March 4, 2020

The 29th National HIPAA Summit

HITRUST CSF®: A Credible Standard for Ensuring HIPAA Compliance

ecfirst | HITRUST®
Authorized External Assessor

ISACA TOP-RATED SPEAKER ★★★★★

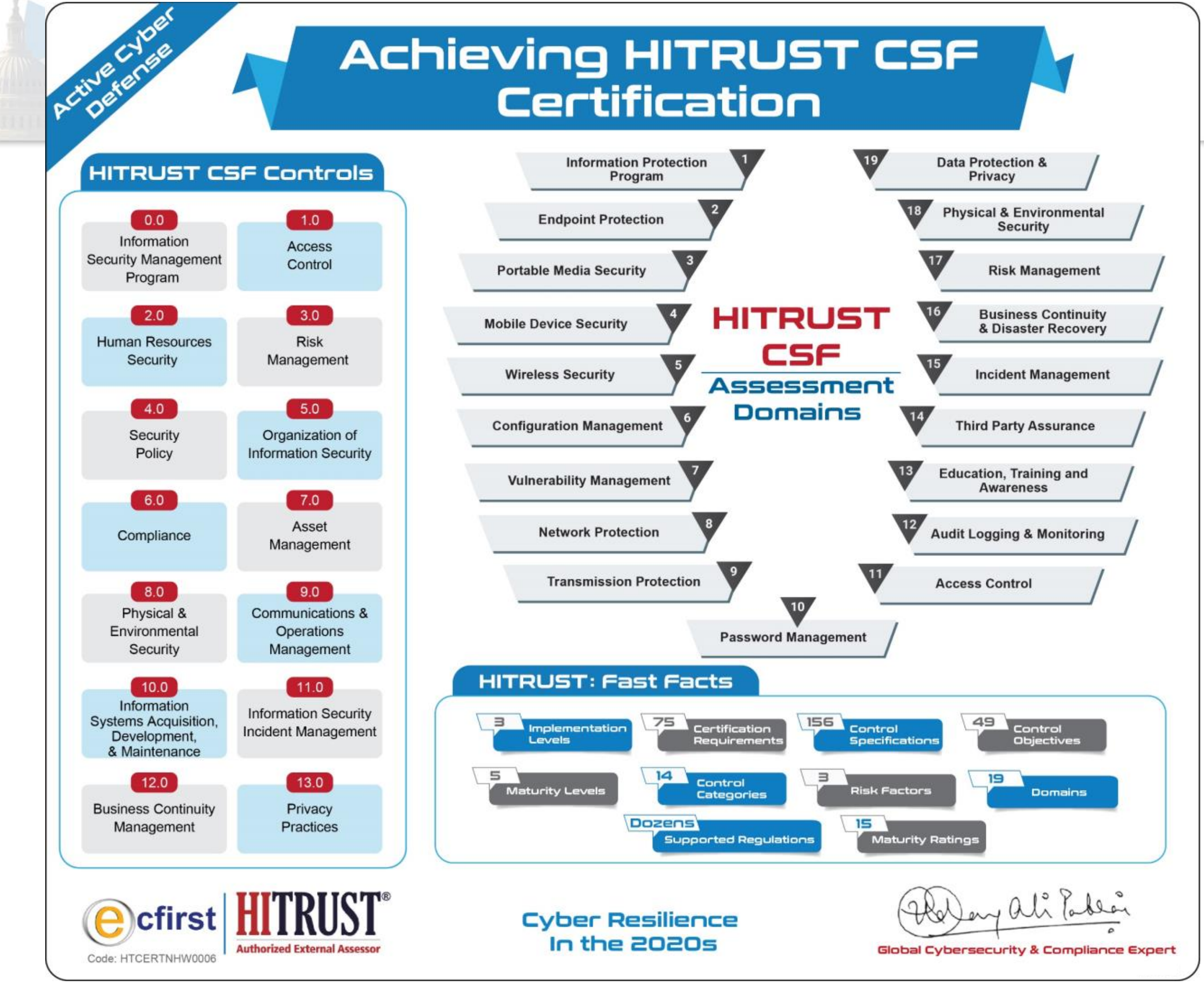
Ali Pabrai
Global Cybersecurity & Compliance Expert

Agenda

- HITRUST CSF 101: Fast Facts
- HITRUST CSF & HIPAA
- HITRUST CSF & NIST
- HITRUST CSF v9.3
- Achieving HITRUST CSF Certification

HITRUST CSF 101 Fast Facts

The 29th National HIPAA Summit



Active Cyber Defense

Achieving HITRUST CSF Certification

HITRUST CSF Controls

0.0	Information Security Management Program
1.0	Access Control
2.0	Human Resources Security
3.0	Risk Management
4.0	Security Policy
5.0	Organization of Information Security
6.0	Compliance
7.0	Asset Management
8.0	Physical & Environmental Security
9.0	Communications & Operations Management
10.0	Information Systems Acquisition, Development, & Maintenance
11.0	Information Security Incident Management
12.0	Business Continuity Management
13.0	Privacy Practices

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

HITRUST: Fast Facts

3	Implementation Levels
75	Certification Requirements
156	Control Specifications
49	Control Objectives
5	Maturity Levels
14	Control Categories
3	Risk Factors
19	Domains
Dozens	Supported Regulations
15	Maturity Ratings

ecfirst HITRUST® Authorized External Assessor

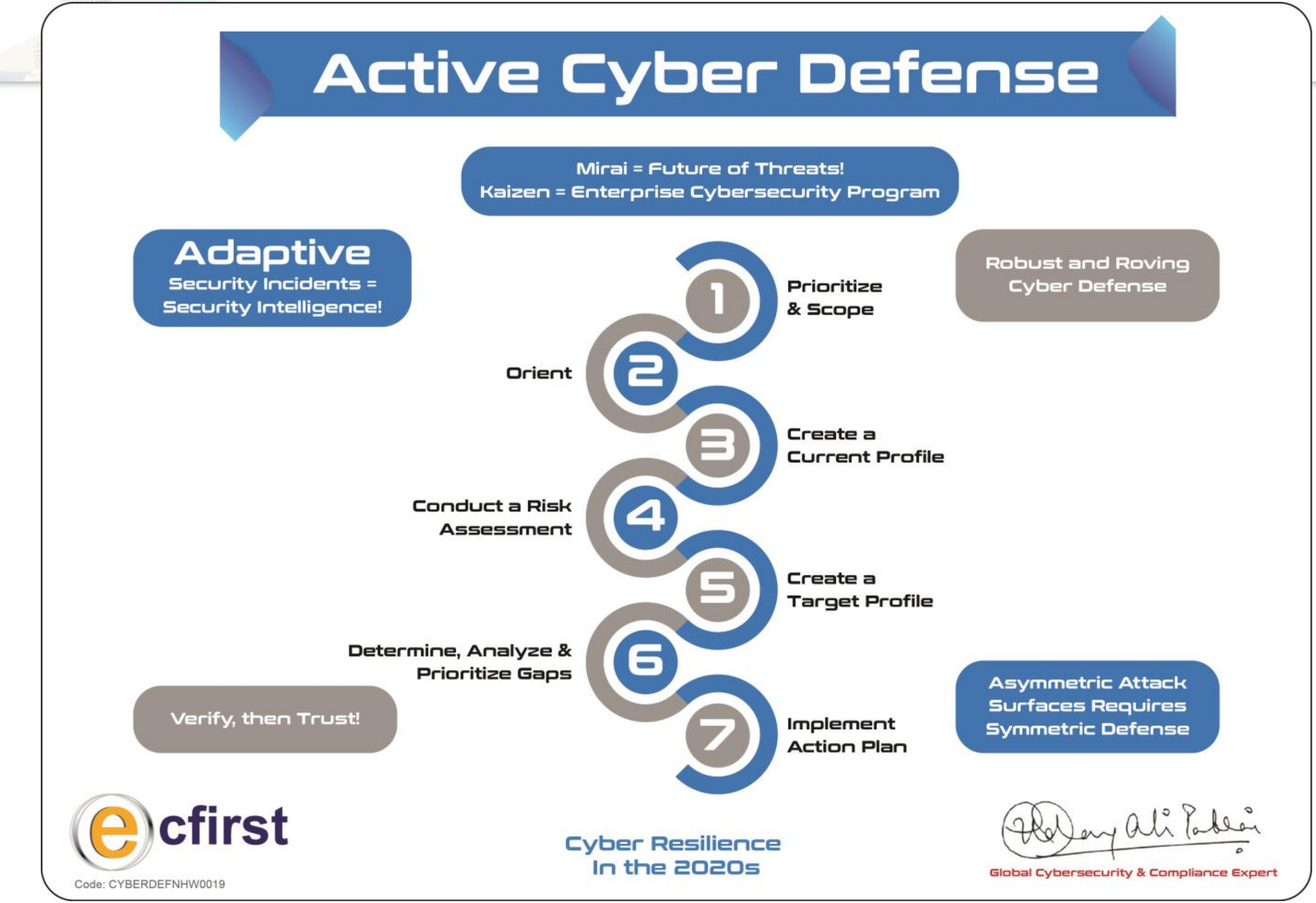
Code: HTCERTNHW0006

Cyber Resilience In the 2020s

Uday Ali Pabrai

Global Cybersecurity & Compliance Expert

ecfirst HITRUST® Authorized External Assessor



Active Cyber Defense

Mirai = Future of Threats!
Kaizen = Enterprise Cybersecurity Program

Adaptive
Security Incidents = Security Intelligence!

Robust and Roving Cyber Defense

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

Verify, then Trust!

Asymmetric Attack Surfaces Requires Symmetric Defense

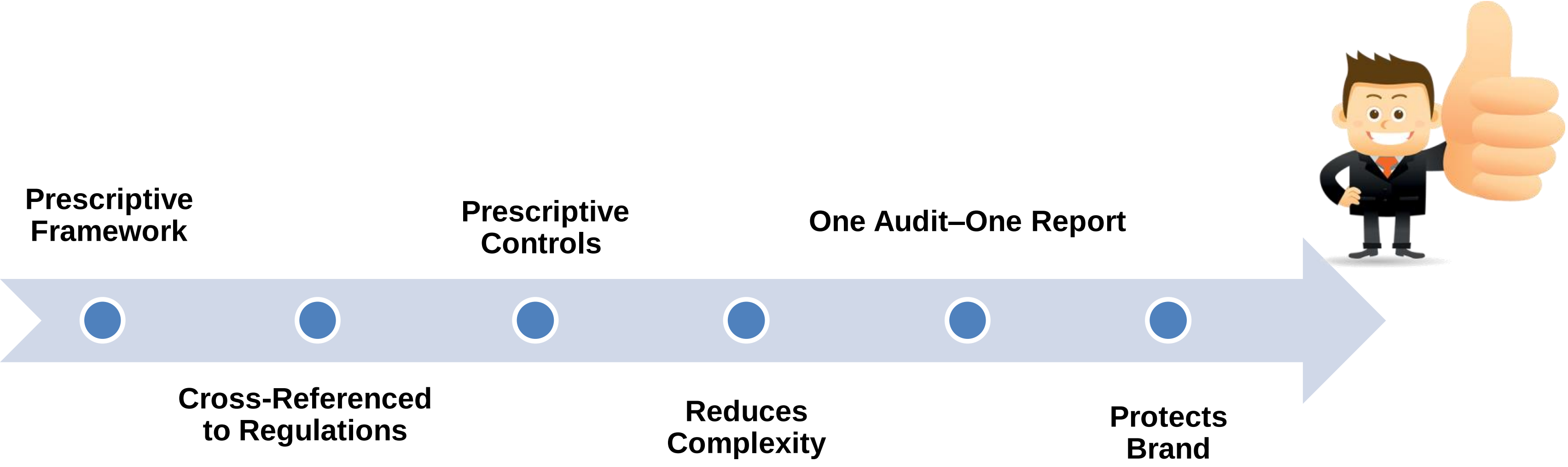
ecfirst

Code: CYBERDEFNHW0019

Cyber Resilience In the 2020s

Uday Ali Pabrai
Global Cybersecurity & Compliance Expert

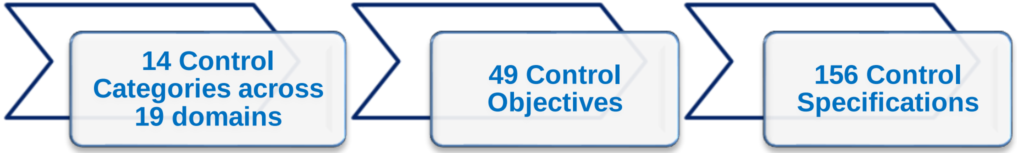
Why HITRUST Certification?



HITRUST: Framework of Frameworks

Organization of the HITRUST CSF

- Built on ISO 27001
- HITRUST CSF organization



14 Control Categories across 19 domains

49 Control Objectives

156 Control Specifications

- Integrates other standards

HIPAA

MARS-E Requirements

FISMA Compliance

FTC Red Flag Rules

PCI Compliance

23 NYCRR 500

CIS Critical Security Controls v6

EU GDPR

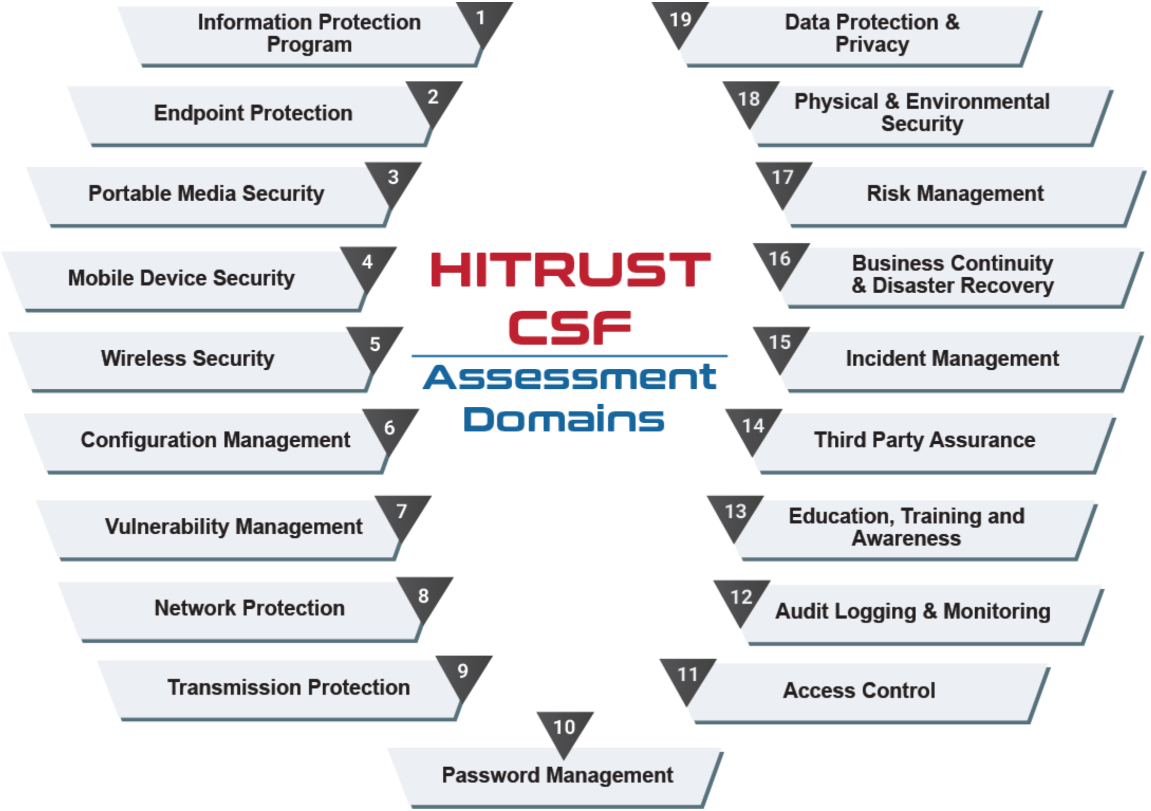
PDPA

And more…

HITRUST CSF Control Categories

	CSF Control Category	Control Specifications	Required For HITRUST CSF Certification
0	Information Security Management Program	1	1
1	Access Control	25	16
2	Human Resources Security	9	5
3	Risk Management	4	3
4	Security Policy	2	2
5	Organization of Information Security	11	5
6	Compliance	10	5
7	Asset Management	5	2
8	Physical & Environmental Security	13	4
9	Communications & Operations Management	32	19
10	Information Systems Acquisition, Development & Maintenance	13	7
11	Information Security Incident Management	5	3
12	Business Continuity Management	5	3
13	Privacy Practices	21	
		156	75

HITRUST CSF Domains



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

HITRUST Authoritative Sources

1. 16 CFR Part 681
2. 201 CMR 17.00
3. AICPA TSP 100
4. APEC
5. CCPA
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. DHS CRR v1.1
13. EHNAC
14. 21 CFR Part 11
15. EU GDPR
16. OCR Guidance for Unsecured PHI
17. FFIEC IS
18. FedRAMP
19. HITRUST De-ID Framework v1
20. 45 CFR Part 164, HIPAA General Provisions
21. 45 CFR Part 164, HIPAA Security Rule
22. 45 CFR Part 164, HIPAA Breach Notification Rule

HITRUST Authoritative Sources

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 800-122

36 NIST SP 800-171 R2 (DFARS)

37 NRS 603A

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

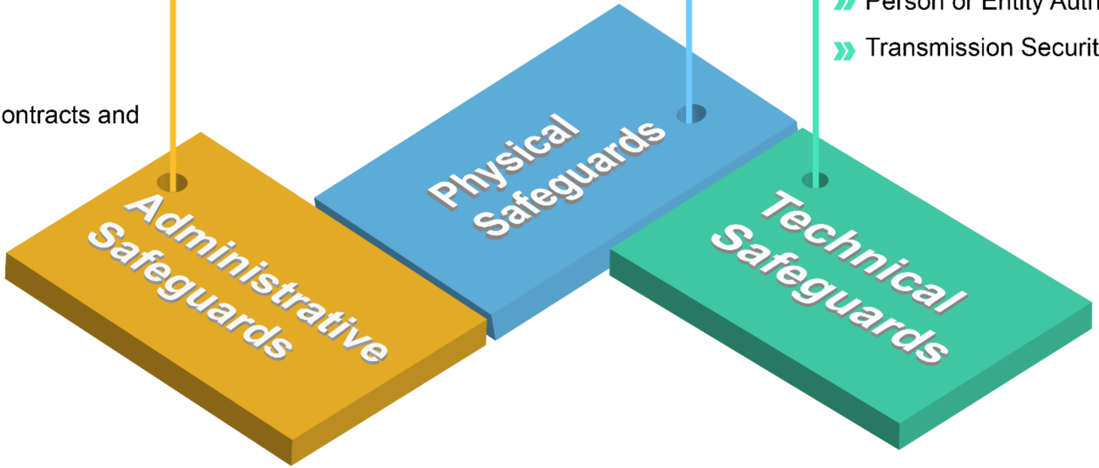
HITRUST CSF & HIPAA

HIPAA Privacy, HIPAA Security & HITECH Breach

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media
- Controls

- Access Control
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security



HIPAA Privacy Rule to HITRUST CSF v9.3 Mapping

#	HIPAA Privacy Rule	HITRUST CSF v9.3
1.	**§164.502(a)** Uses and Disclosures – General Rules STD	13.f Principal Access 13.k Use and Disclosure
2.	**§164.502(a)(2)** Covered entities: Required disclosures STD	13.k Use and Disclosure
3.	**§164.502(a)(4)** Business associates: Permitted uses and disclosures STD	13.k Use and Disclosure
4.	**§164.502(a)(4)** Business associates: Required uses and disclosures	13.k Use and Disclosure
5.	**§164.502(a)(5)** Prohibited uses and disclosures	13.j Data Minimization 13.k Use and Disclosure
6.	**§164.502(f)** Deceased Individuals STD	06.c Protection of Organizational Records
7.	**§164.502(g)**	13.e Choice
8.	**§164.502(j)(1)** Disclosures by whistleblowers	13.k Use and Disclosure
9.	**§164.502(j)(2)** Disclosures by workforce members who are victims of a crime	13.k Use and Disclosure

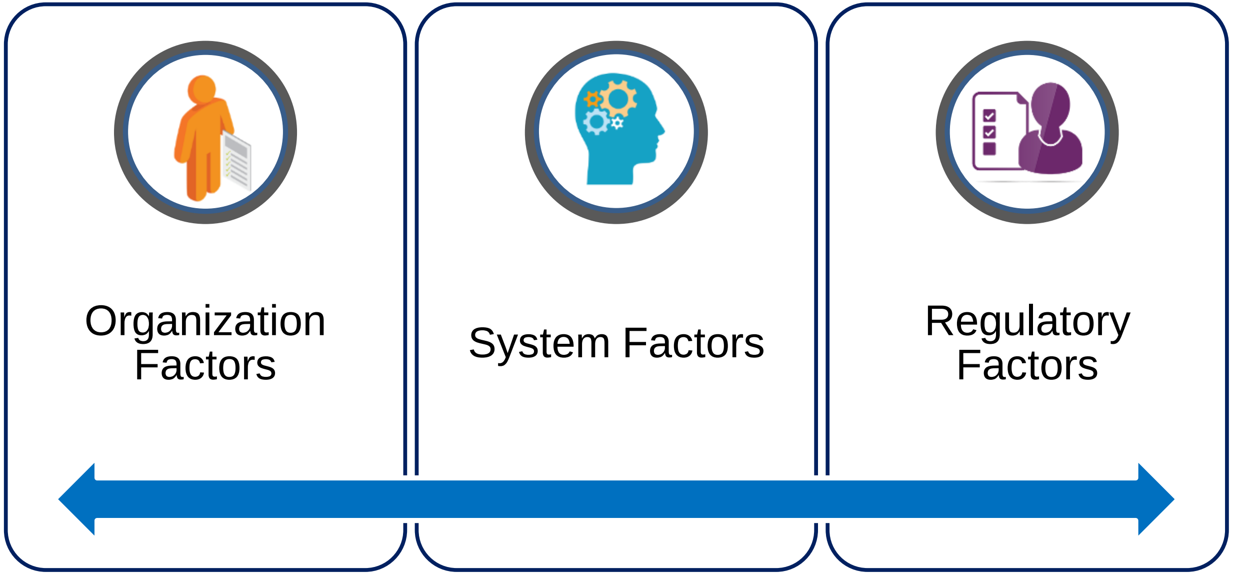
HIPAA Security Rule to HITRUST CSF v9.3 Mapping

#	HIPAA Security Rule	HITRUST CSF v9.3
Administrative Safeguards		
1.	**§164.308(a)(1)(i)** Security Management Process	00.a Information Security Management Program
		02.a Roles and Responsibilities
		03.a Risk Management Program Development
		05.a Management Commitment to Information Security
		05.h Independent Review of Information Security
		09.t Exchange Agreements
2.	**164.308(a)(2)** Assigned Security Responsibility	03.b Performing Risk Assessments
		05.a Management Commitment to Information Security
		05.c Allocation of Information Security Responsibilities
		05.d Authorization Process for Information Assets and Facilities
		06.g Compliance with Security Policies and Standards

HIPAA Breach Notification Rule to HITRUST CSF v9.3 Mapping

#	HIPAA Breach Notification Rule	HITRUST CSF v9.3
1.	**§164.402**	03.b Performing Risk Assessments
2.	**§164.404(a)(1)** General rule STD	11.a Reporting Information Security Events
		11.c Responsibilities and Procedures
3.	**§164.404(a)(2)** Breaches treated as discovered STD	11.a Reporting Information Security Events
4.	**§164.404(b)** Implementation specification: Timeliness of notification SPEC	05.k Addressing Security in Third Party Agreements
		11.a Reporting Information Security Events
5.	**§164.404(c)(1)** Elements SPEC	11.a Reporting Information Security Events
6.	**§164.404(c)(2)** Plain language requirement SPEC	11.a Reporting Information Security Events
7.	**§164.404(c)(3)**	11.a Reporting Information Security Events
8.	**§164.404(d)(1)** Written notice SPEC	11.a Reporting Information Security Events
9.	**§164.404(d)(2)** Substitute notice SPEC	11.a Reporting Information Security Events
10.	**§164.404(d)(3)** Additional notice in urgent situations SPEC	11.a Reporting Information Security Events

HITRUST Assessment: Risk Factors



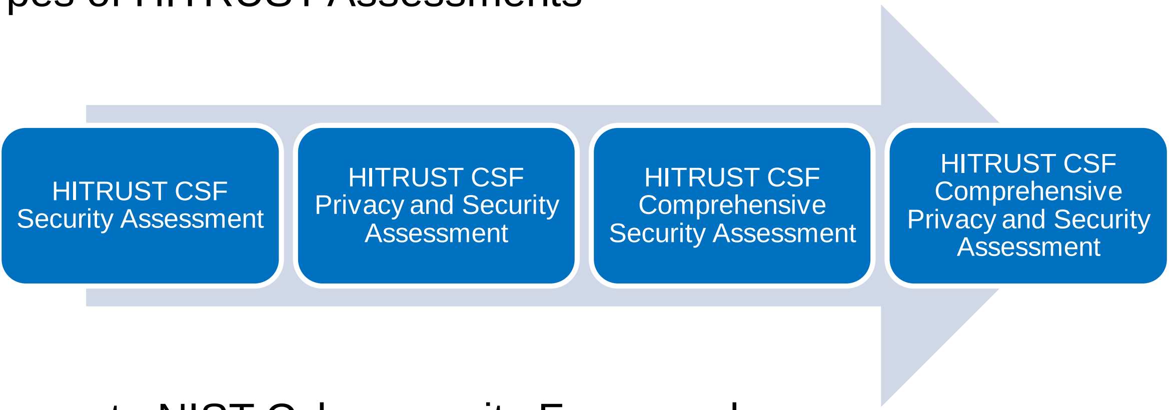
Organization Factors

System Factors

Regulatory Factors

Scoping Options

- Four types of HITRUST Assessments



HITRUST CSF Security Assessment

HITRUST CSF Privacy and Security Assessment

HITRUST CSF Comprehensive Security Assessment

HITRUST CSF Comprehensive Privacy and Security Assessment

- All incorporate NIST Cybersecurity Framework
  - NIST Cybersecurity Framework Certification with HITRUST CSF Certification
- Determined as part of scoping process

HITRUST: A Prescriptive Standard

1.0 Access Control

Automatically remove or disable accounts that have been inactive for a period of *sixty (60) days* or more. (01.b) (Level 1)

03.0 Risk Management

Repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a *minimum annually*. (03.a) (Level 1)

07.0 Asset Management

Records of property assigned to employees shall be reviewed and updated *annually*. (07.a) (Level 1)

11.0 Information Security Incident Management

The incident management plan is reviewed and updated annually (11.c) (Level 2)

09.0 Communications and Operations Management

The firewall and router rule sets shall be reviewed at least every six (6) months. (09.m) (Level 3).

Perform quarterly scans for unauthorized wireless access points and take appropriate action if any access points are discovered. (09.m) (Level 2)

12.01 Information Security Aspects of Business Continuity Management

Responsibilities are assigned for regular reviews of at least a part of the business continuity plan, at a minimum, *annually*. (12.e) (Level 1)

Implementation Guidance

Baseline ID: 0707.10b2System.1

Requirement Statement

Applications that store, process or transmit covered information undergo automated application **vulnerability testing** by a qualified party on an annual basis.

Policy

Review policies related to input validation in applications.

Process

Determine if the procedures address all the required elements of the policy.

Implementation

Examine the most recent application vulnerability test and determine if it was performed within the past twelve (12) months by a qualified party.

Measured

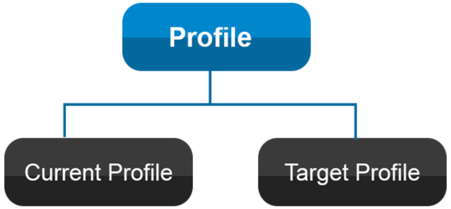
Measure the effectiveness of the implemented controls and to vulnerability testing by a qualified party on an annual basis.

Managed

Determine if ad hoc processes for investigation and resolution exist and if deviations occurred and were corrected.

HITRUST CSF & NIST

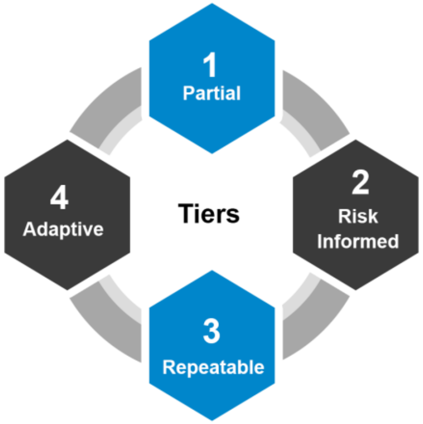
NIST Cybersecurity Framework



Profile

Current Profile

Target Profile



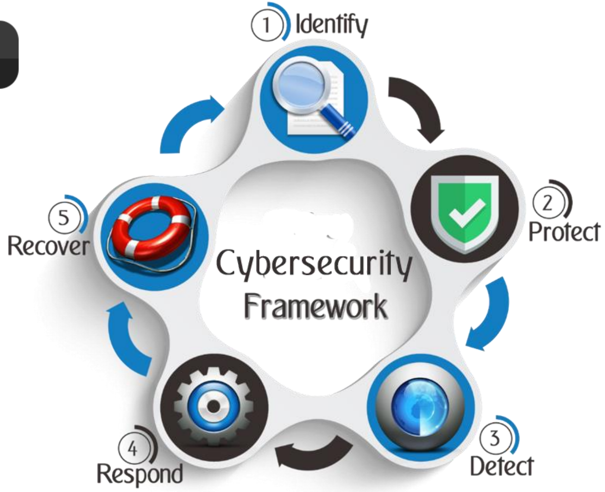
Tiers

1 Partial

2 Risk Informed

3 Repeatable

4 Adaptive



Cybersecurity Framework

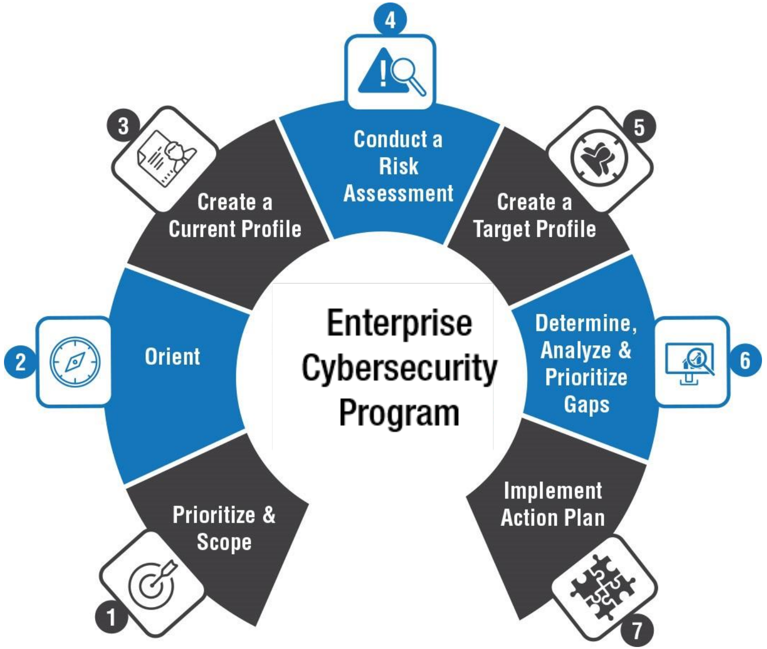
1 Identify

2 Protect

3 Detect

4 Respond

5 Recover



Enterprise Cybersecurity Program

1 Prioritize & Scope

2 Orient

3 Create a Current Profile

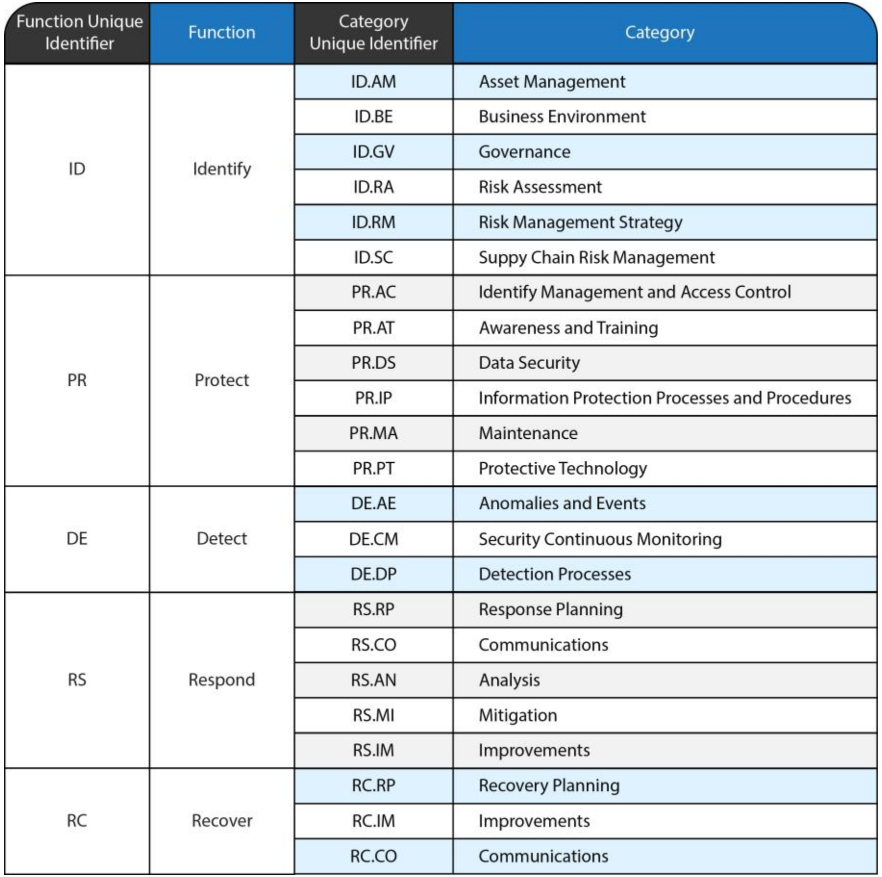
4 Conduct a Risk Assessment

5 Create a Target Profile

6 Determine, Analyze & Prioritize Gaps

7 Implement Action Plan

NIST Cybersecurity Framework: Foundation for Cybersecurity



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	Suppy 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

NIST Cybersecurity Framework v1.1 to HITRUST CSF v9.3 Mapping

#	NIST Cybersecurity Framework v1.1	HITRUST CSF v9.3
Identify (ID)		
1.	**ID.AM-1** Physical devices and systems within the organization are inventoried.	07.a Inventory of Assets
		07.d Classification Guidelines
2.	**ID.AM-2** Software platforms and applications within the organization are inventoried.	01.l Remote Diagnostic and Configuration Port Protection
		07.a Inventory of Assets
		07.d Classification Guidelines
3.	**ID.AM-3** Organizational communication and data flows are mapped.	01.l Remote Diagnostic and Configuration Port Protection
		01.m Segregation in Networks
		01.o Network Routing Control
		05.i Identification of Risks Related to External Parties
		09.m Network Controls
		09.n Security of Network Services
4.	**ID.AM-4** External information systems are catalogued.	01.i Policy on the Use of Network Services
		09.e Service Delivery
		09.n Security of Network Services
5.	**ID.AM-5** Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	01.a Access Control Policy
		01.w Sensitive System Isolation
		06.c Protection of Organizational Records
		07.a Inventory of Assets

HITRUST CSF v9.3

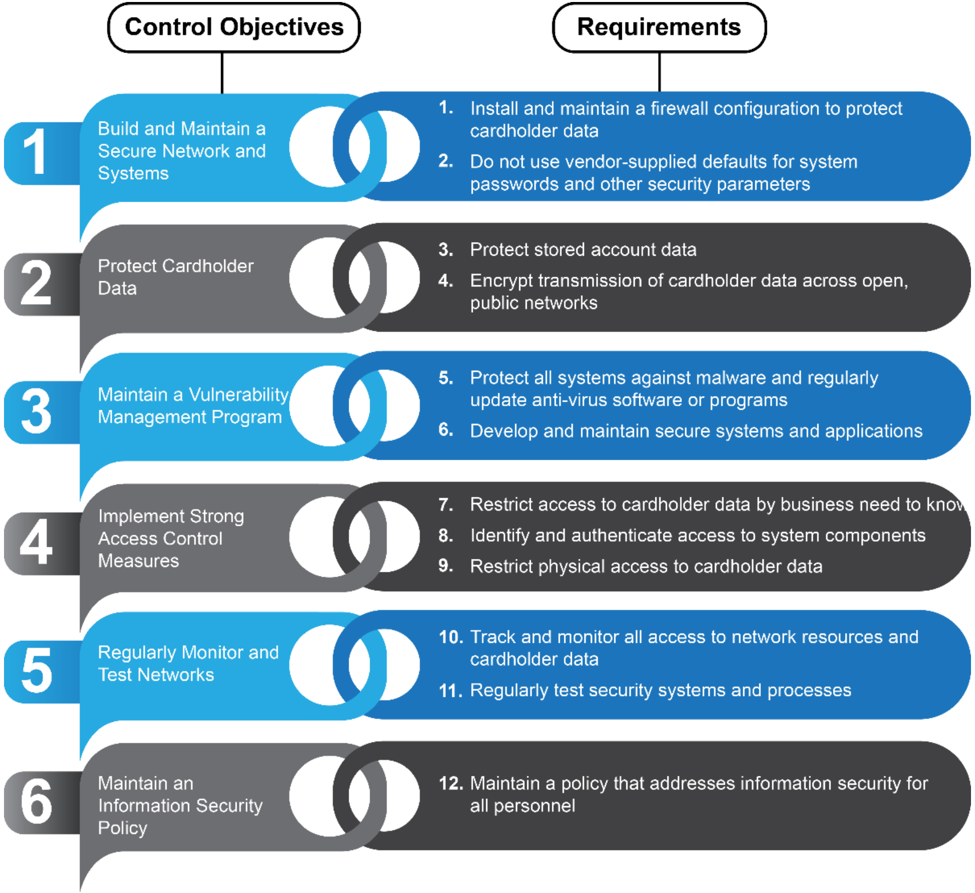
HITRUST CSF v9.3

- HITRUST CSF v9.3 incorporates and harmonizes 44 authoritative sources, added one new data privacy-related and two new security-related authoritative sources, as well as updated six existing sources.
- HITRUST CSF v9.3 updates include:
  - CCPA – requiring qualifying organizations to protect consumer data in specific ways as well as that consumers be able to opt-out sharing of their data.
  - The South Carolina Insurance Data Security Act 2018 (SCIDSA) – requiring qualifying organizations have a comprehensive information security program and the reporting of cybersecurity events.
  - NIST SP 800-171 R2 (DFARS) – providing guidance on protecting Controlled Unclassified Information (CUI) in non-federal systems and organizations.

HITRUST CSF v9.3 Cont'd.

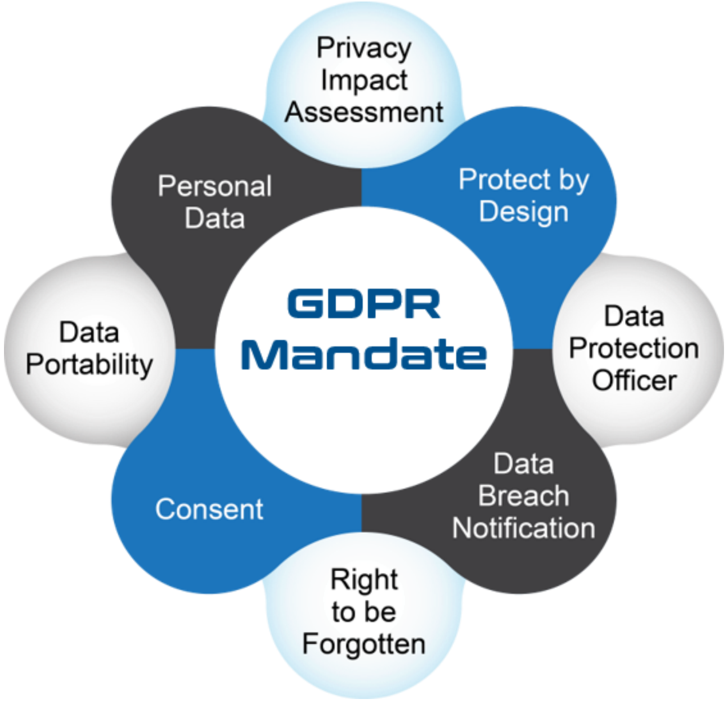
  - Updating various authoritative sources to latest versions, specifically:
    - AICPA 2017
    - CIS CSC v7.1
    - ISO 27799:2016
    - CMS/ARS v3.1
    - IRS Publication 1075 2016
    - NIST Cybersecurity Framework v1.1
  - Establish and prioritize solutions that address root-cause issues to mitigate system vulnerabilities.
- Further enhancements include:
  - Updates to the glossary to better clarify terms found in the HITRUST CSF.
  - Adjusted authoritative source mappings to more fully harmonize requirements across industries and sectors.

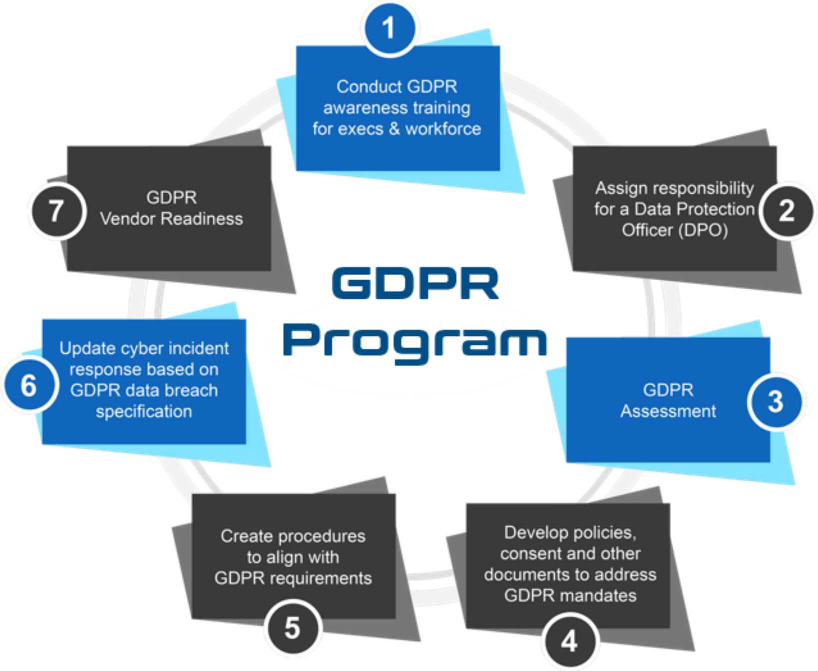
PCI DSS



Control Objectives	Requirements
1 Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
2 Protect Cardholder Data	3. Protect stored account data 4. Encrypt transmission of cardholder data across open, public networks
3 Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
4 Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
5 Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
6 Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

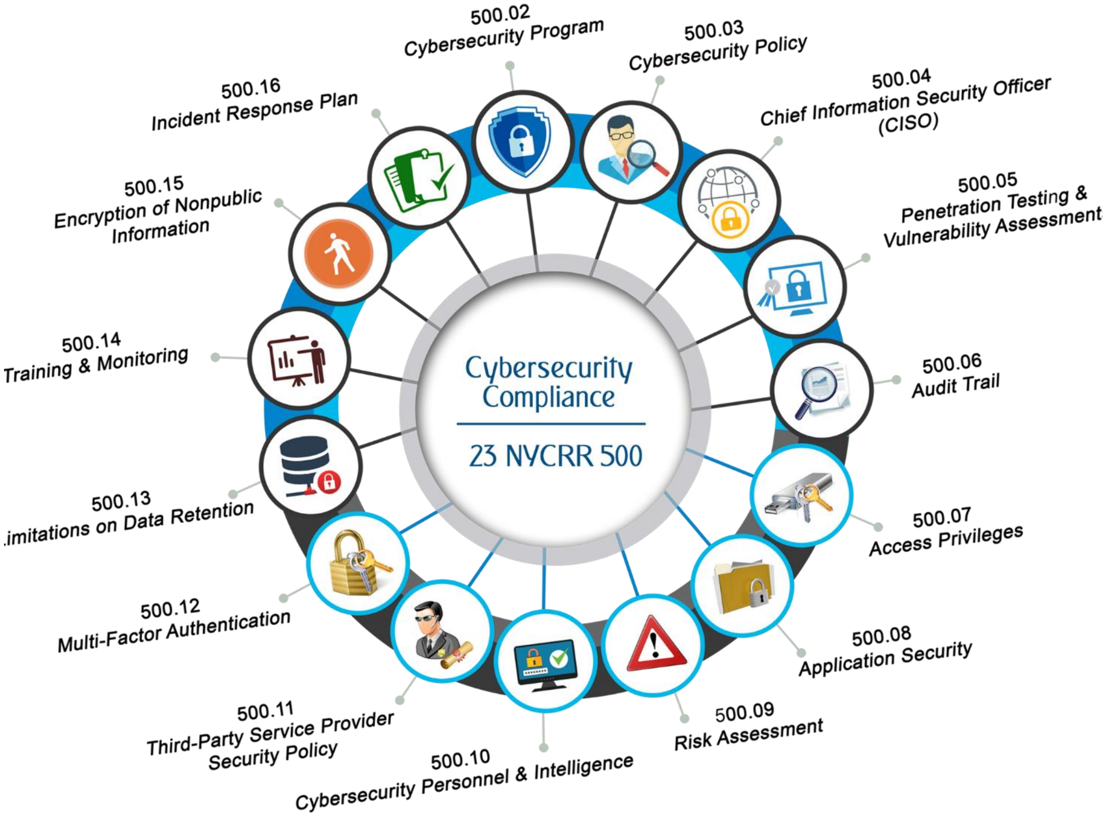
GDPR Fast Facts




GDPR Program
1 Conduct GDPR awareness training for execs & workforce
2 Assign responsibility for a Data Protection Officer (DPO)
3 GDPR Assessment
4 Develop policies, consent and other documents to address GDPR mandates
5 Create procedures to align with GDPR requirements
6 Update cyber incident response based on GDPR data breach specification
7 GDPR Vendor Readiness

ecfirst HITRUST® Authorized External Assessor

23 NYCRR 500



Cybersecurity Compliance

23 NYCRR 500

500.02 Cybersecurity Program

500.03 Cybersecurity Policy

500.04 Chief Information Security Officer (CISO)

500.05 Penetration Testing & Vulnerability Assessment

500.06 Audit Trail

500.07 Access Privileges

500.08 Application Security

500.09 Risk Assessment

500.10 Cybersecurity Personnel & Intelligence

500.11 Third-Party Service Provider Security Policy

500.12 Multi-Factor Authentication

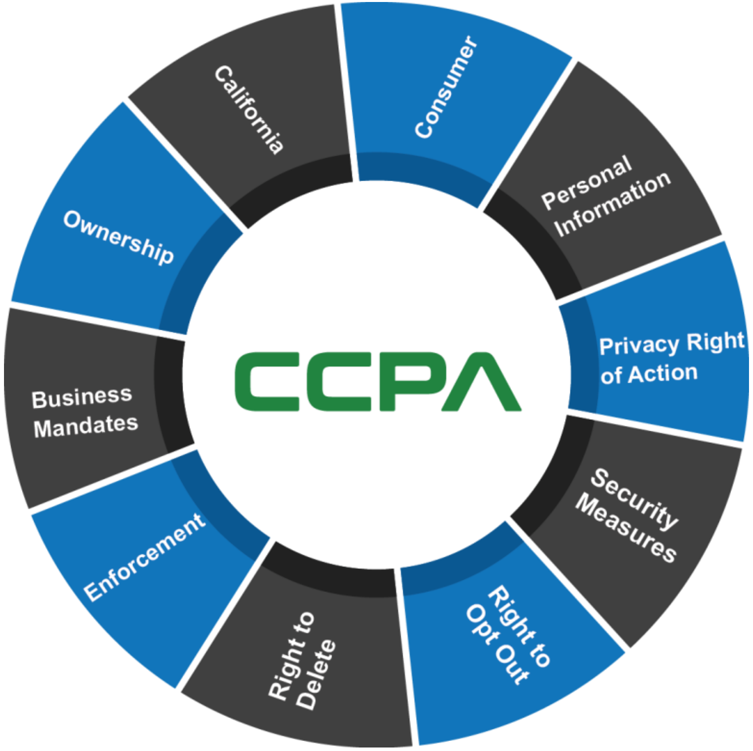
500.13 Limitations on Data Retention

500.14 Training & Monitoring

500.15 Encryption of Nonpublic Information

500.16 Incident Response Plan

CCPA Fast Facts



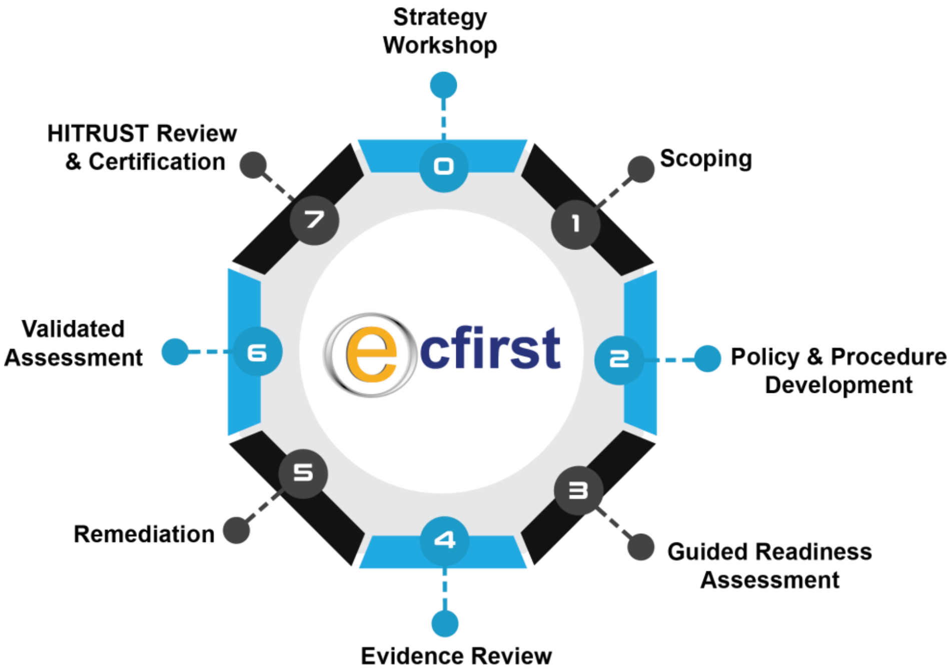
Key Facts

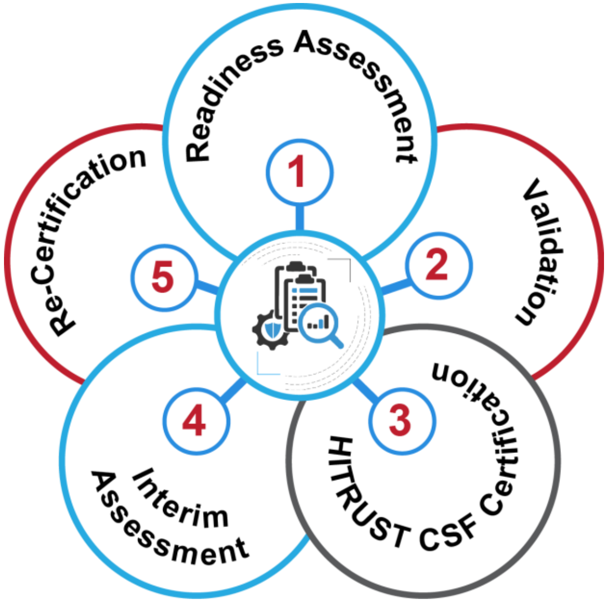
- Effective January 1, 2020.
- Enforced July 1, 2020.
- Privacy rights for California residents.
- Grants new enforcement power to the Attorney General.

Gives Ownership
Gives Security
Gives Control

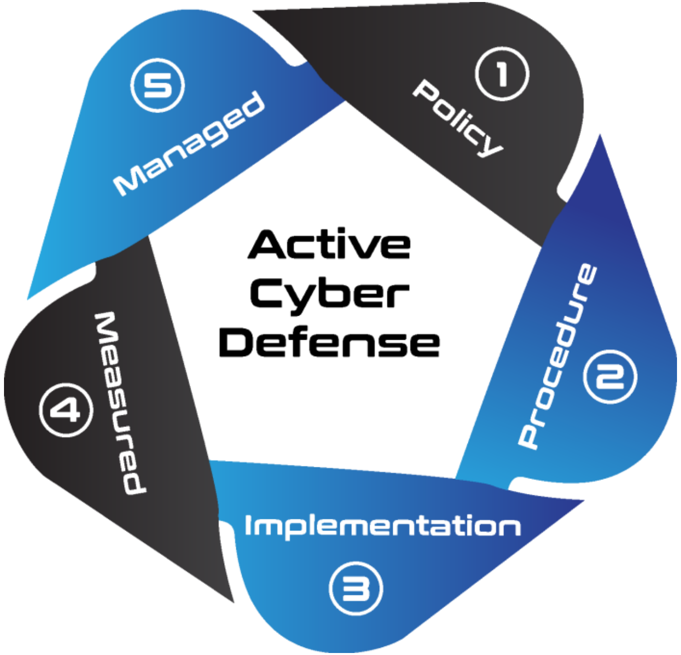
Achieving HITRUST CSF Certification

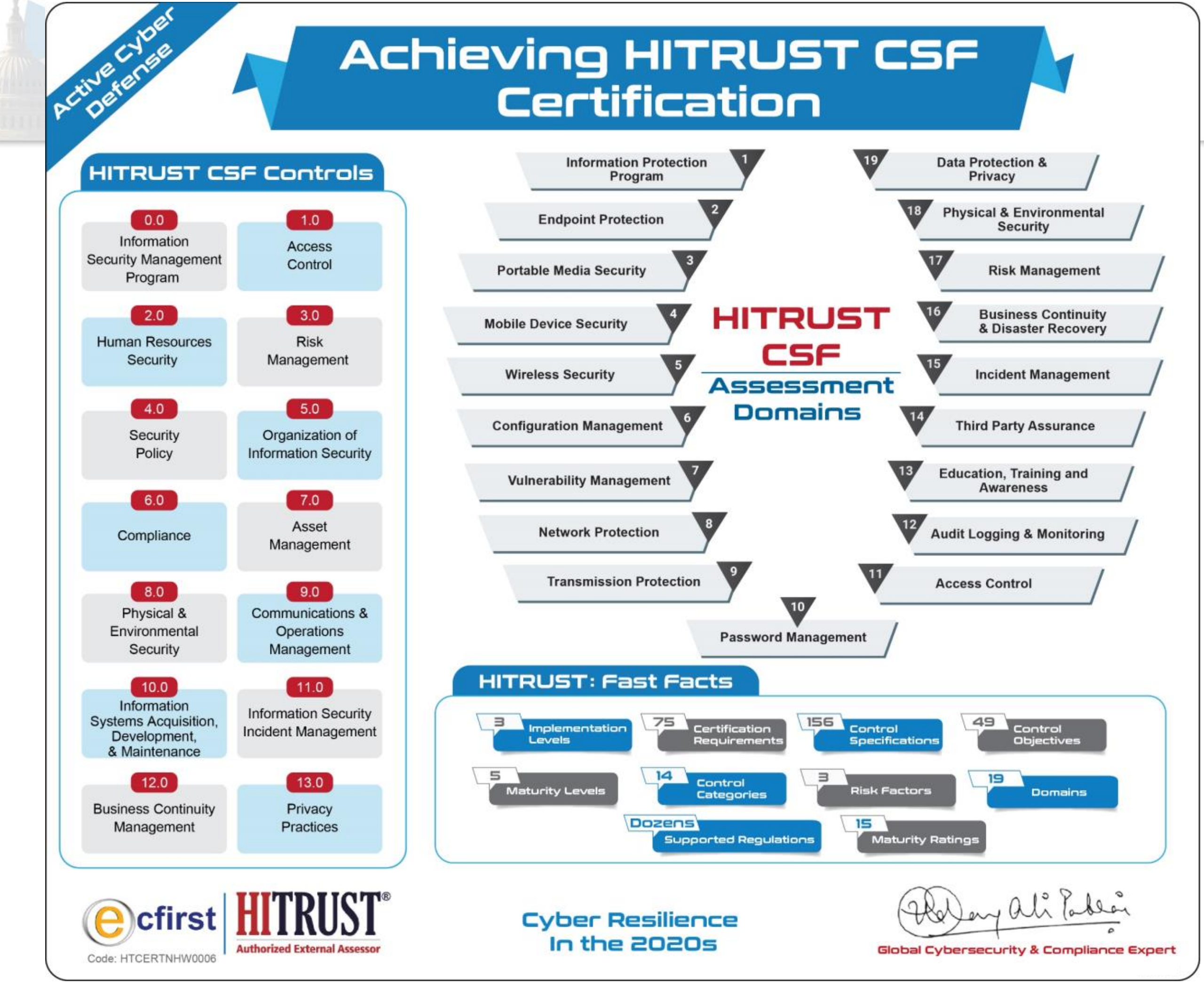
Journey to Certification


Strategy Workshop
0
Scoping
1
Policy & Procedure Development
2
Guided Readiness Assessment
3
Evidence Review
4
Remediation
5
Validated Assessment
6
HITRUST Review & Certification
7
ecfirst



HITRUST CSF Certification: Five Dimensions Aligned





Active Cyber Defense

Achieving HITRUST CSF Certification

HITRUST CSF Controls

0.0 Information Security Management Program	1.0 Access Control
2.0 Human Resources Security	3.0 Risk Management
4.0 Security Policy	5.0 Organization of Information Security
6.0 Compliance	7.0 Asset Management
8.0 Physical & Environmental Security	9.0 Communications & Operations Management
10.0 Information Systems Acquisition, Development, & Maintenance	11.0 Information Security Incident Management
12.0 Business Continuity Management	13.0 Privacy Practices

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

HITRUST: Fast Facts

3	Implementation Levels
75	Certification Requirements
156	Control Specifications
49	Control Objectives
5	Maturity Levels
14	Control Categories
3	Risk Factors
19	Domains
Dozens	Supported Regulations
15	Maturity Ratings

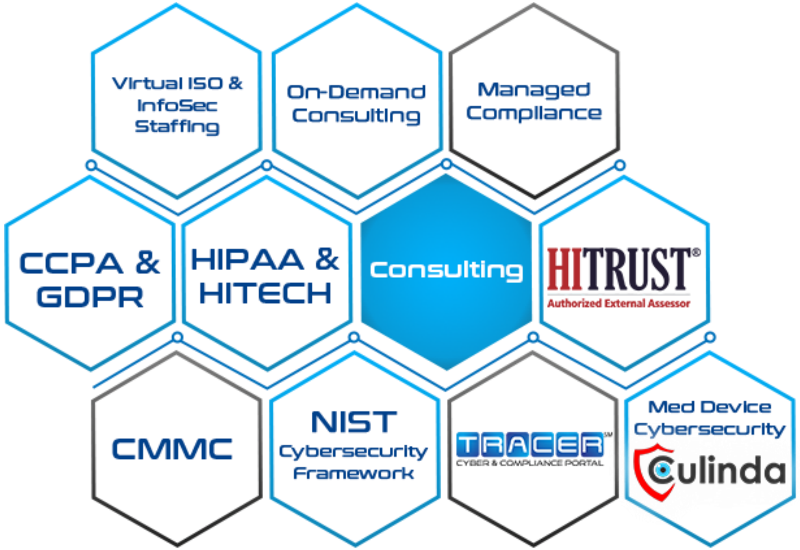
ecfirst | HITRUST® Authorized External Assessor

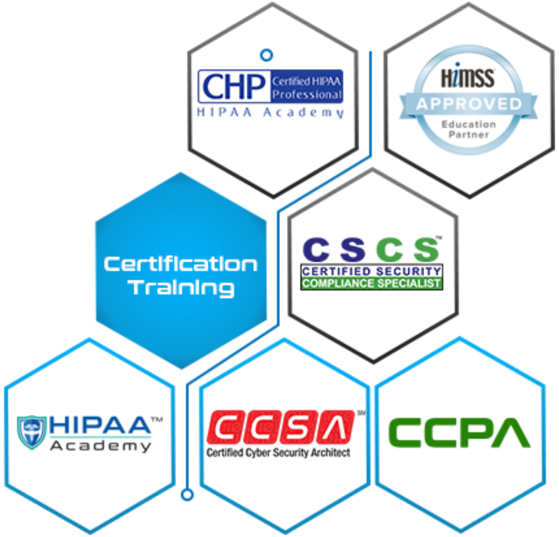
Code: HTCERTNHW0006

Cyber Resilience In the 2020s

Global Cybersecurity & Compliance Expert

ecfirst | Perfecting the Art of *Active* Cyber Defense


Virtual ISO & InfoSec Staffing
On-Demand Consulting
Managed Compliance
CCPA & GDPR
HIPAA & HITECH
Consulting
HITRUST® Authorized External Assessor
CMMC
NIST Cybersecurity Framework
TRACER℠ CYBER & COMPLIANCE PORTAL
Med Device Cybersecurity
Culinda


CHP Certified HIPAA Professional HIPAA Academy
HIMSS APPROVED Education Partner
Certification Training
CSCS™ CERTIFIED SECURITY COMPLIANCE SPECIALIST
HIPAA™ Academy
CCSA℠ Certified Cyber Security Architect
CCPA

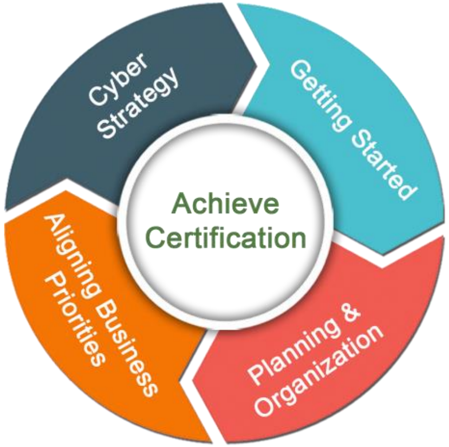
NIST | CMMC
Certification Training

HITRUST Cybersecurity Workshop

Irvine, CA	Phoenix, AZ	Dallas, TX	Chicago, IL
March 23, 2020	April 14, 2020	May 4, 2020	July 20, 2020
Washington, DC	**San Jose, CA**	**New Orleans, LA**	**Las Vegas, NV**
August 7, 2020	October 5, 2020	November 5, 2020	December 7, 2020

Learning Objectives

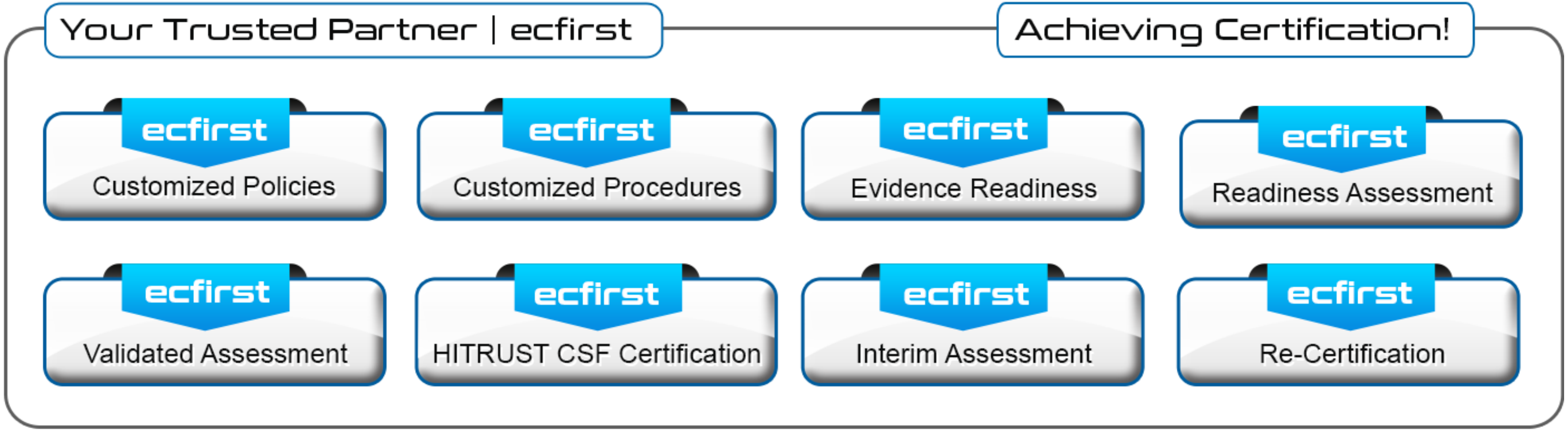
- Examine the fundamentals of the HITRUST CSF.
- Leveraging the HITRUST CSF to implement the NIST Cybersecurity Framework.
- Addressing regulatory mandates such as GDPR, HIPAA, and FISMA.
- Getting organized: From a Readiness-Assessment, through a Validated Assessment to Certification.
- Roadmap to HITRUST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



Delivered On-Site!

ecfirst HITRUST® Authorized External Assessor

HITRUST End-to-End Services from ecfirst



Your Trusted Partner | ecfirst

Achieving Certification!

- ecfirst Customized Policies
- ecfirst Customized Procedures
- ecfirst Evidence Readiness
- ecfirst Readiness Assessment
- ecfirst Validated Assessment
- ecfirst HITRUST CSF Certification
- ecfirst Interim Assessment
- ecfirst Re-Certification

Thank You!

Ali Pabrai | Ali.Pabrai@ecfirst.com | +1.949.528.5224

Robert Acosta | Bob.Acosta@ecfirst.com | +1.949.793.5700

ecfirst | HITRUST®

Authorized External Assessor