executive Dashboard

Compliance Progress



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

SAMPLE

© ecfirst. All Rights Reserved. 2022

Virtual ISO & Infosec Staffing Program

ecfirst

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.

© ecfirst. All Rights Reserved. 2022

Biomed & Internet of Things (IoT) Cybersecurity Readiness

ecfirst

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℠ (CCSA℠) 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

© ecfirst. All Rights Reserved. 2022

Biomed & Internet of Things (IoT) Cybersecurity Readiness

ecfirst

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

Training & Certification

CCSA℠
Certified Cyber Security Architect

- 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).

© ecfirst. All Rights Reserved. 2022

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

Virtual | On-site | Public Schedule

CHP Certified HIPAA Professional HIPAA Academy | HIMSS APPROVED EDUCATION PARTNER | CEU 16 Hours

Learn HIPAA. Know HIPAA!

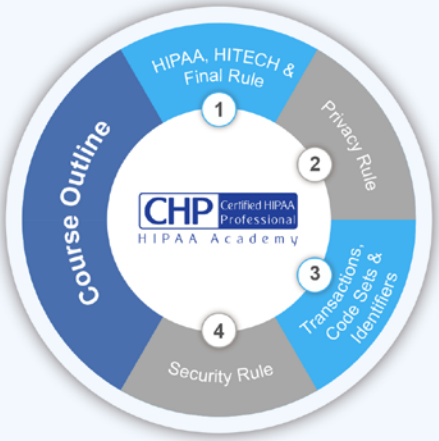
The Health Insurance Portability and Accountability Act (HIPAA) is about insurance portability, fraud, and administrative simplification.

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 correction 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

© ecfirst. All Rights Reserved. 2022

The World's First Program Focused on Compliance & Cybersecurity

Virtual | On-site | Public Schedule

CSCS™ CERTIFIED SECURITY COMPLIANCE SPECIALIST | HIMSS APPROVED EDUCATION PARTNER | CEU 16 Hours

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

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

© ecfirst. All Rights Reserved. 2022

An Executive Cyber Security Program

Virtual | On-site | Public Schedule

CCSA℠ Certified Cyber Security Architect | HIMSS APPROVED EDUCATION PARTNER | CEU 8 Hours

Step thru U.S. DoD Cybersecurity Mandate: CMMC

CCSA℠ 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.
- Examine CMMC domains and CMMC practices required for organizations.



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℠ 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

© ecfirst. All Rights Reserved. 2022

Ali Pabrai



U.S. Department of Defense CMMC Program

CMMC-AB PROVISIONAL INSTRUCTOR

CMMC-AB PROVISIONAL ASSESSOR

Global Cyber Defense Thought Leader

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

ISACA TOP-RATED SPEAKER ★★★★★

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*

ISACA® Trust in, and value from, information systems

FBI Conference

INFRAGARD 25 YEARS PARTNERSHIP FOR PROTECTION

"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*

Author



Getting Started with HIPAA
First published book on HIPAA



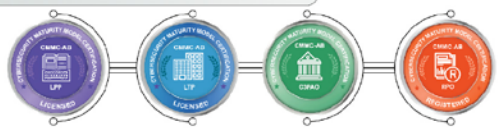
UNIX Internetworking
First book on UNIX & Networks



Internet & TCP/IP Network Security
First book on TCP/IP security

The ecfirst CMMC Ecosystem

ecfirst



HITRUST®
Authorized External Assessor

ecfirst | Reimagining Cyber Defense

Corporate Office

295 NE Venture Drive

Waukee, IA 50263

United States

Kris Laidley

Team Lead, Business Development & Certification Program

Email: Kris.Laidley@ecfirst.com

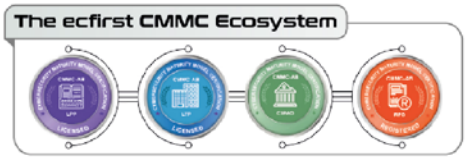
HIPAA™ Academy

CSCS™ CERTIFIED SECURITY COMPLIANCE SPECIALIST

CHP Certified HIPAA Professional HIPAA Academy

CCSA℠ Certified Cyber Security Architect

TRACER℠ ASSET RISK MANAGEMENT



HIMSS APPROVED EDUCATION PARTNER

© ecfirst. All Rights Reserved. 2022