June 10, 2022
Anaheim, CA

HCCA™
Health Care Compliance Association

NIST Cybersecurity Framework

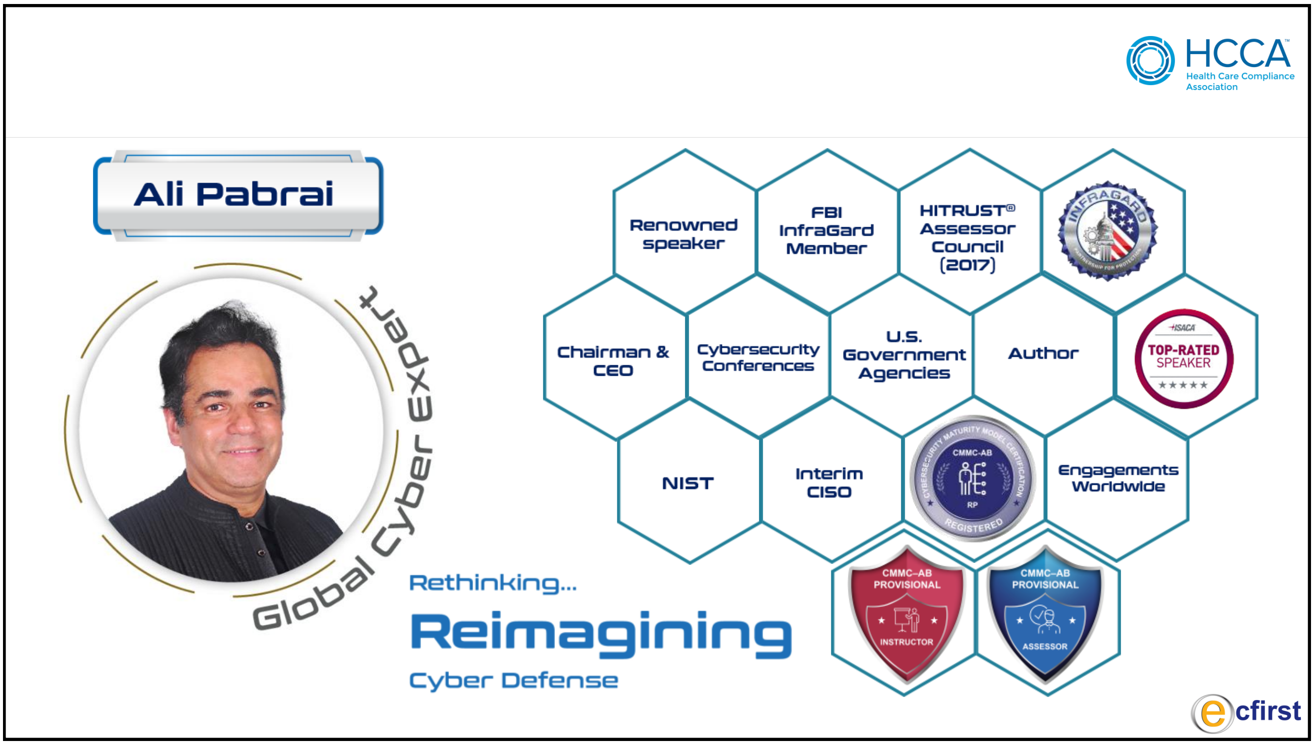
Reimagining Cyber Defense

TOP-RATED SPEAKER

Ali Pabrai
Global Cybersecurity & Compliance Expert

ecfirst

HITRUST®
Authorized External Assessor



HCCA™
Health Care Compliance Association

Ali Pabrai

Global Cyber Expert

- Renowned speaker
- FBI InfraGard Member
- HITRUST® Assessor Council (2017)
- Chairman & CEO
- Cybersecurity Conferences
- U.S. Government Agencies
- Author
- TOP-RATED SPEAKER
- NIST
- Interim CISO
- Engagements Worldwide

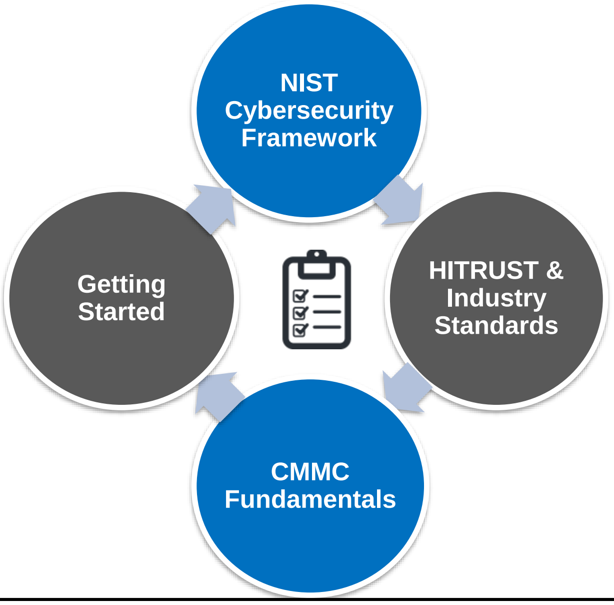
INFRAGARD
CMMC-AB RP REGISTERED
CMMC-AB PROVISIONAL INSTRUCTOR
CMMC-AB PROVISIONAL ASSESSOR

Rethinking...
Reimagining
Cyber Defense

ecfirst

Agenda

HCCA Health Care Compliance Association



NIST Cybersecurity Framework

HITRUST & Industry Standards

CMMC Fundamentals

Getting Started

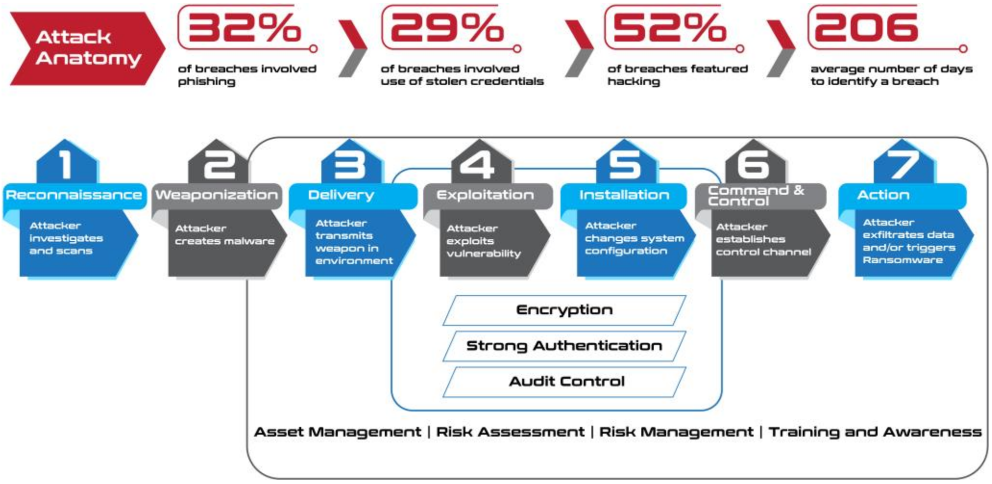
Learning Objectives

- Establishing an evidence-based program based NIST standards.
- Achieving CMMC Certification, a new DoD cyber standard based on NIST.
- Managing the cyber supply chain to mitigate risk from business associates and third parties.

ecfirst

Cyber Kill chain

HCCA Health Care Compliance Association



Attack Anatomy

32% of breaches involved phishing

29% of breaches involved use of stolen credentials

52% of breaches featured hacking

206 average number of days to identify a breach

1 Reconnaissance: Attacker investigates and scans

2 Weaponization: Attacker creates malware

3 Delivery: Attacker transmits weapon in environment

4 Exploitation: Attacker exploits vulnerability

5 Installation: Attacker changes system configuration

6 Command & Control: Attacker establishes control channel

7 Action: Attacker exfiltrates data and/or triggers Ransomware

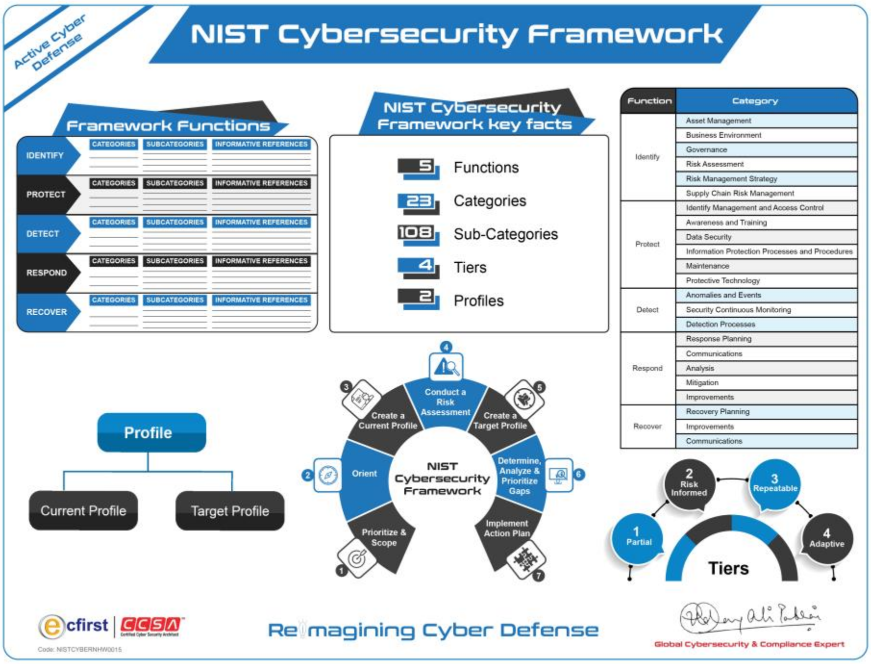
Encryption

Strong Authentication

Audit Control

Asset Management | Risk Assessment | Risk Management | Training and Awareness

ecfirst



Active Cyber Defense

NIST Cybersecurity Framework

Framework Functions

IDENTIFY	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
PROTECT	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
DETECT	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
RESPOND	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
RECOVER	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES

NIST Cybersecurity Framework key facts

5	Functions
23	Categories
108	Sub-Categories
4	Tiers
2	Profiles

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Identify Management and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

Profile
Current Profile
Target Profile

NIST Cybersecurity Framework
1 Prioritize & Scope
2 Orient
3 Create a Current Profile
4 Conduct a Risk Assessment
5 Create a Target Profile
6 Determine, Analyze & Prioritize Gaps
7 Implement Action Plan

Tiers
1 Partial
2 Risk Informed
3 Repeatable
4 Adaptive

ecfirst | CCSA Certified Cyber Security Architect

Code: NISTCYBERNHW0015

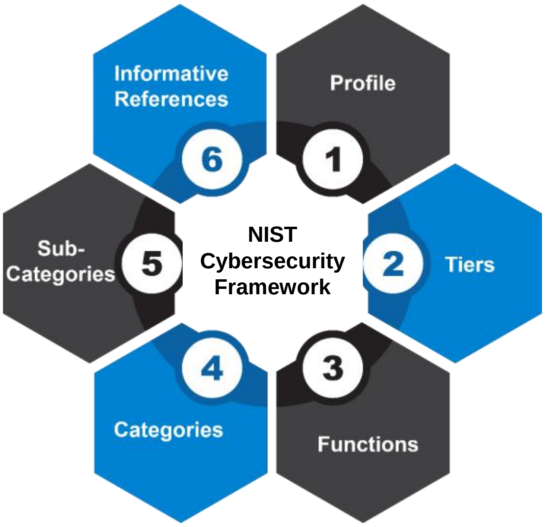
Reimagining Cyber Defense

Global Cybersecurity & Compliance Expert

NIST Cybersecurity Framework

NIST Cybersecurity Framework
Core Concepts

HCCA Health Care Compliance Association

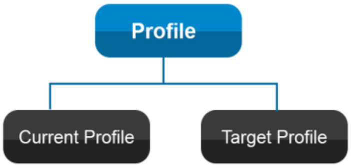


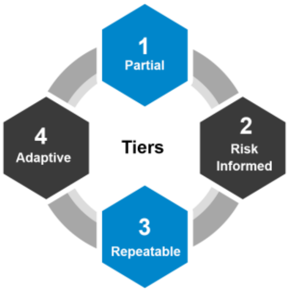
- NIST Cybersecurity Framework is the framework that executives can trust to base their HIPAA compliance program.
- This framework can be used by organizations that may be small or large, including business associates, physician practices, hospitals, IT firms, government agencies, and other healthcare entities.

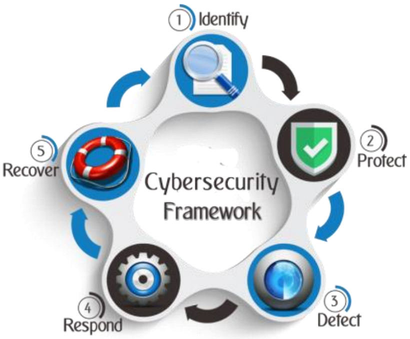
ecfirst

Align Compliance with NIST Cybersecurity Framework

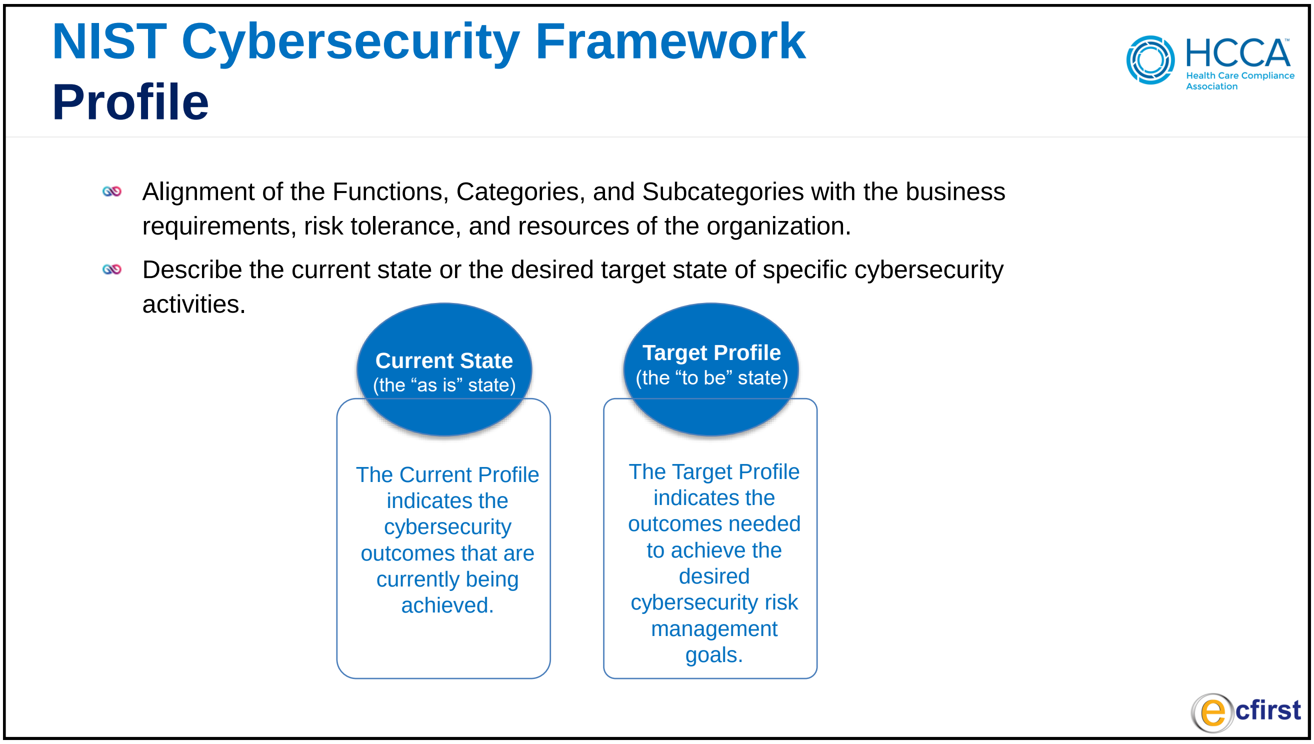
HCCA Health Care Compliance Association







ecfirst



NIST Cybersecurity Framework
Profile

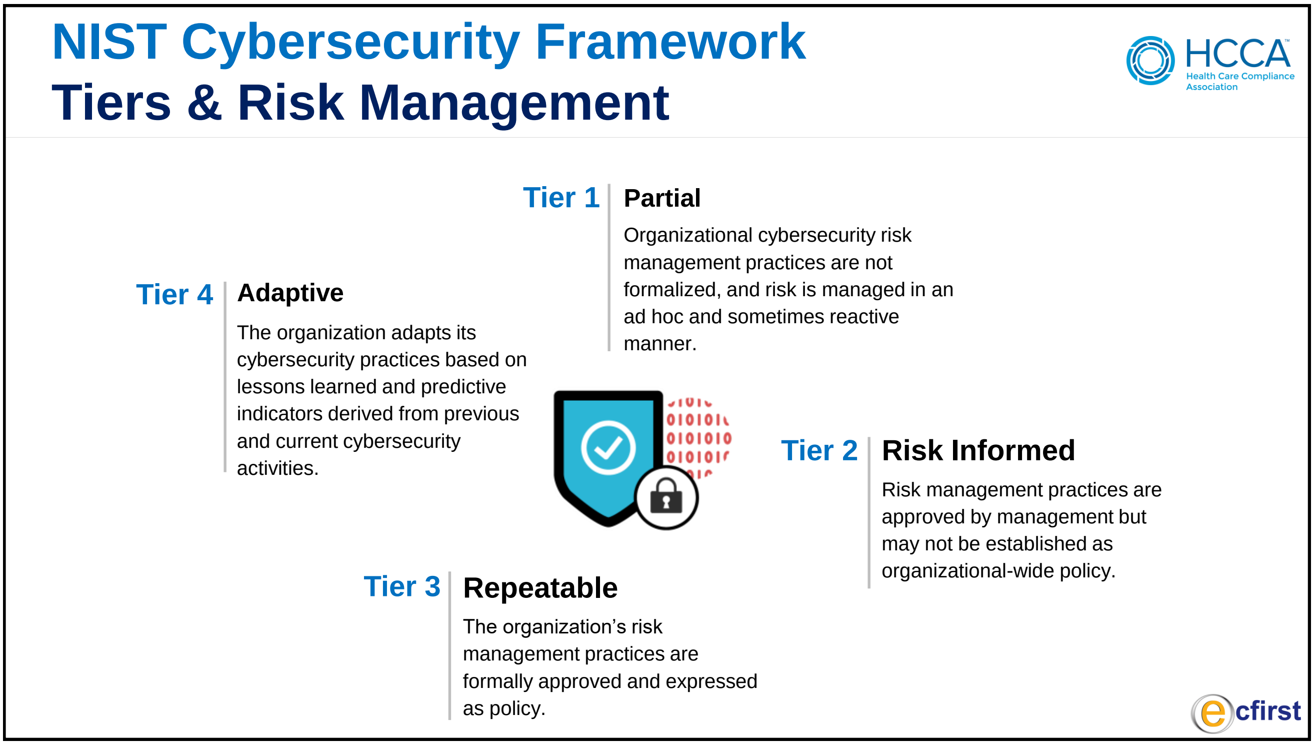
- Alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization.
- Describe the current state or the desired target state of specific cybersecurity activities.

Current State
(the "as is" state)

The Current Profile indicates the cybersecurity outcomes that are currently being achieved.

Target Profile
(the "to be" state)

The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals.



NIST Cybersecurity Framework
Tiers & Risk Management

Tier 1 **Partial**

Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.

Tier 2 **Risk Informed**

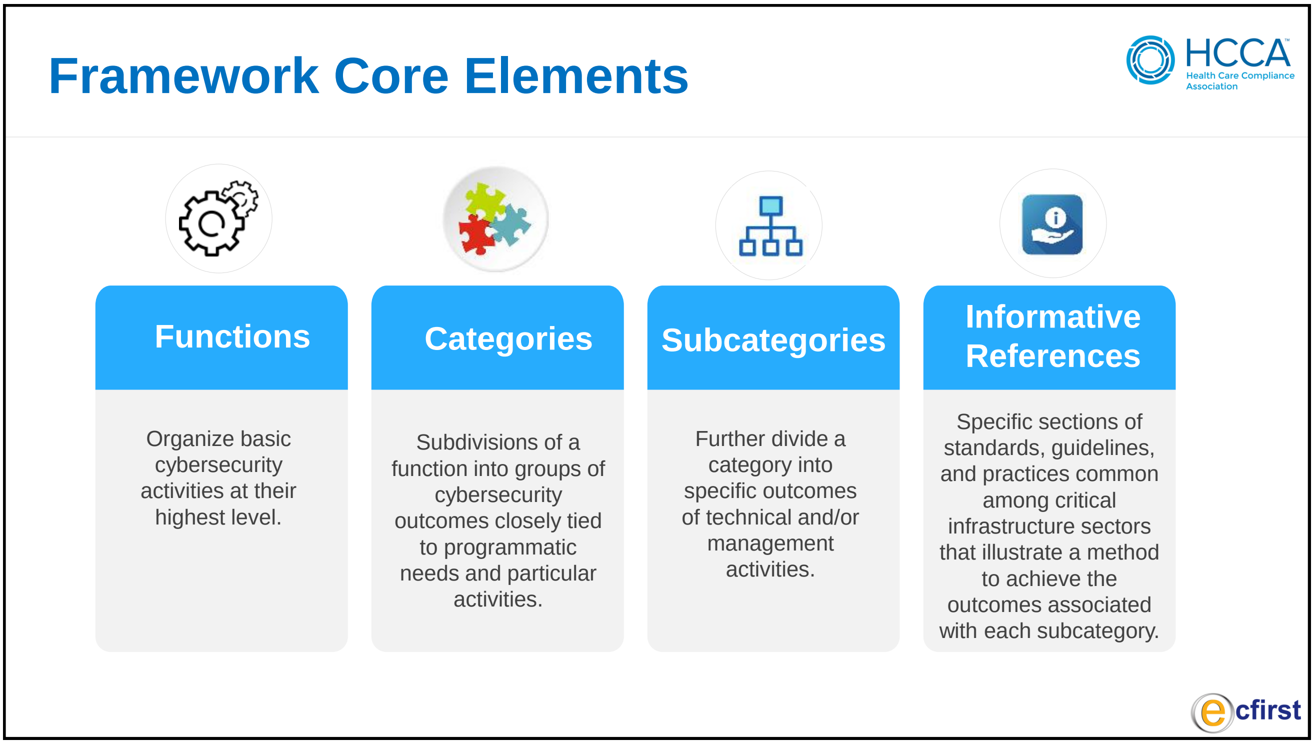
Risk management practices are approved by management but may not be established as organizational-wide policy.

Tier 3 **Repeatable**

The organization's risk management practices are formally approved and expressed as policy.

Tier 4 **Adaptive**

The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.



Framework Core Elements

HCCA Health Care Compliance Association

Functions

Organize basic cybersecurity activities at their highest level.

Categories

Subdivisions of a function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities.

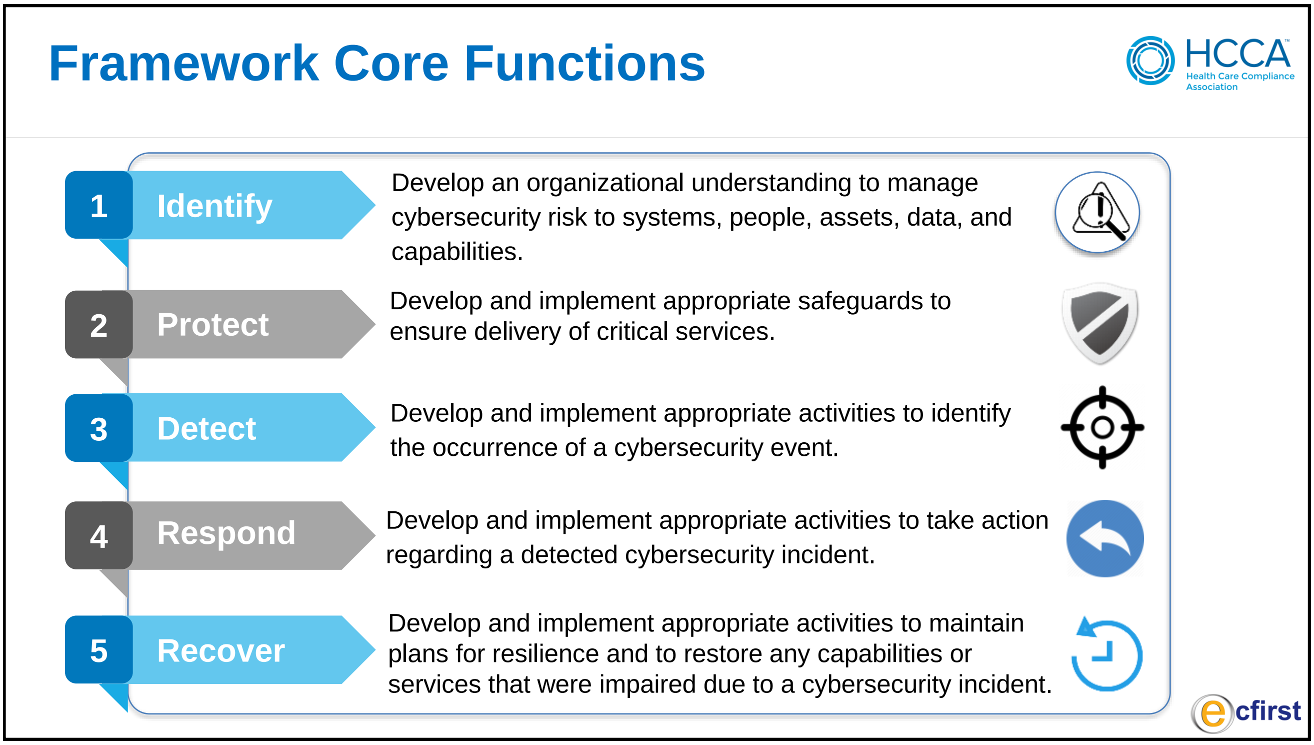
Subcategories

Further divide a category into specific outcomes of technical and/or management activities.

Informative References

Specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each subcategory.

ecfirst



Framework Core Functions

HCCA Health Care Compliance Association

1 **Identify** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

2 **Protect** Develop and implement appropriate safeguards to ensure delivery of critical services.

3 **Detect** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

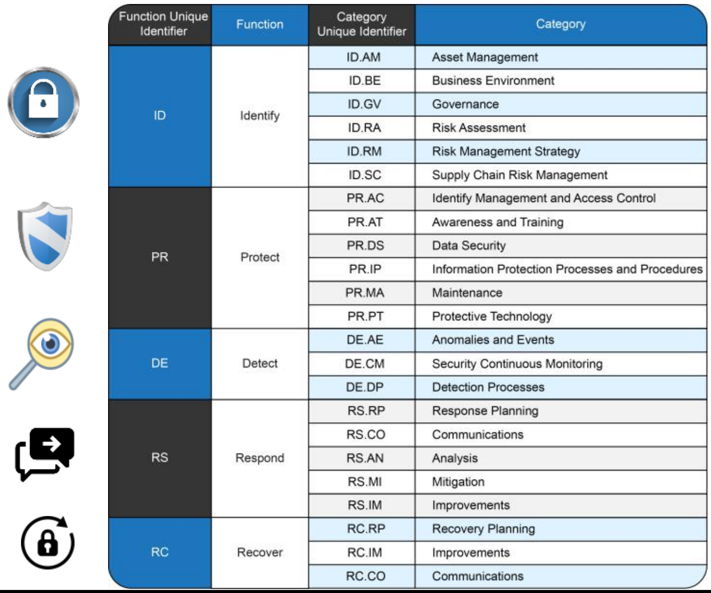
4 **Respond** Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

5 **Recover** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

ecfirst

NIST Cybersecurity Framework
Foundation for Cybersecurity

HCCA Health Care Compliance Association



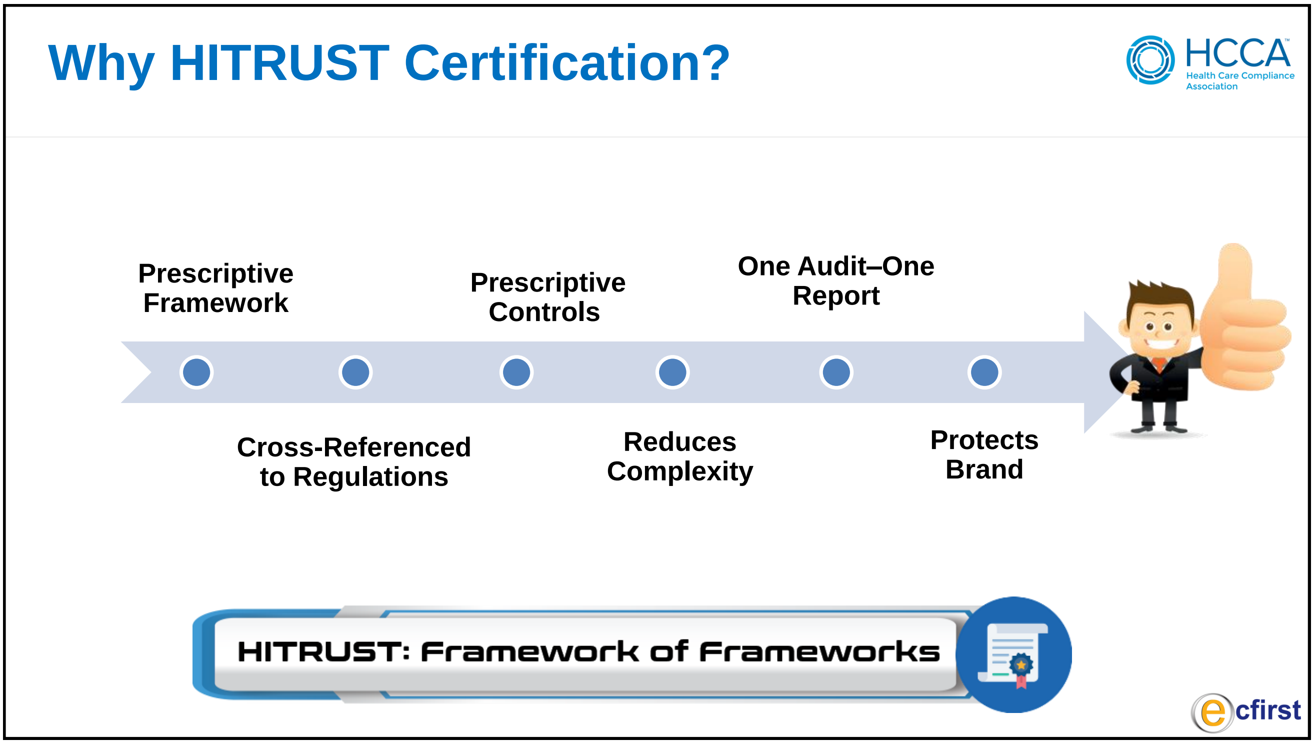
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identify Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

ecfirst

HCCA Health Care Compliance Association

HITRUST & Industry Standards

ecfirst



Why HITRUST Certification?

Prescriptive Framework

Cross-Referenced to Regulations

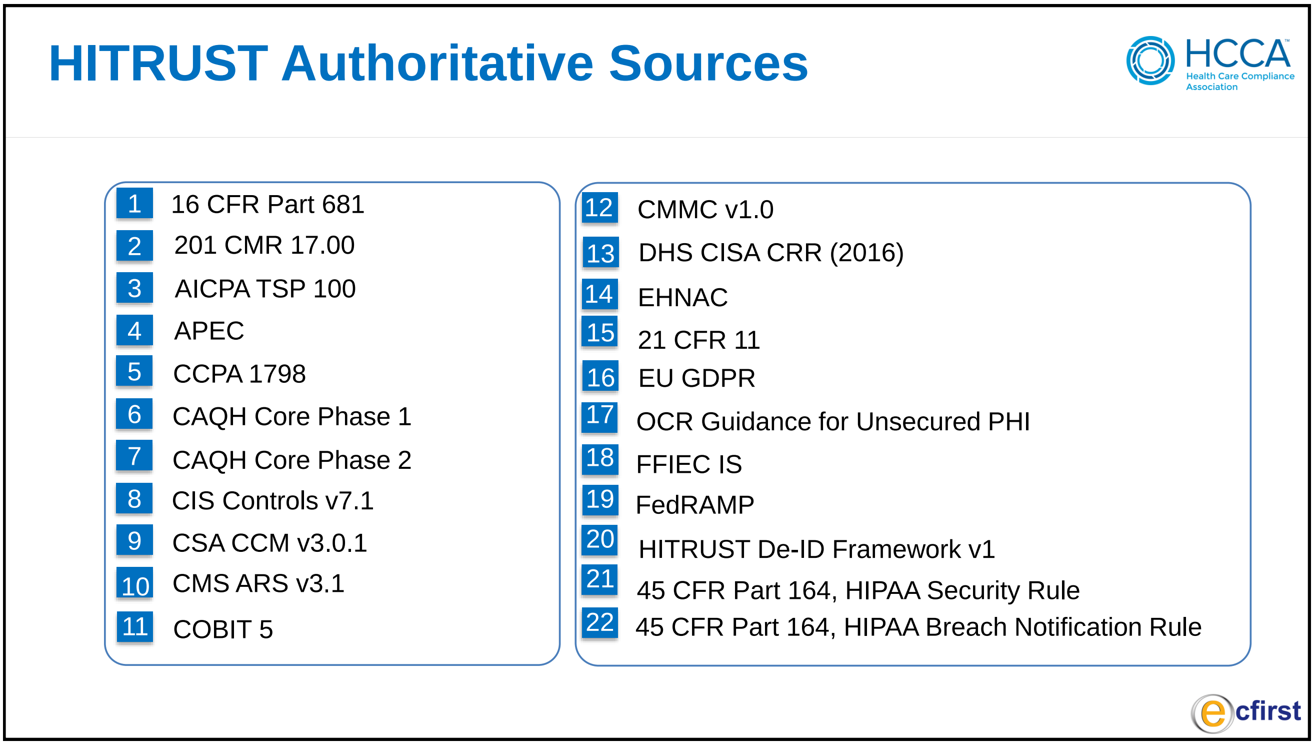
Prescriptive Controls

Reduces Complexity

One Audit–One Report

Protects Brand

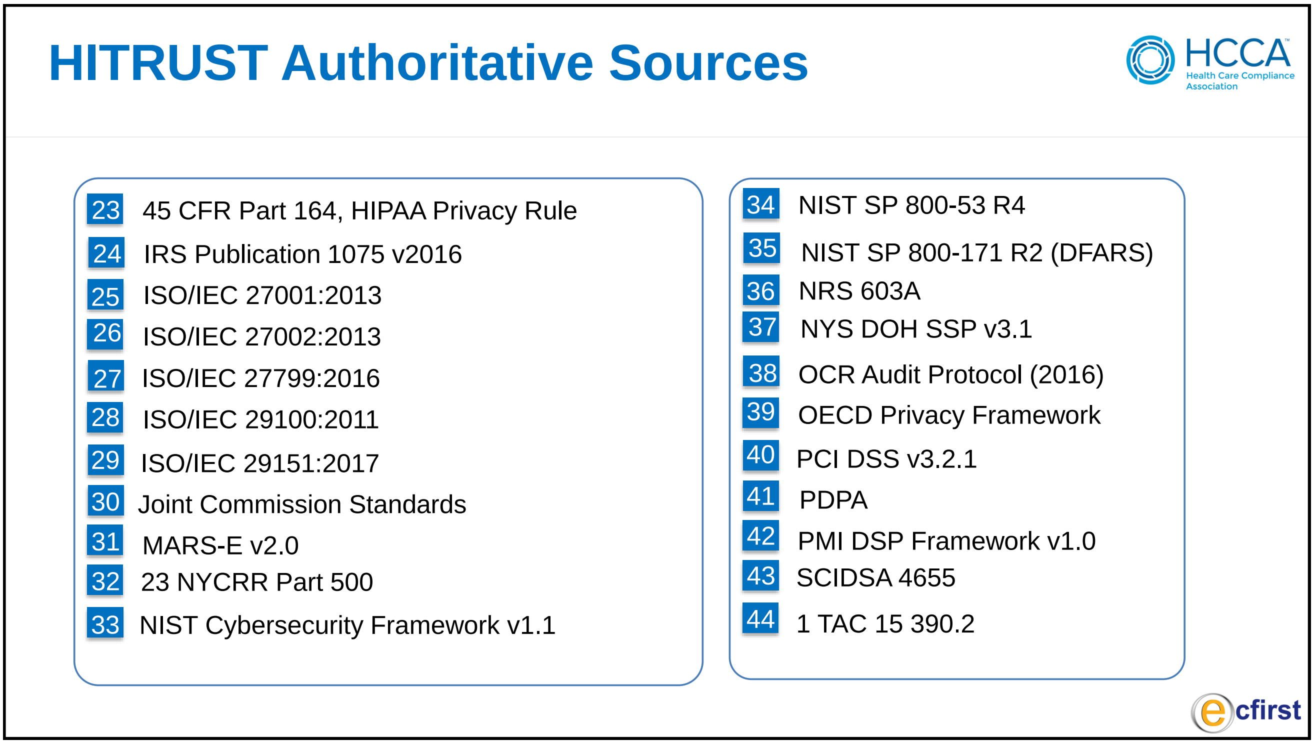
HITRUST: Framework of Frameworks



HITRUST Authoritative Sources

1 16 CFR Part 681
2 201 CMR 17.00
3 AICPA TSP 100
4 APEC
5 CCPA 1798
6 CAQH Core Phase 1
7 CAQH Core Phase 2
8 CIS Controls v7.1
9 CSA CCM v3.0.1
10 CMS ARS v3.1
11 COBIT 5

12 CMMC v1.0
13 DHS CISA CRR (2016)
14 EHNAC
15 21 CFR 11
16 EU GDPR
17 OCR Guidance for Unsecured PHI
18 FFIEC IS
19 FedRAMP
20 HITRUST De-ID Framework v1
21 45 CFR Part 164, HIPAA Security Rule
22 45 CFR Part 164, HIPAA Breach Notification Rule



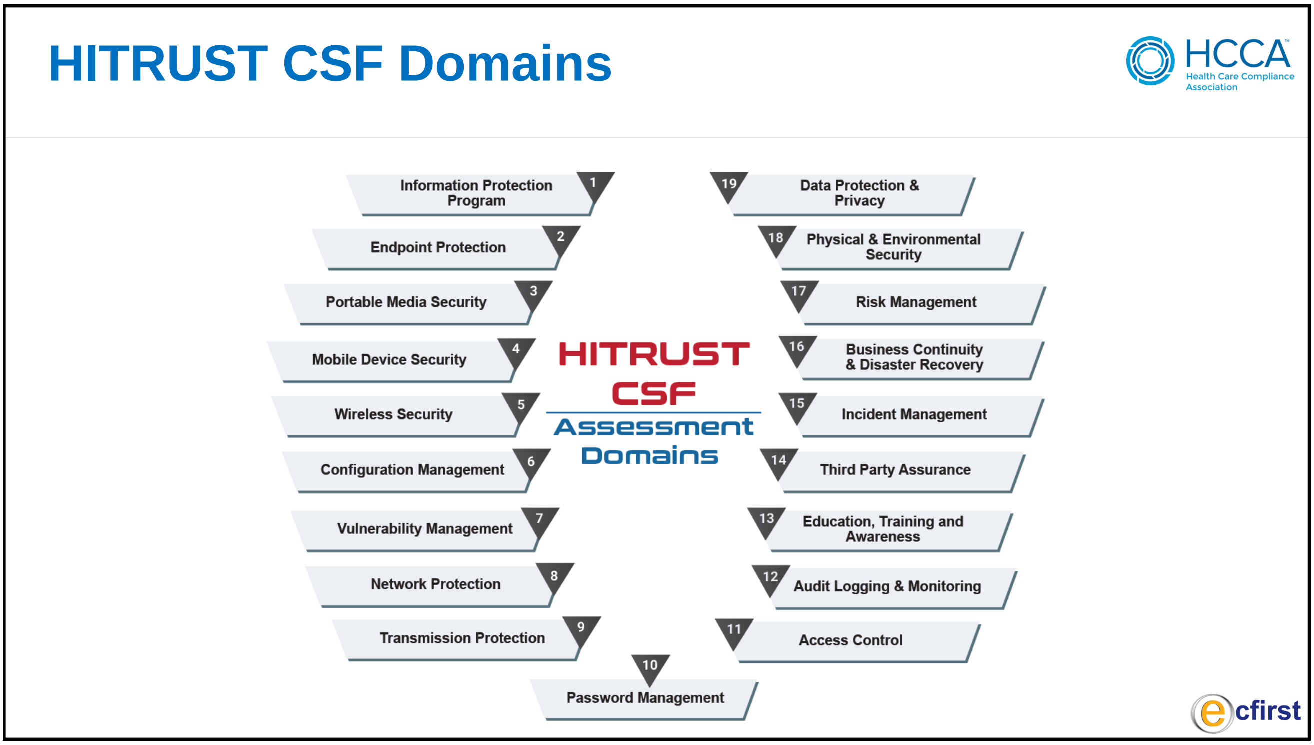
HITRUST Authoritative Sources

HCCA Health Care Compliance Association

23 45 CFR Part 164, HIPAA Privacy Rule
24 IRS Publication 1075 v2016
25 ISO/IEC 27001:2013
26 ISO/IEC 27002:2013
27 ISO/IEC 27799:2016
28 ISO/IEC 29100:2011
29 ISO/IEC 29151:2017
30 Joint Commission Standards
31 MARS-E v2.0
32 23 NYCRR Part 500
33 NIST Cybersecurity Framework v1.1

34 NIST SP 800-53 R4
35 NIST SP 800-171 R2 (DFARS)
36 NRS 603A
37 NYS DOH SSP v3.1
38 OCR Audit Protocol (2016)
39 OECD Privacy Framework
40 PCI DSS v3.2.1
41 PDPA
42 PMI DSP Framework v1.0
43 SCIDSA 4655
44 1 TAC 15 390.2

ecfirst

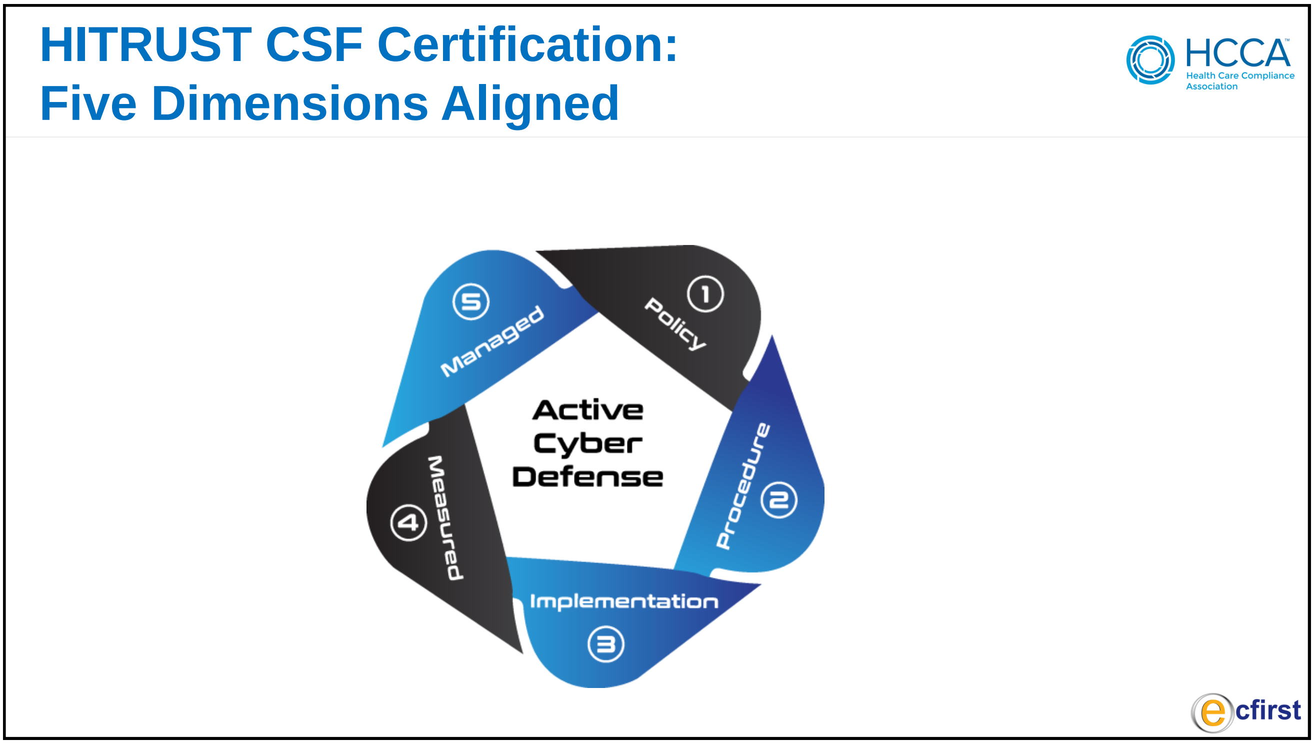


HITRUST CSF Domains

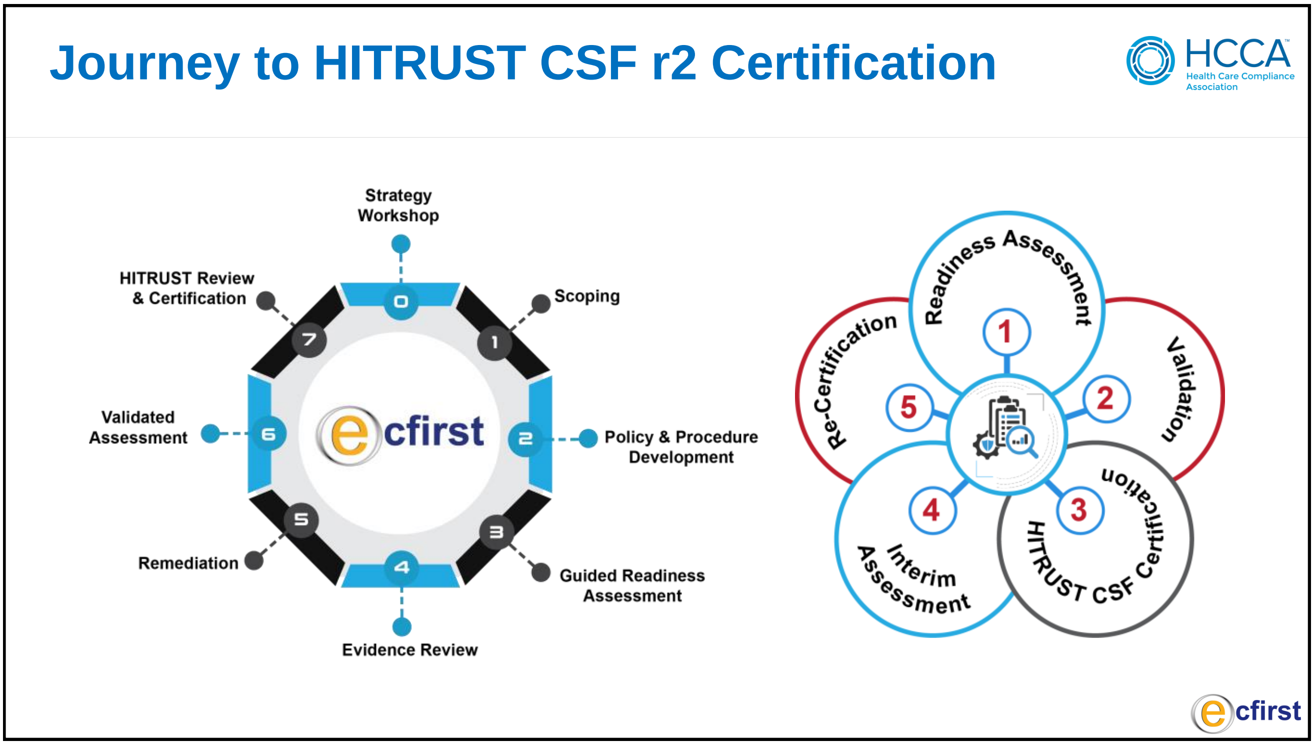
HCCA Health Care Compliance Association

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

ecfirst



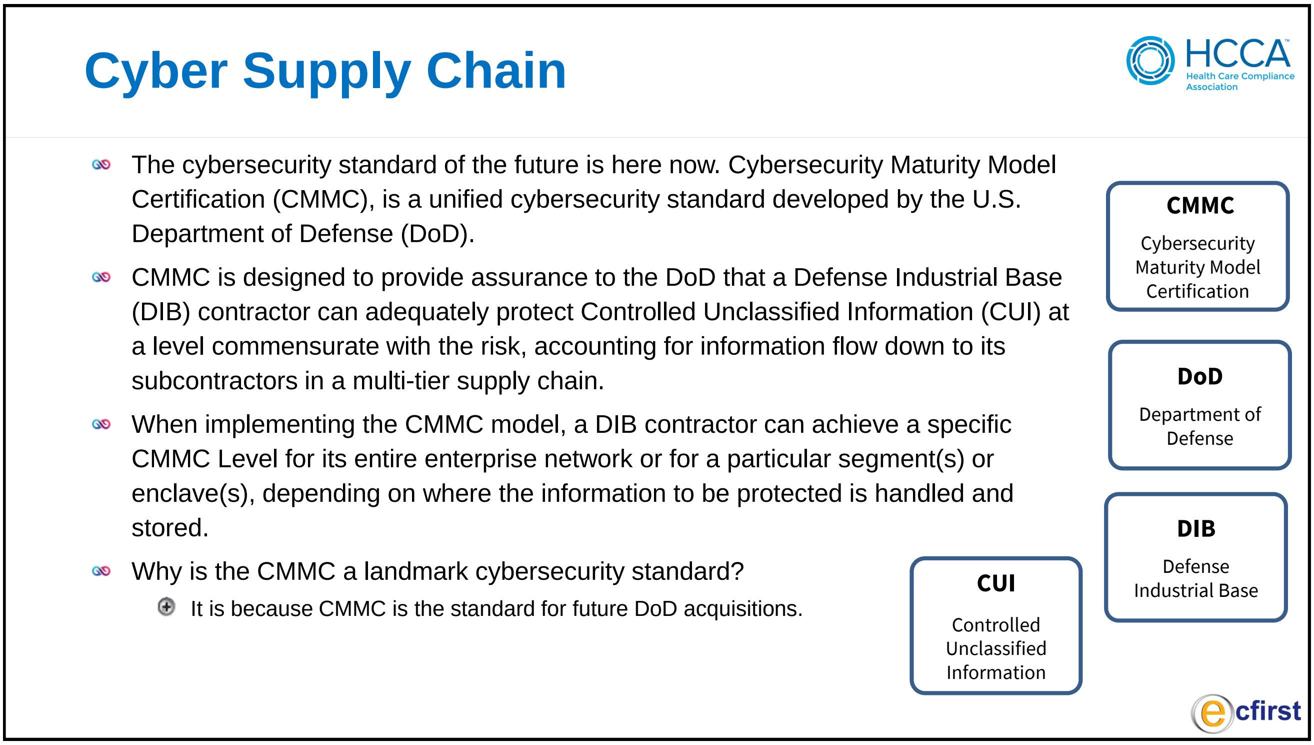
HITRUST CSF Certification: Five Dimensions Aligned



Journey to HITRUST CSF r2 Certification

CMMC Fundamentals

CMMC Cybersecurity Maturity Model Certification (CMMC)



Cyber Supply Chain

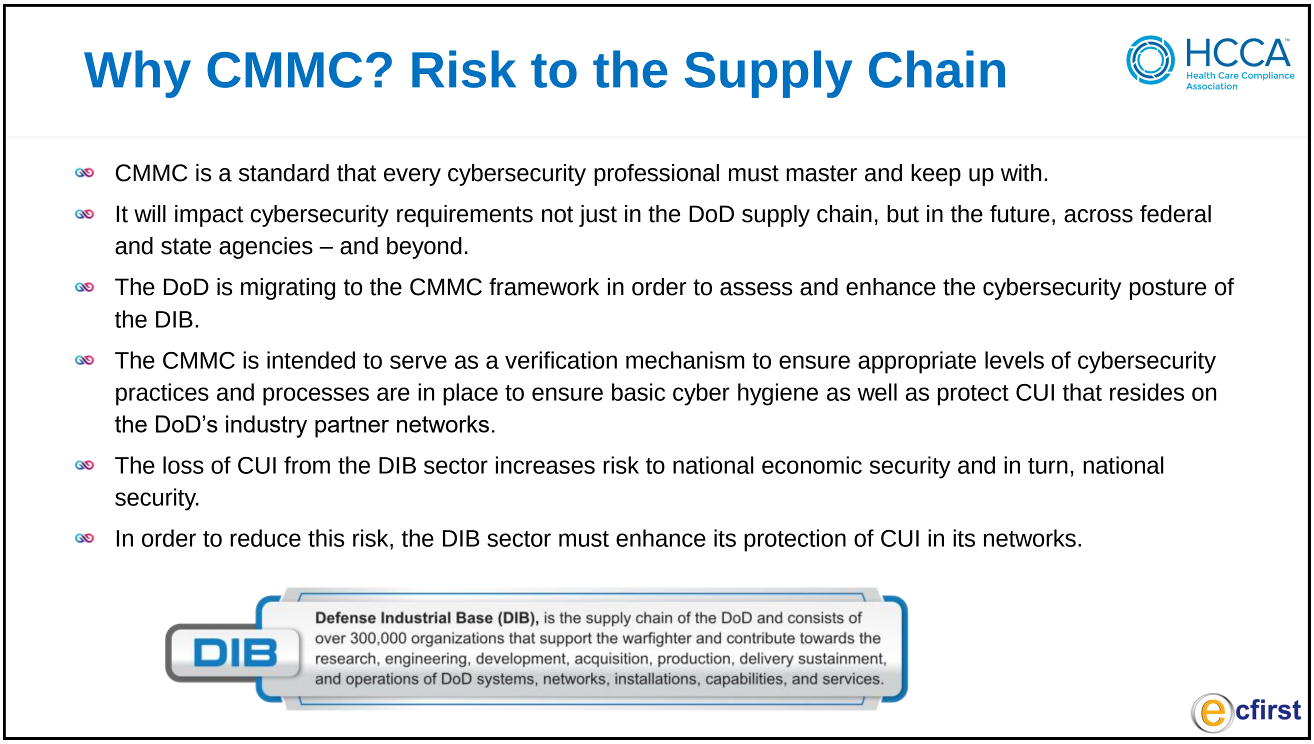
- The cybersecurity standard of the future is here now. Cybersecurity Maturity Model Certification (CMMC), is a unified cybersecurity standard developed by the U.S. Department of Defense (DoD).
- CMMC is designed to provide assurance to the DoD that a Defense Industrial Base (DIB) contractor can adequately protect Controlled Unclassified Information (CUI) at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain.
- When implementing the CMMC model, a DIB contractor can achieve a specific CMMC Level for its entire enterprise network or for a particular segment(s) or enclave(s), depending on where the information to be protected is handled and stored.
- Why is the CMMC a landmark cybersecurity standard?
  - It is because CMMC is the standard for future DoD acquisitions.

CMMC
Cybersecurity Maturity Model Certification

DoD
Department of Defense

DIB
Defense Industrial Base

CUI
Controlled Unclassified Information



Why CMMC? Risk to the Supply Chain

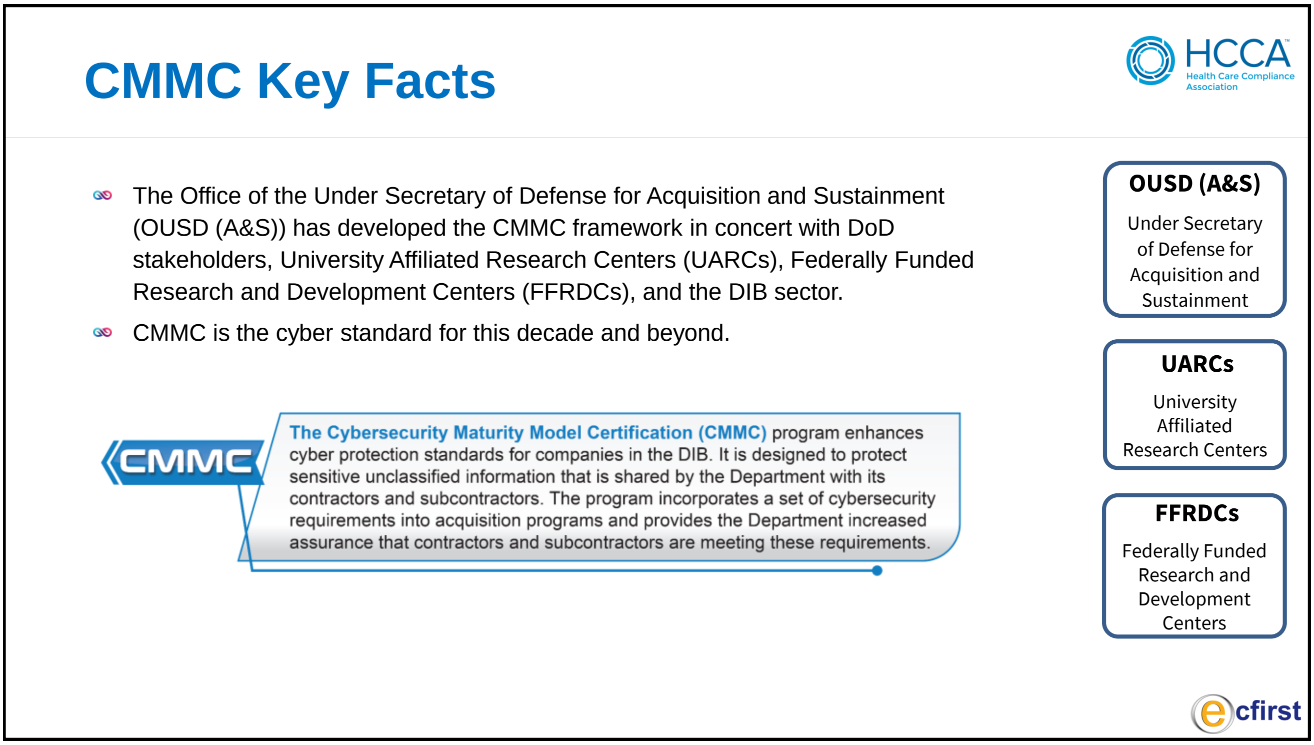
HCCA Health Care Compliance Association

- CMMC is a standard that every cybersecurity professional must master and keep up with.
- It will impact cybersecurity requirements not just in the DoD supply chain, but in the future, across federal and state agencies – and beyond.
- The DoD is migrating to the CMMC framework in order to assess and enhance the cybersecurity posture of the DIB.
- The CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene as well as protect CUI that resides on the DoD's industry partner networks.
- The loss of CUI from the DIB sector increases risk to national economic security and in turn, national security.
- In order to reduce this risk, the DIB sector must enhance its protection of CUI in its networks.

DIB

Defense Industrial Base (DIB), is the supply chain of the DoD and consists of over 300,000 organizations that support the warfighter and contribute towards the research, engineering, development, acquisition, production, delivery sustainment, and operations of DoD systems, networks, installations, capabilities, and services.

ecfirst



CMMC Key Facts

HCCA Health Care Compliance Association

- The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD (A&S)) has developed the CMMC framework in concert with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDCs), and the DIB sector.
- CMMC is the cyber standard for this decade and beyond.

CMMC

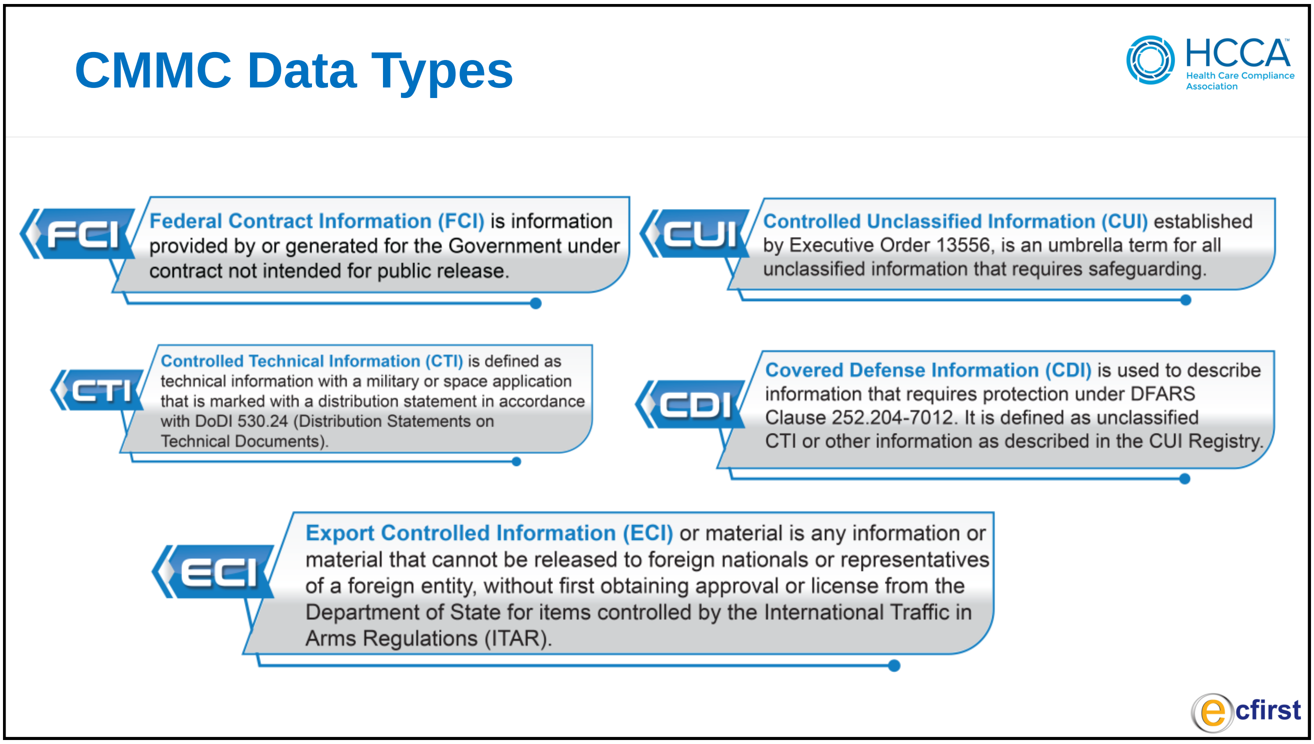
The Cybersecurity Maturity Model Certification (CMMC) program enhances cyber protection standards for companies in the DIB. It is designed to protect sensitive unclassified information that is shared by the Department with its contractors and subcontractors. The program incorporates a set of cybersecurity requirements into acquisition programs and provides the Department increased assurance that contractors and subcontractors are meeting these requirements.

OUSD (A&S)
Under Secretary of Defense for Acquisition and Sustainment

UARCs
University Affiliated Research Centers

FFRDCs
Federally Funded Research and Development Centers

ecfirst



CMMC Data Types

HCCA Health Care Compliance Association

FCI — **Federal Contract Information (FCI)** is information provided by or generated for the Government under contract not intended for public release.

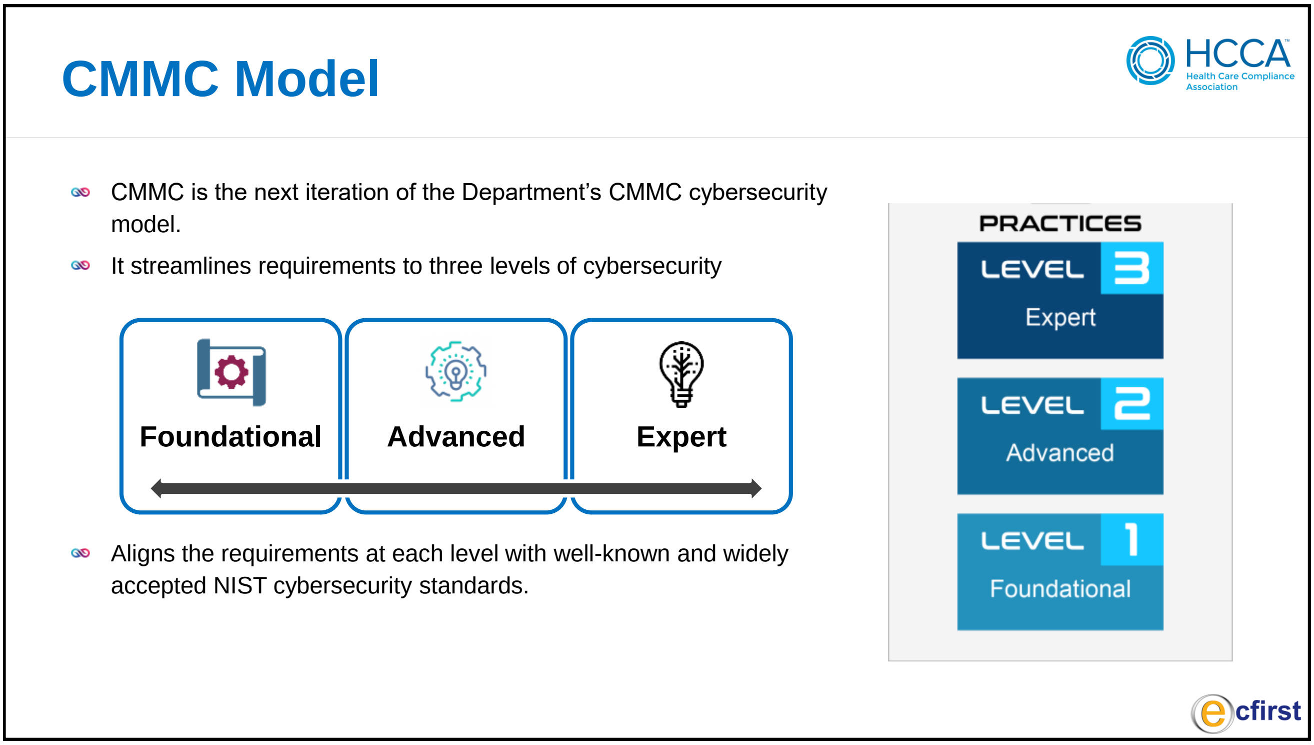
CUI — **Controlled Unclassified Information (CUI)** established by Executive Order 13556, is an umbrella term for all unclassified information that requires safeguarding.

CTI — **Controlled Technical Information (CTI)** is defined as technical information with a military or space application that is marked with a distribution statement in accordance with DoDI 530.24 (Distribution Statements on Technical Documents).

CDI — **Covered Defense Information (CDI)** is used to describe information that requires protection under DFARS Clause 252.204-7012. It is defined as unclassified CTI or other information as described in the CUI Registry.

ECI — **Export Controlled Information (ECI)** or material is any information or material that cannot be released to foreign nationals or representatives of a foreign entity, without first obtaining approval or license from the Department of State for items controlled by the International Traffic in Arms Regulations (ITAR).

ecfirst



CMMC Model

HCCA Health Care Compliance Association

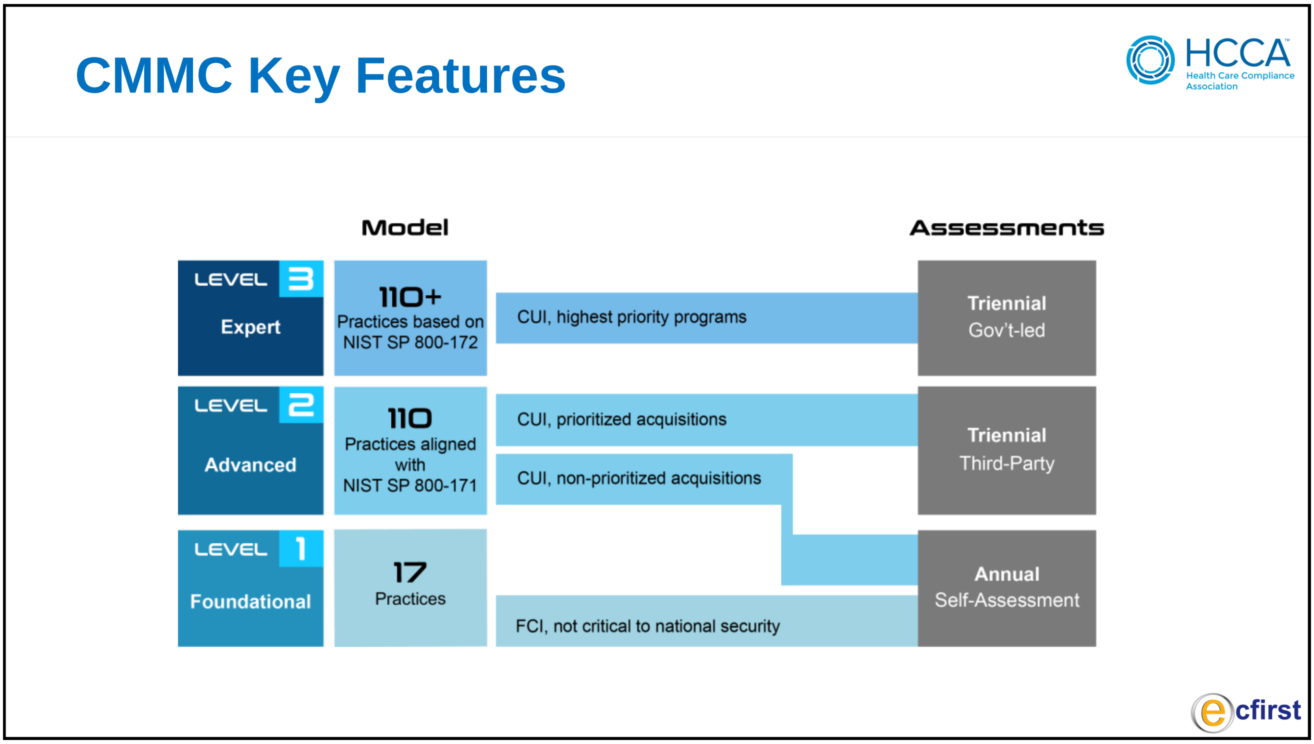
- CMMC is the next iteration of the Department's CMMC cybersecurity model.
- It streamlines requirements to three levels of cybersecurity

Foundational
Advanced
Expert

- Aligns the requirements at each level with well-known and widely accepted NIST cybersecurity standards.

PRACTICES
LEVEL 3
Expert
LEVEL 2
Advanced
LEVEL 1
Foundational

ecfirst

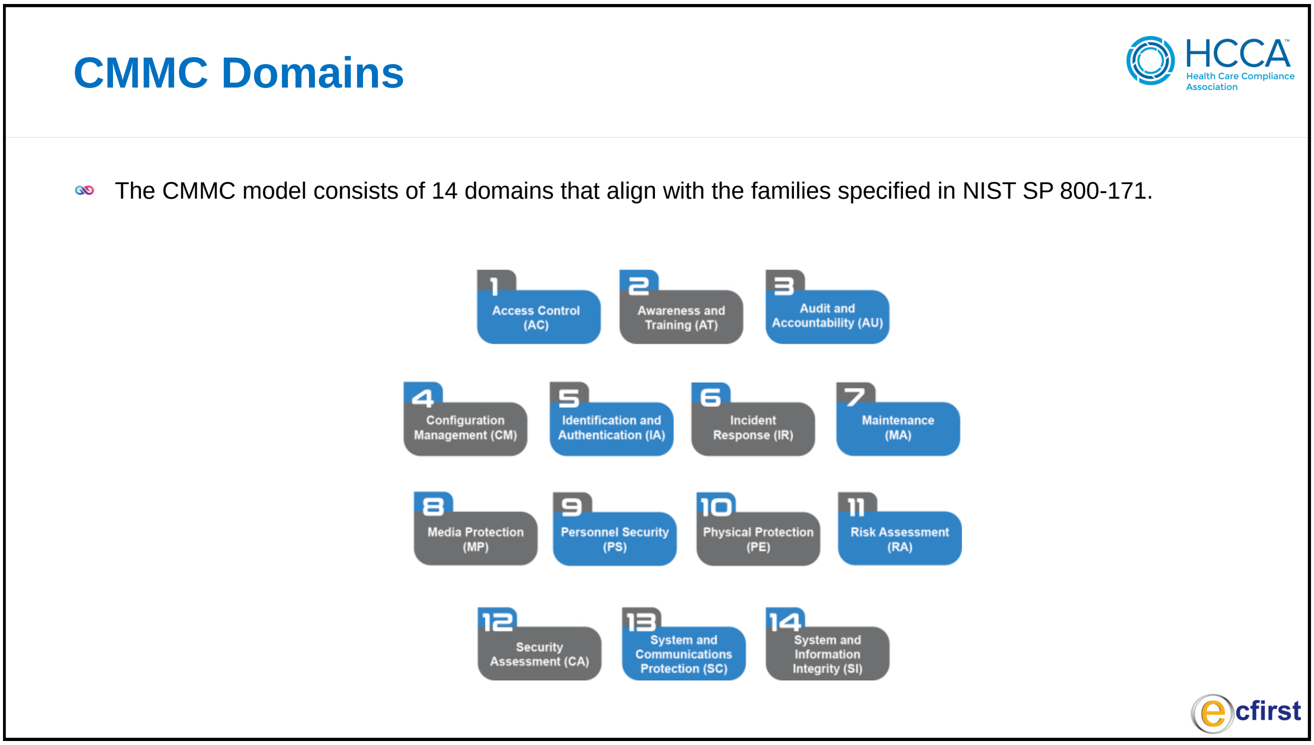


CMMC Key Features

HCCA Health Care Compliance Association

Model			Assessments
LEVEL 3 Expert	110+ Practices based on NIST SP 800-172	CUI, highest priority programs	Triennial Gov't-led
LEVEL 2 Advanced	110 Practices aligned with NIST SP 800-171	CUI, prioritized acquisitions	Triennial Third-Party
		CUI, non-prioritized acquisitions	Annual Self-Assessment
LEVEL 1 Foundational	17 Practices	FCI, not critical to national security	Annual Self-Assessment

ecfirst



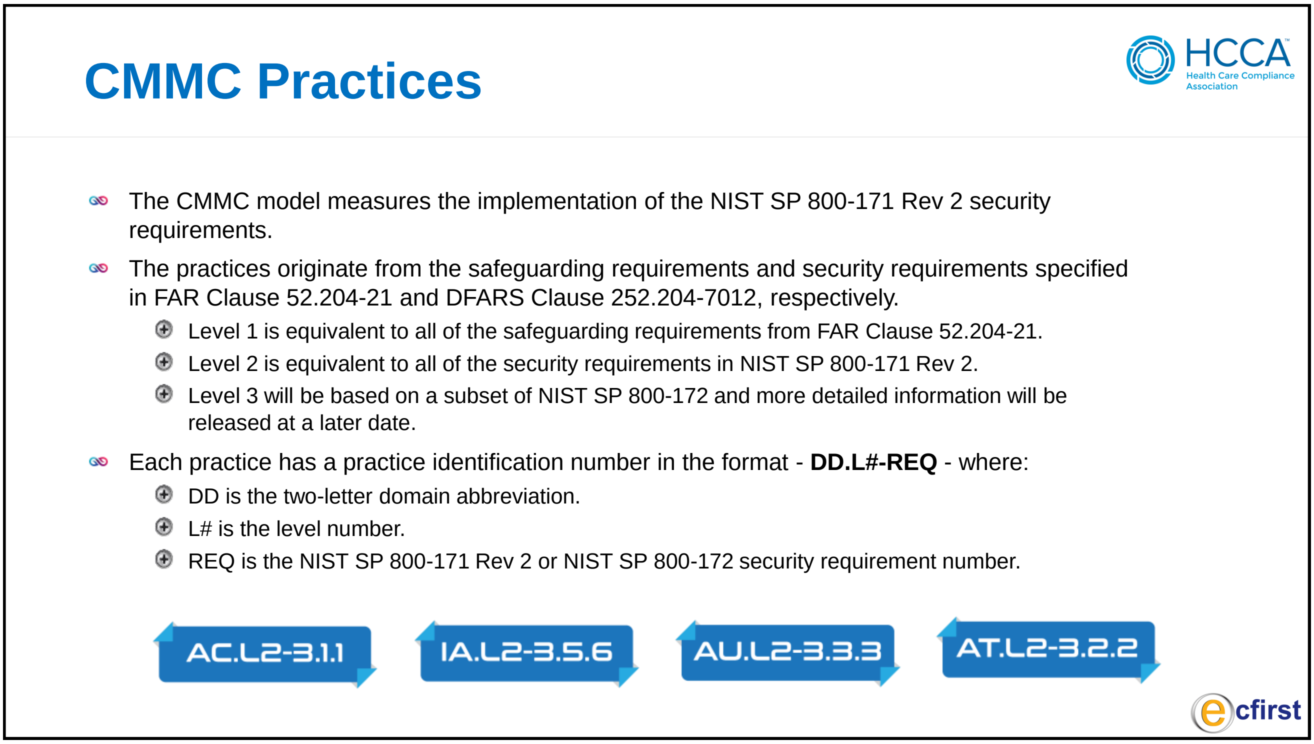
CMMC Domains

HCCA Health Care Compliance Association

- The CMMC model consists of 14 domains that align with the families specified in NIST SP 800-171.

1. Access Control (AC)
2. Awareness and Training (AT)
3. Audit and Accountability (AU)
4. Configuration Management (CM)
5. Identification and Authentication (IA)
6. Incident Response (IR)
7. Maintenance (MA)
8. Media Protection (MP)
9. Personnel Security (PS)
10. Physical Protection (PE)
11. Risk Assessment (RA)
12. Security Assessment (CA)
13. System and Communications Protection (SC)
14. System and Information Integrity (SI)

ecfirst



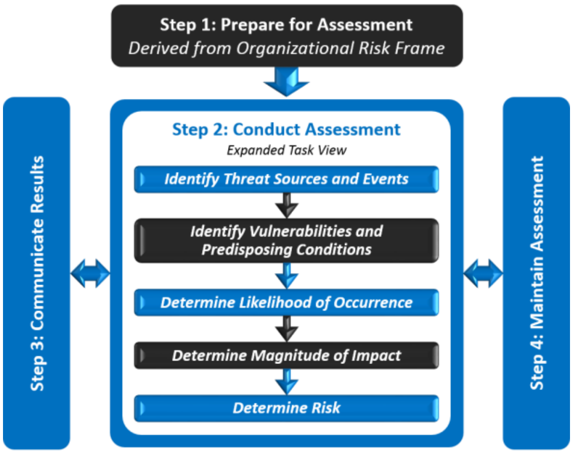
CMMC Practices

- The CMMC model measures the implementation of the NIST SP 800-171 Rev 2 security requirements.
- The practices originate from the safeguarding requirements and security requirements specified in FAR Clause 52.204-21 and DFARS Clause 252.204-7012, respectively.
  - Level 1 is equivalent to all of the safeguarding requirements from FAR Clause 52.204-21.
  - Level 2 is equivalent to all of the security requirements in NIST SP 800-171 Rev 2.
  - Level 3 will be based on a subset of NIST SP 800-172 and more detailed information will be released at a later date.
- Each practice has a practice identification number in the format - **DD.L#-REQ** - where:
  - DD is the two-letter domain abbreviation.
  - L# is the level number.
  - REQ is the NIST SP 800-171 Rev 2 or NIST SP 800-172 security requirement number.

AC.L2-3.1.1 IA.L2-3.5.6 AU.L2-3.3.3 AT.L2-3.2.2

Getting Started

Align Compliance with NIST Cybersecurity Framework



Step 1: Prepare for Assessment
Derived from Organizational Risk Frame

Step 2: Conduct Assessment
Expanded Task View

Identify Threat Sources and Events

Identify Vulnerabilities and Predisposing Conditions

Determine Likelihood of Occurrence

Determine Magnitude of Impact

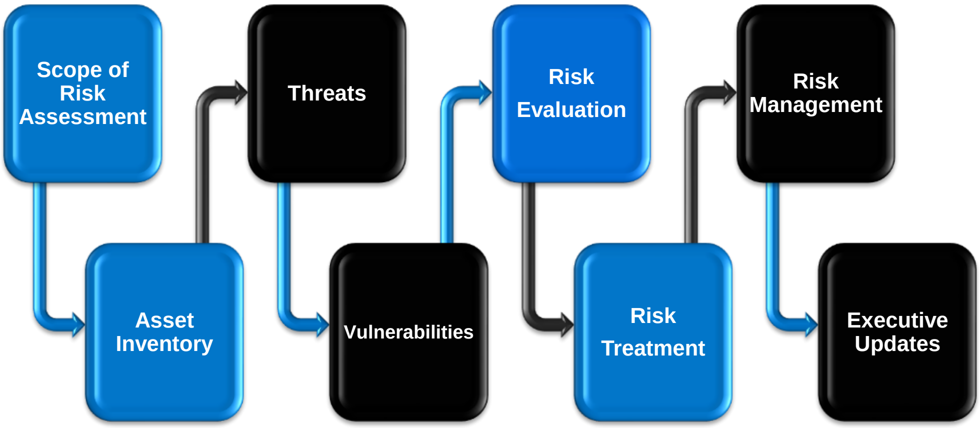
Determine Risk

Step 3: Communicate Results

Step 4: Maintain Assessment

Enterprise Risk Assessment

NIST Cybersecurity Framework Credible Reference for Risk Assessment



Scope of Risk Assessment

Asset Inventory

Threats

Vulnerabilities

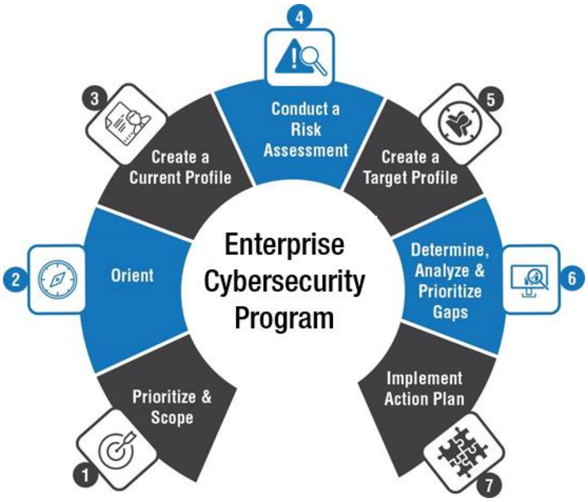
Risk Evaluation

Risk Treatment

Risk Management

Executive Updates

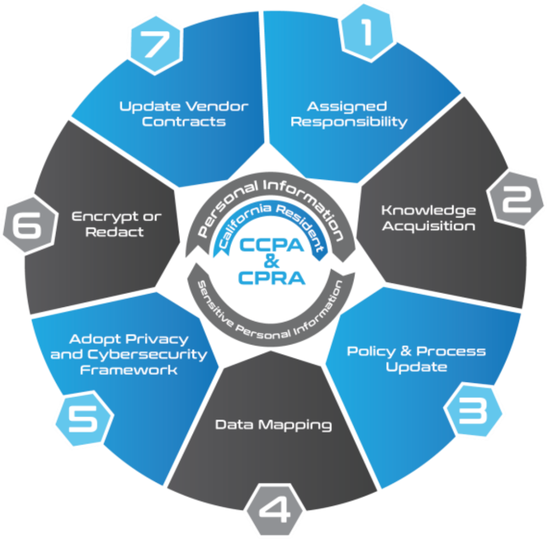
NIST Enterprise Cybersecurity Program



California Privacy Rights Act (CPRA) Facts

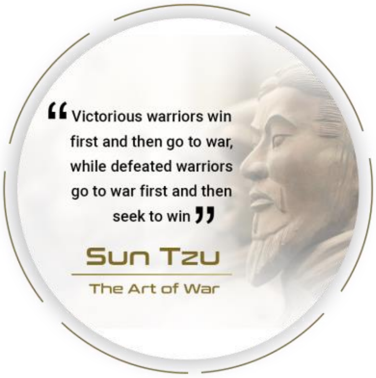
- CPRA, also referred to as CCPA v2.
- CPRA provides additional **rights to consumers** and places additional obligations on businesses introduces a new data category, **sensitive personal information**.
- CPRA requires businesses to provide additional mechanisms for individuals to access, correct, or delete data.

Jan 1, 2023 | CPRA



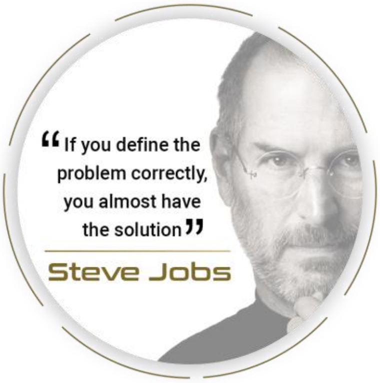
Reimagine Compliance.
Reimagine Cybersecurity!

HCCA
Health Care Compliance Association



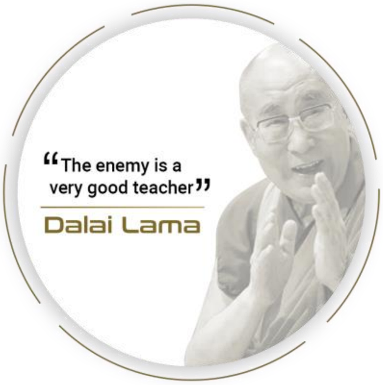
“Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win”

Sun Tzu
The Art of War



“If you define the problem correctly, you almost have the solution”

Steve Jobs



“The enemy is a very good teacher”

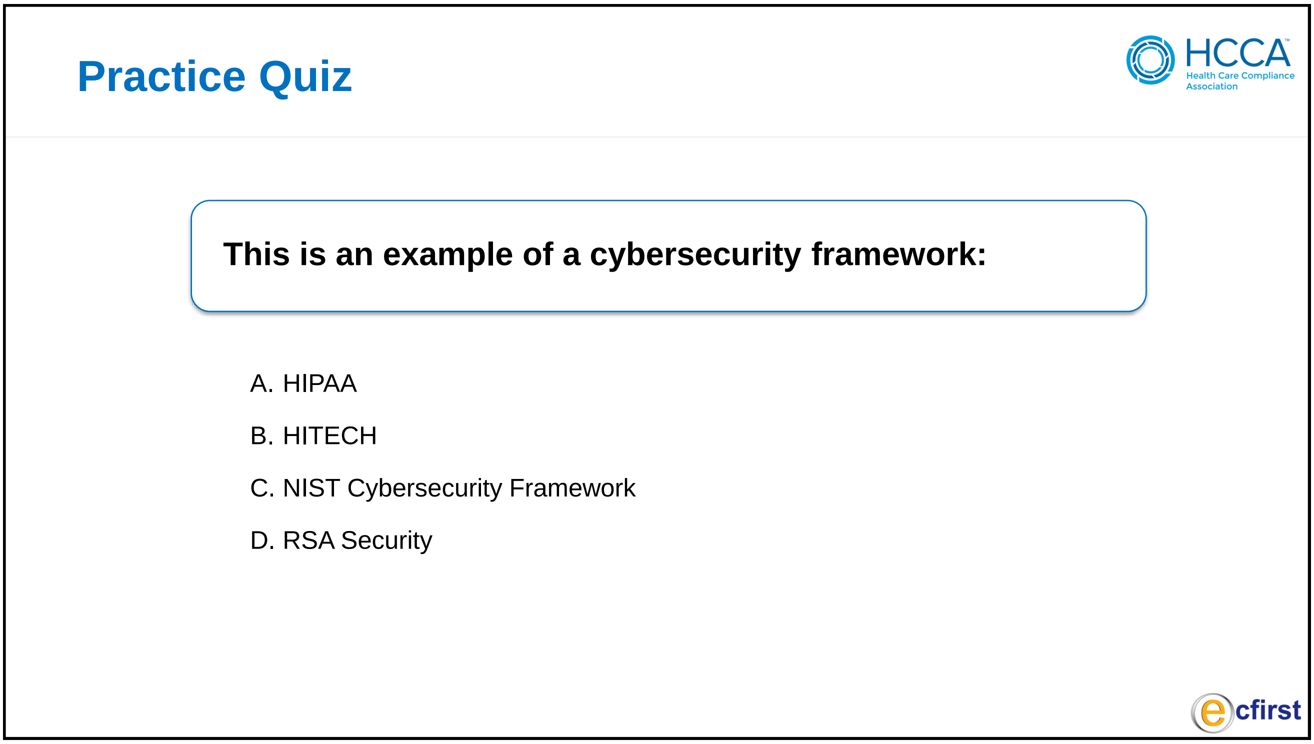
Dalai Lama

ecfirst

HCCA
Health Care Compliance Association

Quiz

ecfirst



Practice Quiz

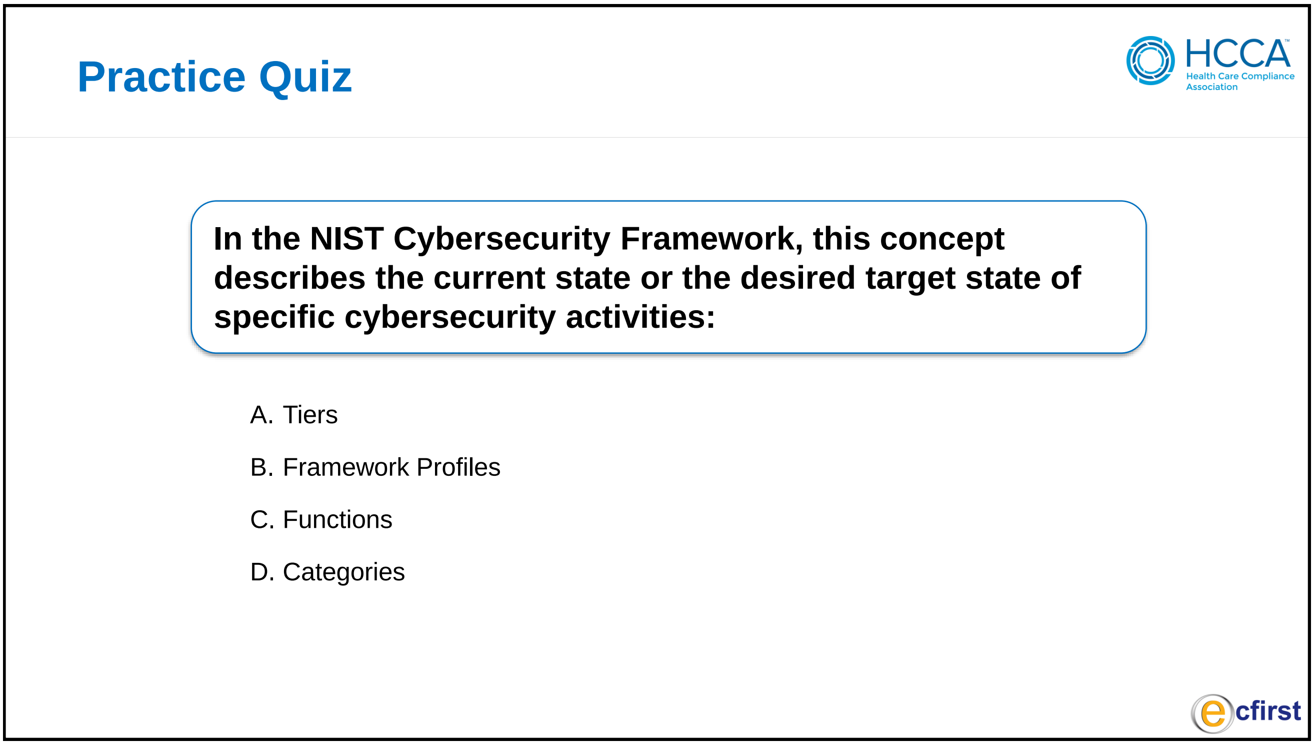
This is an example of a cybersecurity framework:

A. HIPAA

B. HITECH

C. NIST Cybersecurity Framework

D. RSA Security



Practice Quiz

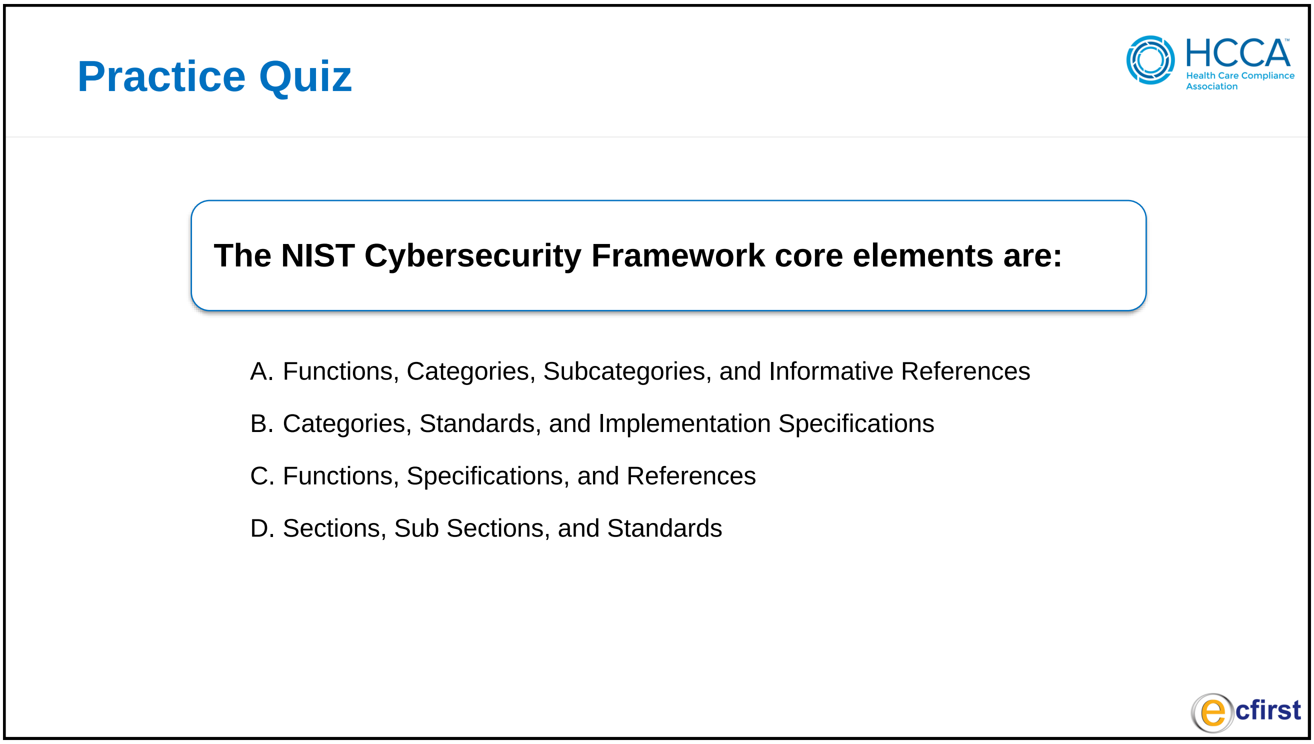
In the NIST Cybersecurity Framework, this concept describes the current state or the desired target state of specific cybersecurity activities:

A. Tiers

B. Framework Profiles

C. Functions

D. Categories



Practice Quiz

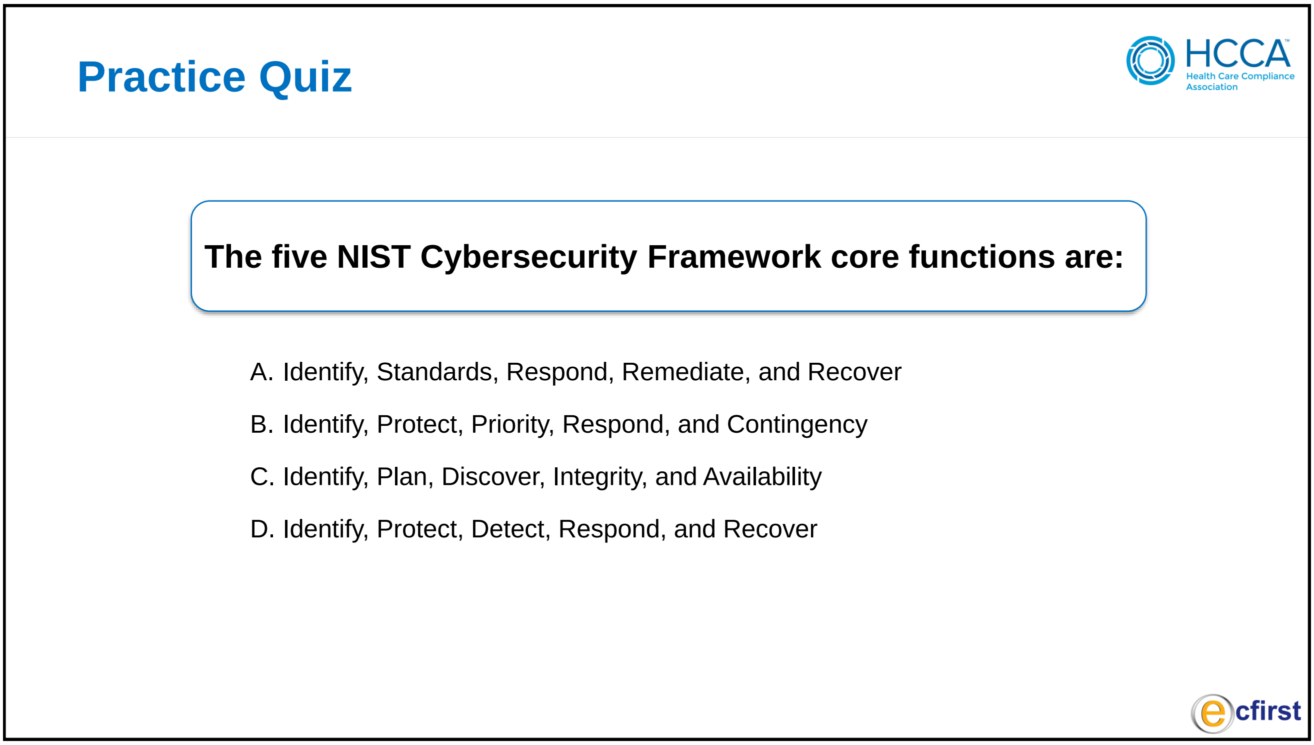
The NIST Cybersecurity Framework core elements are:

A. Functions, Categories, Subcategories, and Informative References

B. Categories, Standards, and Implementation Specifications

C. Functions, Specifications, and References

D. Sections, Sub Sections, and Standards



Practice Quiz

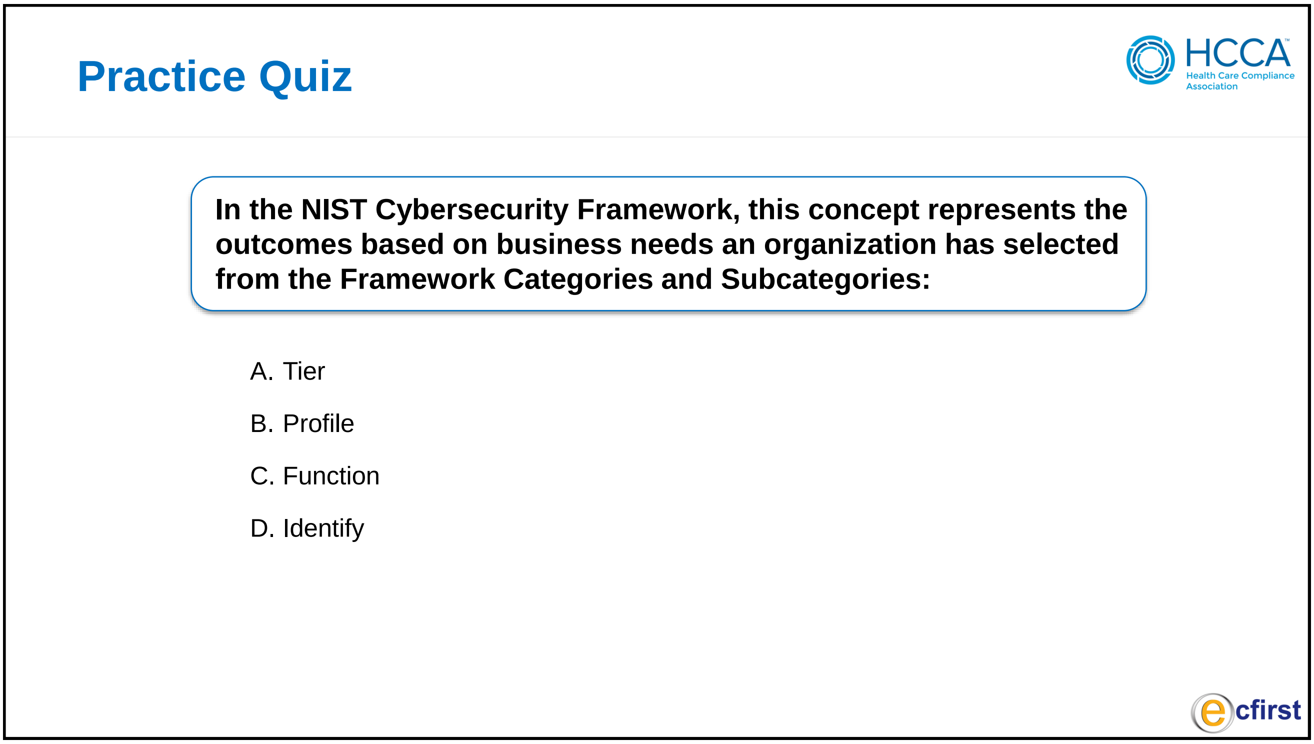
The five NIST Cybersecurity Framework core functions are:

A. Identify, Standards, Respond, Remediate, and Recover

B. Identify, Protect, Priority, Respond, and Contingency

C. Identify, Plan, Discover, Integrity, and Availability

D. Identify, Protect, Detect, Respond, and Recover



Practice Quiz

HCCA Health Care Compliance Association

In the NIST Cybersecurity Framework, this concept represents the outcomes based on business needs an organization has selected from the Framework Categories and Subcategories:

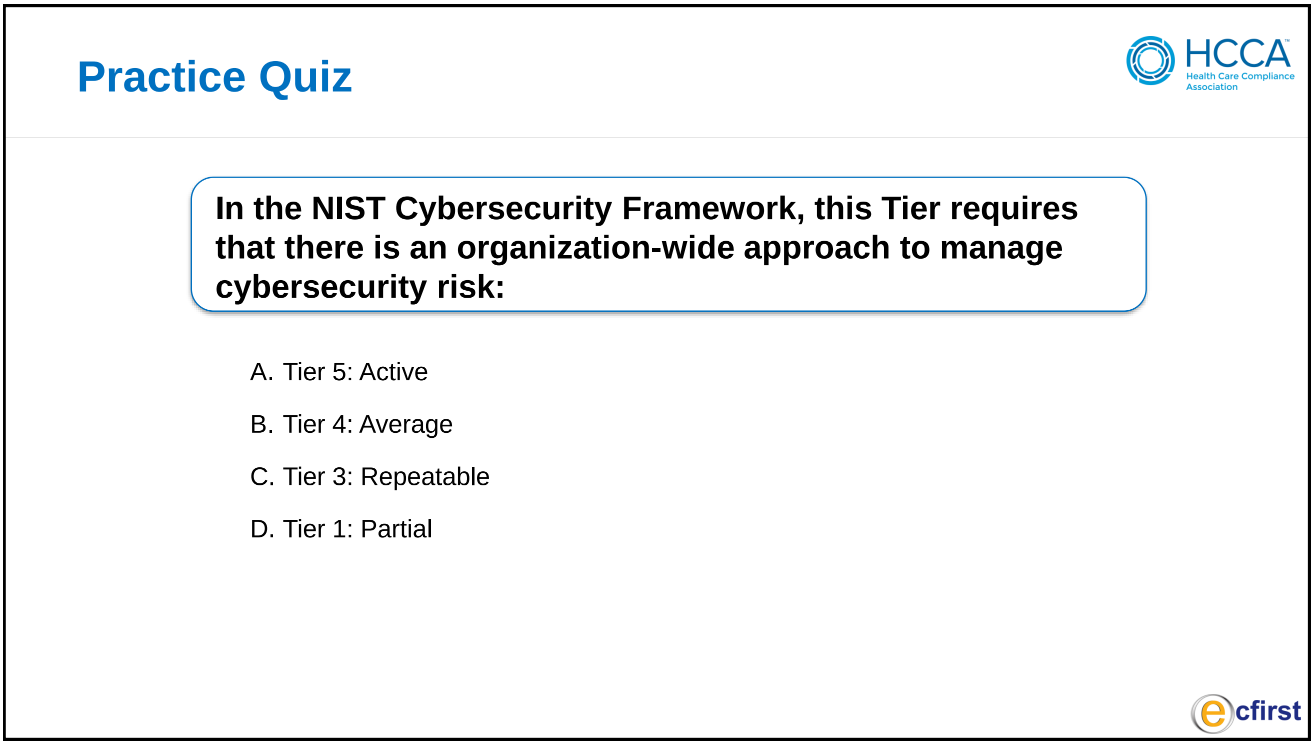
A. Tier

B. Profile

C. Function

D. Identify

ecfirst



Practice Quiz

HCCA Health Care Compliance Association

In the NIST Cybersecurity Framework, this Tier requires that there is an organization-wide approach to manage cybersecurity risk:

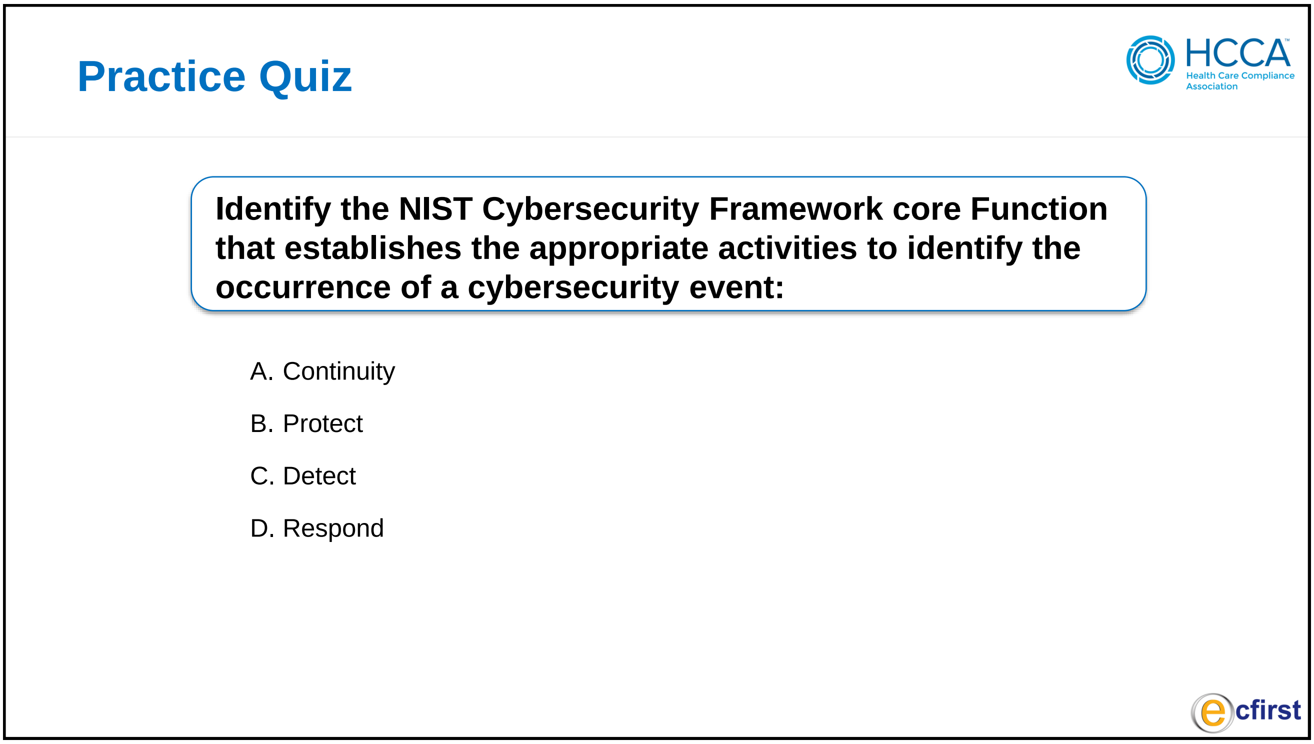
A. Tier 5: Active

B. Tier 4: Average

C. Tier 3: Repeatable

D. Tier 1: Partial

ecfirst



Practice Quiz

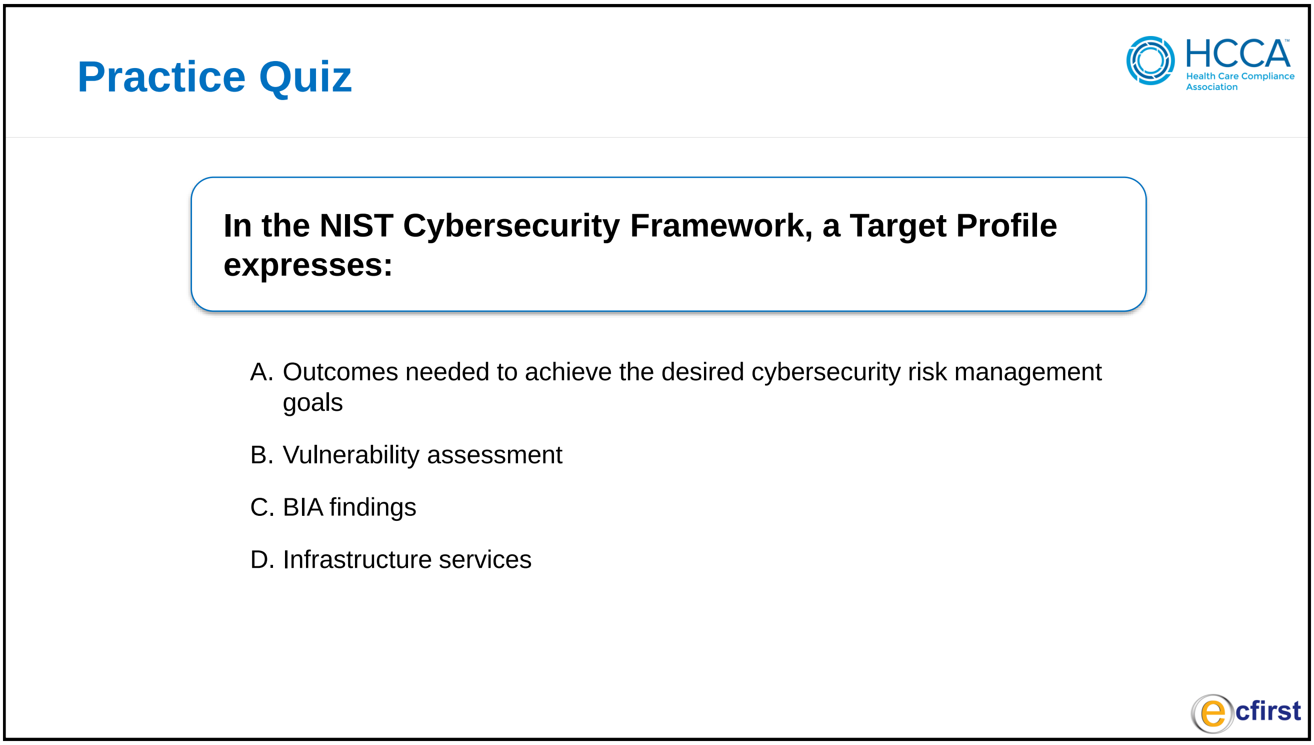
Identify the NIST Cybersecurity Framework core Function that establishes the appropriate activities to identify the occurrence of a cybersecurity event:

A. Continuity

B. Protect

C. Detect

D. Respond



Practice Quiz

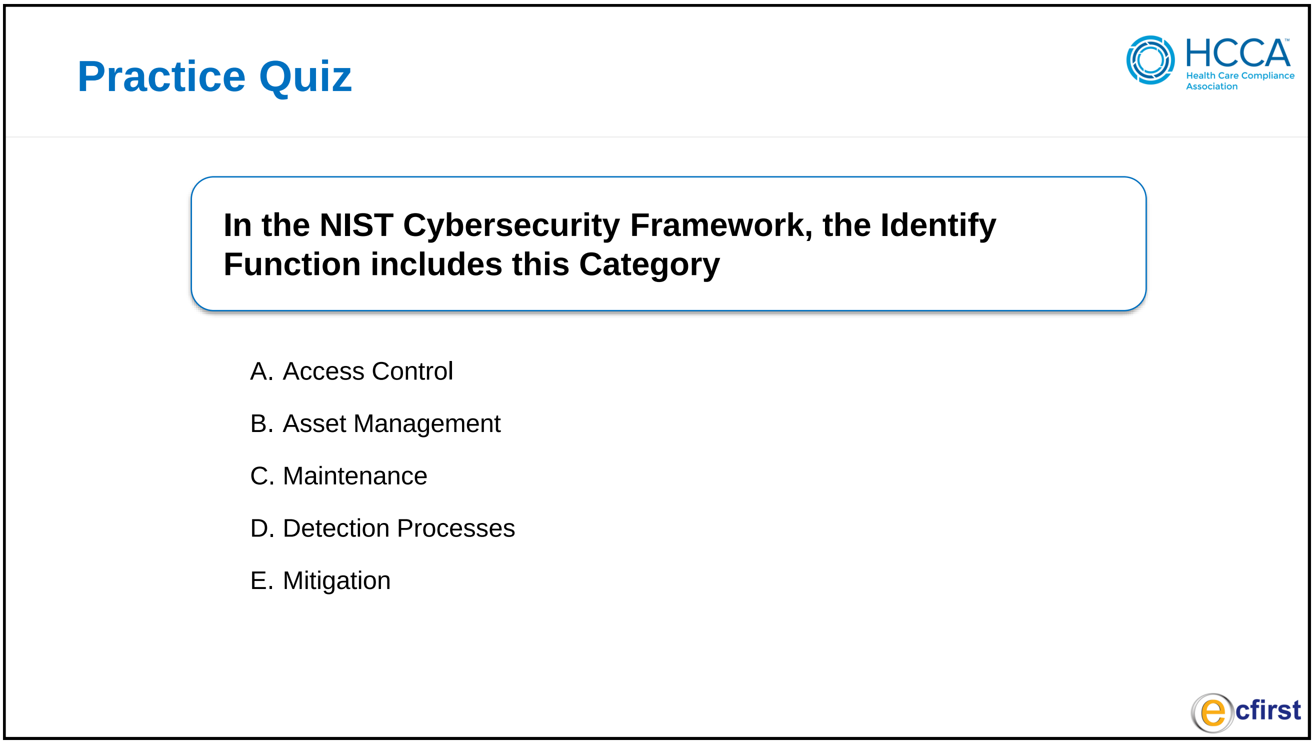
In the NIST Cybersecurity Framework, a Target Profile expresses:

A. Outcomes needed to achieve the desired cybersecurity risk management goals

B. Vulnerability assessment

C. BIA findings

D. Infrastructure services



Practice Quiz

In the NIST Cybersecurity Framework, the Identify Function includes this Category

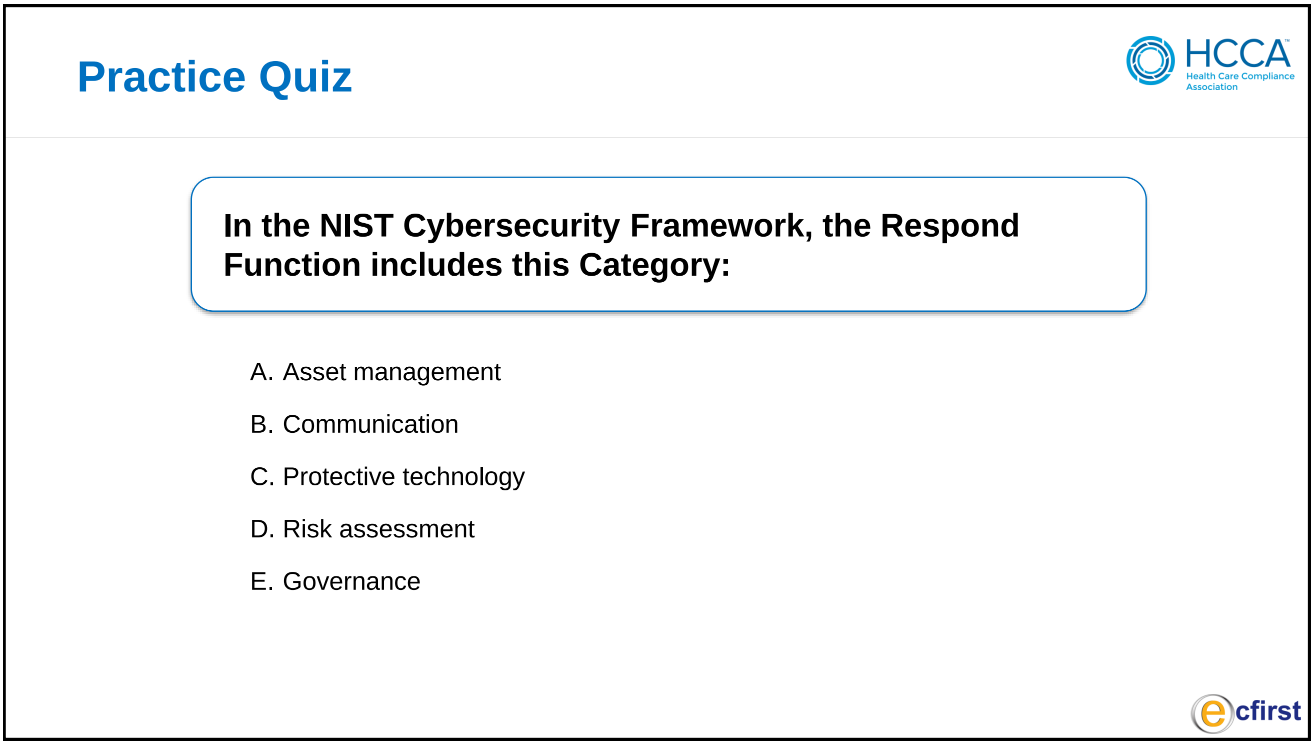
A. Access Control

B. Asset Management

C. Maintenance

D. Detection Processes

E. Mitigation



Practice Quiz

In the NIST Cybersecurity Framework, the Respond Function includes this Category:

A. Asset management

B. Communication

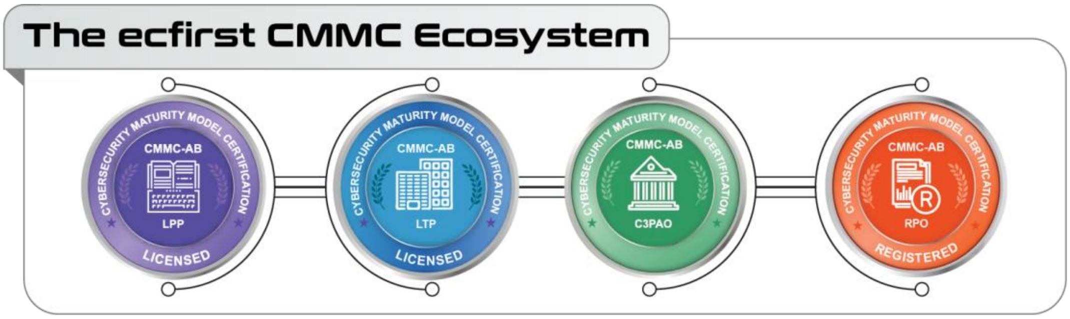
C. Protective technology

D. Risk assessment

E. Governance

CMMC Ecosystem

HCCA Health Care Compliance Association


The ecfirst CMMC Ecosystem
CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
LPP
LICENSED
CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
LTP
LICENSED
CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
C3PAO
CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
RPO
REGISTERED

ecfirst

HCCA™
Health Care Compliance Association

Thank You!

Ali Pabrai | Ali.Pabrai@ecfirst.com

ecfirst | HITRUST®
Authorized External Assessor