

Nov 5, 2019

Health Care Compliance Association | **HCCA**

## Compliance and Risk Assessments: Prepared?

**Marcie Swenson**, RN, JD, LLM, CHC, Attorney & Counselor, Skyda Law Group  
**Ali Pabrai**, MSEE, CISSP (ISSAP, ISSMP), HITRUST (CCSFP) 

**ecfirst** | **HITRUST**  
Authorized CSF Assessor




A diagram consisting of seven interconnected hexagons. The hexagons are arranged in a cluster. The top row contains 'Vulnerability' and 'HITRUST'. The middle row contains 'Risk', 'Cybersecurity', and 'NIST CsF'. The bottom row contains 'Compliance' and 'Assessment'. The hexagons are interconnected, suggesting a holistic approach to risk and compliance.

1

## Agenda

Health Care Compliance Association | **HCCA**



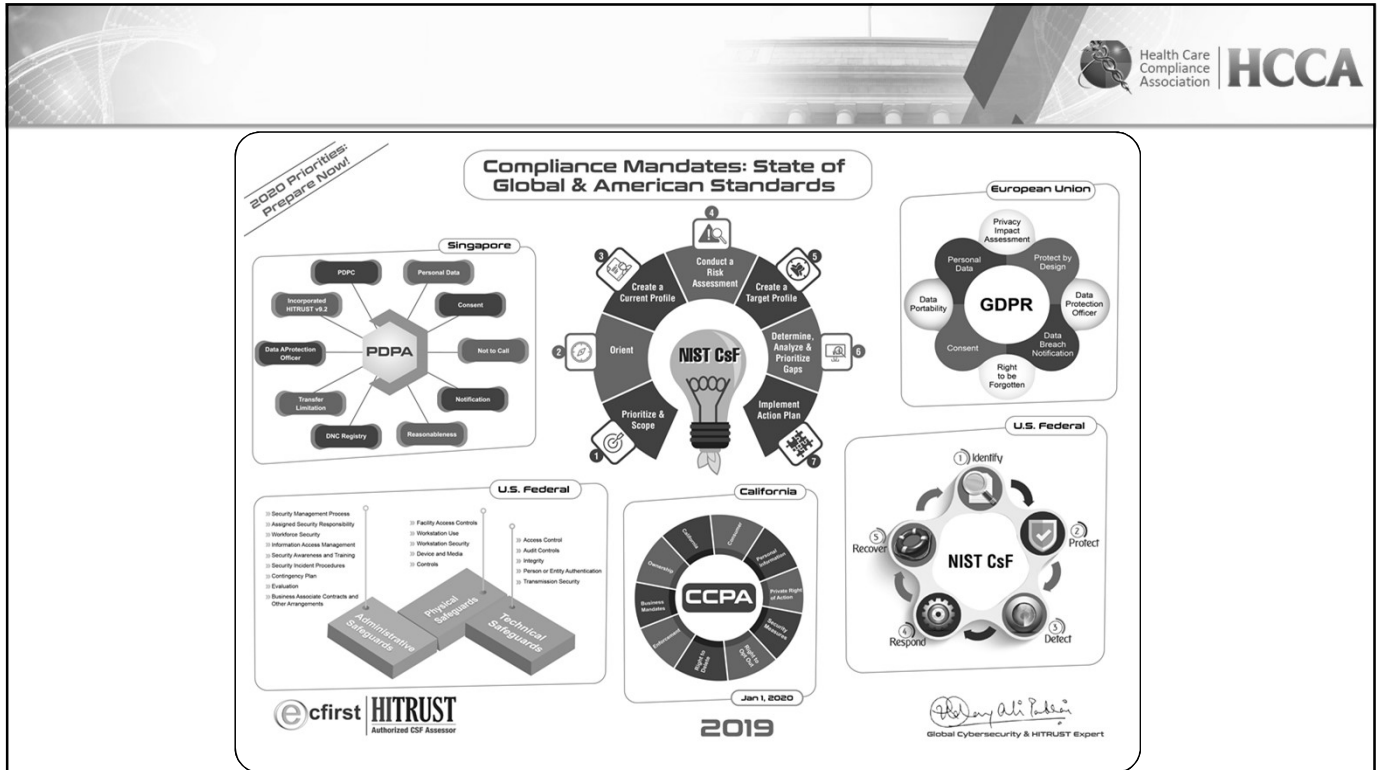
A Venn diagram with three overlapping circles. The top circle is labeled 'Risk Analysis' and contains a warning icon. The bottom-left circle is labeled 'Getting Started' and contains a shield icon. The bottom-right circle is labeled 'Cybersecurity Assessment' and contains a laptop icon. The intersection of all three circles is shaded, indicating a comprehensive approach.

### Learning Objectives

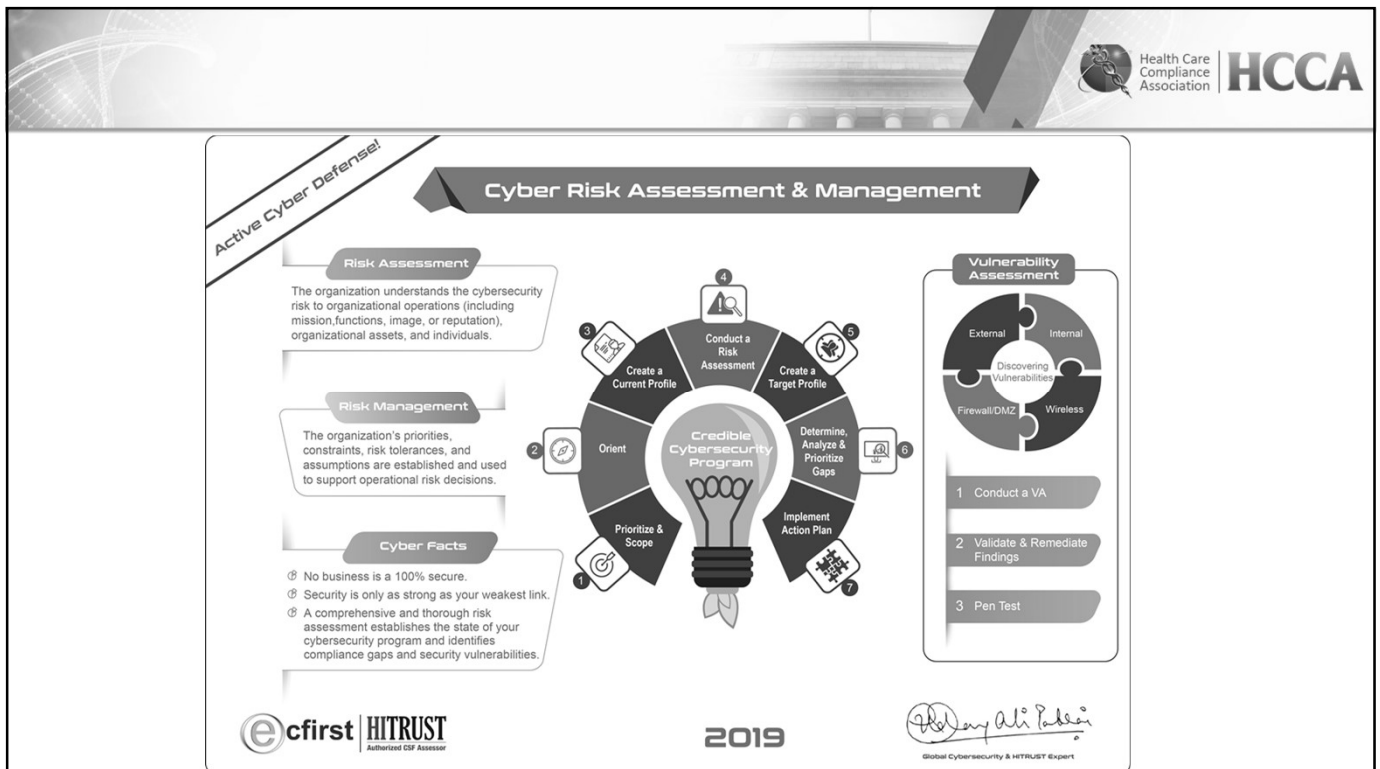
- Prepare for 2020 compliance mandates including lessons learned from 2019 settlements and enforcement
- Examine core components for a comprehensive and thorough risk assessment exercise
- Step through key areas for establishing a credible, evidence-based compliance and risk assessment program

2

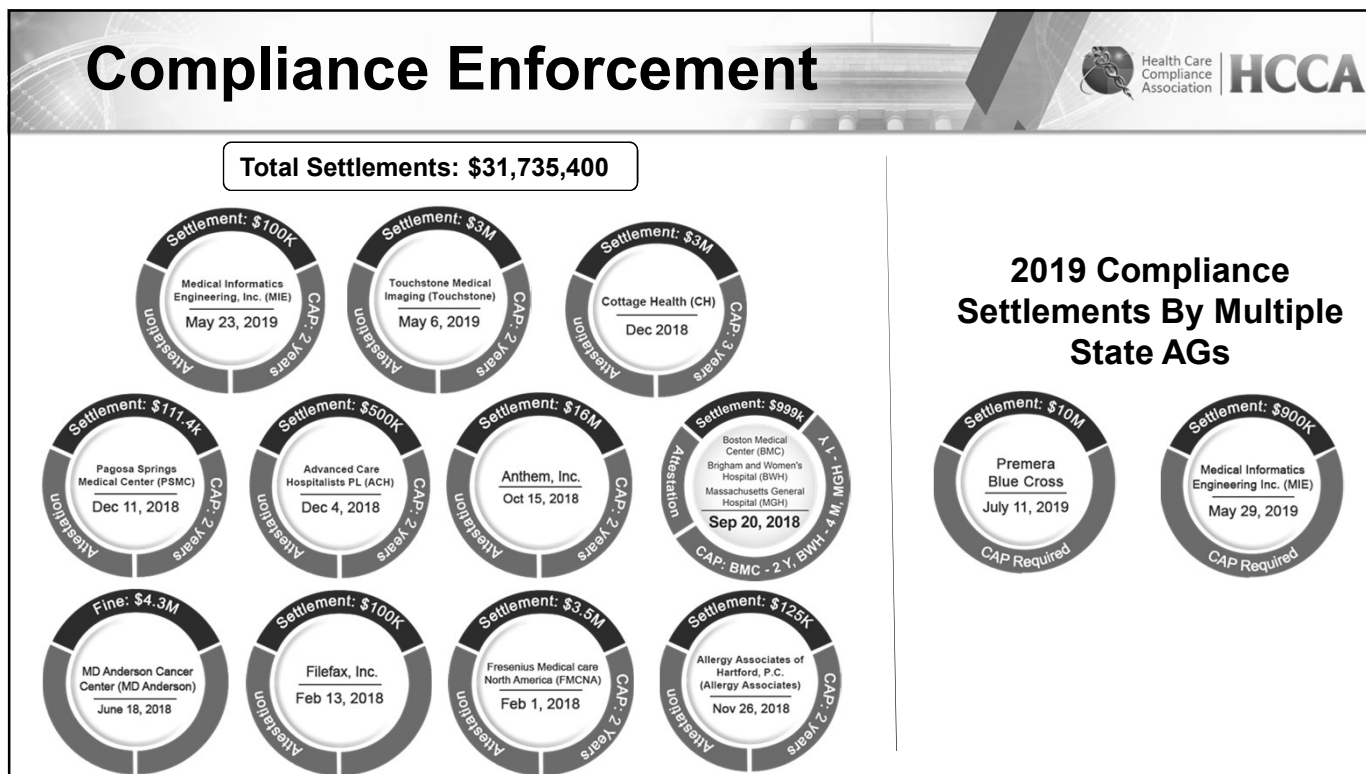
# Applying HITRUST to Address NIST CsF, GDPR & More



3



4



5



6

## Risk Assessment



**A Risk Assessment is a “point-in-time” assessment of current compliance status; it does not, and cannot, provide an assessment of unknown or undeclared risks and vulnerabilities or those that may evolve in the future.**



7

## Critical Findings



- 🔗 Risk Assessment established the following areas of risk:
- 🔗 **Epic:** Access is not segmented by facility and employees can access records that they are not authorized for.
  - 🔗 **Workstation Security.** Controls not in place on personal mobile devices or removable devices.
  - 🔗 **Encryption.** Data at rest not encrypted.
  - 🔗 **Audit Controls.** Documented procedures not in place; audits are not conducted regularly.
  - 🔗 **Information System Activity Review.** Documented procedure or processes are not in place to review information system activity.

8

## State of Compliance



Compliance Mandate	Report 2019
<b>Security Rule</b>	
Administrative Safeguards	C-
Physical Safeguards	D+
Technical Safeguards	D+
Organizational Requirements	A
Policies, Procedures and Documentation	D+
<b>Breach Notification</b>	
Reporting	A
Policies, Procedures and Documentation	A
<b>Privacy Rule</b>	
Administrative Requirements	A
Uses and Disclosures	B-
Policies, Procedures and Documentation	A-

9

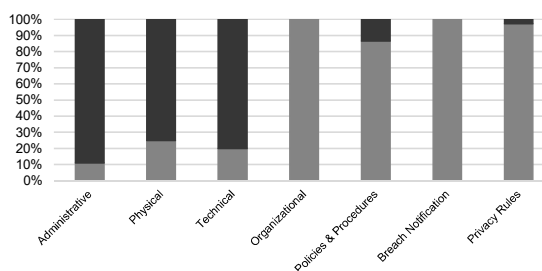
## Compliance Dashboard



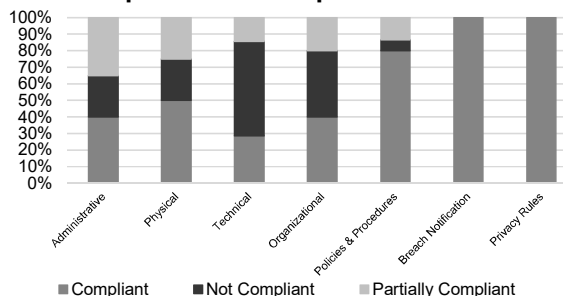
### Compliance Progress



### Standards



### Implementation Specifications



10

## Compliance Status Detail Table



Security Rule		
Administrative Safeguards		
Standard / Implementation Specification	Compliance Status	Grade
Security Management Process § 164.308 (a)(1)(i) STD	Not Compliant	F
Risk Analysis (R) § 164.308 (a)(1)(ii)(A) SPEC	Not Compliant	D+
Risk Management (R) § 164.308 (a)(1)(ii)(B) SPEC	Partially Compliant	C-
Sanction Policy (R) § 164.308 (a)(1)(ii)(C) SPEC	Compliant	A
Information System Activity Review (R) § 164.308 (a)(1)(ii)(D) SPEC	Not Compliant	F
Assigned Security Responsibility § 164.308 (a)(2) STD	Not Compliant	F
Workforce Security § 164.308 (a)(3)(i) STD	Compliant	A-
Authorization and/or Supervision (A) § 164.308 (a)(3)(ii)(A) SPEC	Compliant	A
Workforce Clearance Procedure (A) § 164.308 (a)(3)(ii)(B) SPEC	Compliant	A-

11

## Compliance Status Detail Table (Cont'd...)



Technical Safeguards		
Standard / Implementation Specification	Compliance Status	Grade
Access Control § 164.312 (a)(1) STD	Not Compliant	F
Unique User Identification (R) § 164.312 (a)(2)(i) SPEC	Compliant	B+
Emergency Access Procedure (R) § 164.312 (a)(2)(ii) SPEC	Compliant	A
Automatic Logoff (A) § 164.312 (a)(2)(iii) SPEC	Partially Compliant	C+
Encryption and Decryption (A) § 164.312 (a)(2)(iv) SPEC	Not Compliant	F
Audit Controls § 164.312 (b) STD	Not Compliant	F
Integrity § 164.312 (c)(1) STD	Not Compliant	F
Mechanism to Authenticate ePHI (A) § 164.312 (c)(2) SPEC	Not Compliant	F
Person or Entity Authentication § 164.312 (d) STD	Compliant	A-

12

## Corrective Action Plan: HIGH



Description	Standard / Implementation Specification	Priority
Document the Information Security Official's appointment and responsibilities in a policy that complies with this Standard.	Assigned Security Responsibility §164.308 (a) (2) STD	3
Develop, approve and publish a policy and procedures to address this requirement.	Security Management Process §164.308 (a) (1) (I) STD	1
Develop a policy and procedures to address Information Access Management (164.308 (a) (4) (I)). Implement, and train the workforce accordingly.	Information Access Management (164.308 (a) (4) (I)) STD	3
Develop, approve and publish a policy and appropriate procedures to address Audit Controls (164.312 (b)).	Audit Controls (164.312 (b)) STD	1
Create a schedule for proactive reviews, but also include opportunities for ad-hoc validation of reviews and audit procedures.	Information System Activity Review §164.308 (a) (1) (ii) (D) SPEC	3
In cases where the ePHI cannot be encrypted, reasons should be documented and periodically reviewed to determine if and when encryption can be enabled in the future.	Encryption and Decryption §164.312 (a) (2) (iv) SPEC	1

13

## Corrective Action Plan: MEDIUM



Description	Standard / Implementation Specification	Priority
Document all Compliance Standards and Implementation Specifications that the evaluation procedure considers in a policy covering information security evaluations. Include all information security regulations to which complies in this policy.	Evaluation (164.308 (a) (8)) STD	7
Create needed network diagrams and ensure they are regularly reviewed and updated.	Security Management Process §164.308 (a) (1) (I) STD	7
Identify all types of data and assign a sensitivity category. Best practice is to use FIPS 199 and NIST SP 800-60 for guidance.	Security Management Process §164.308 (a) (1) (I) STD	7
Establish procedures to review access authorizations for accuracy; ensure proper access establishment and modification protocols have been followed.	Access Establishment and Modification §164.308 (a) (4) (ii) (C) SPEC	5
Periodically audit log files for admin/DBA access to ensure appropriate use.	Mechanism to Authenticate Electronic Protected Health Information §164.312 (c) (2) SPEC	6

14

## Corrective Action Plan: LOW



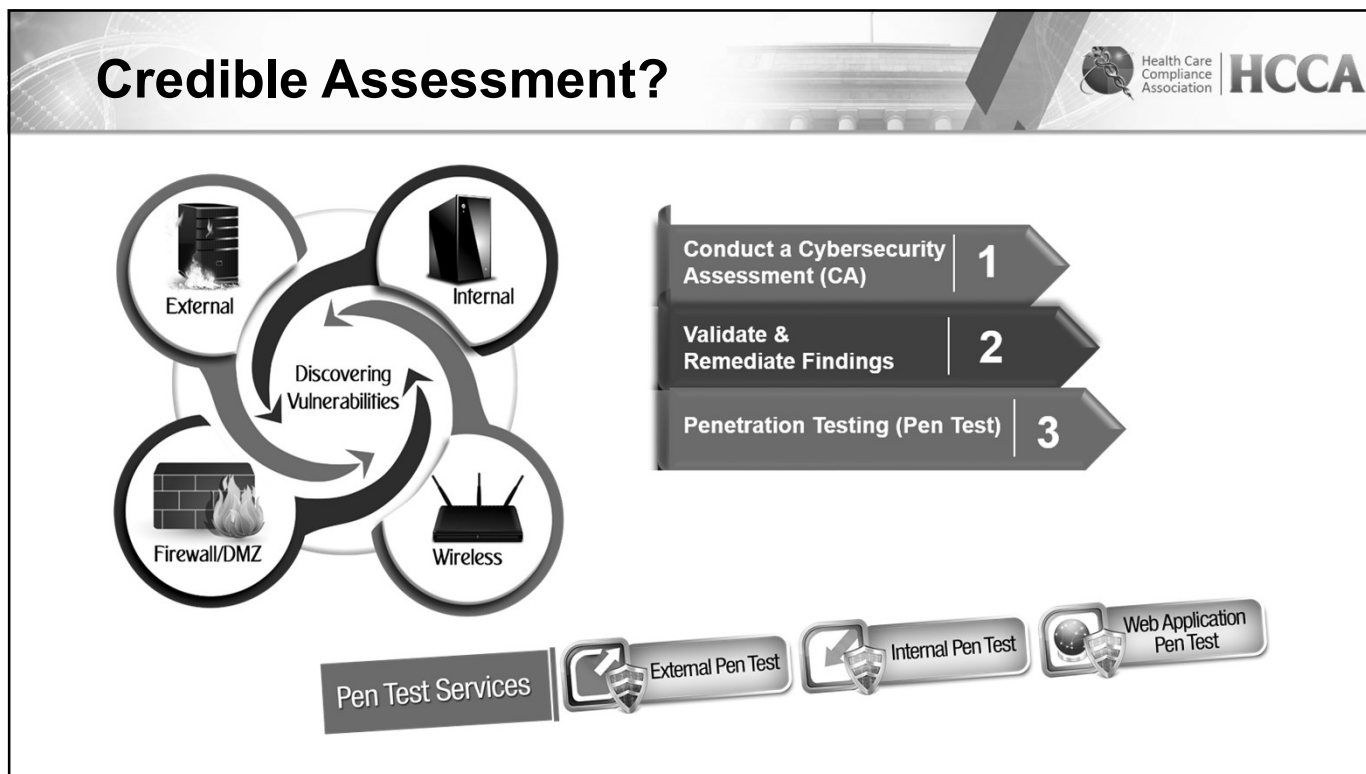
Description	Standard / Implementation Specification	Priority
Budget and perform risk analysis exercises on a regular schedule; such exercise must include a comprehensive technical vulnerability assessment to identify security gaps. the best practice in the industry is to conduct this exercise on an annual basis.	Risk Analysis §164.308 (a) (1) (ii) (A) SPEC	9
An initial comprehensive assessment must be conducted to set a baseline for future evaluations.	Evaluation (164.308 (a) (8)) STD	9
Evaluations should be conducted periodically; best practice is to do this annually.	Evaluation (164.308 (a) (8)) STD	9
Implement the automated vulnerability assessment tool. Document findings of all scans and assessments and report those findings to senior management. Document the details of the vulnerability scans and penetration tests in a policy and procedures.	Risk Analysis §164.308 (a) (1) (ii) (A) SPEC	10.75
Patch management procedures need to be documented and fully understood by all concerned parties.	Risk Management §164.308 (a) (1) (ii) (B) SPEC	9.5

15

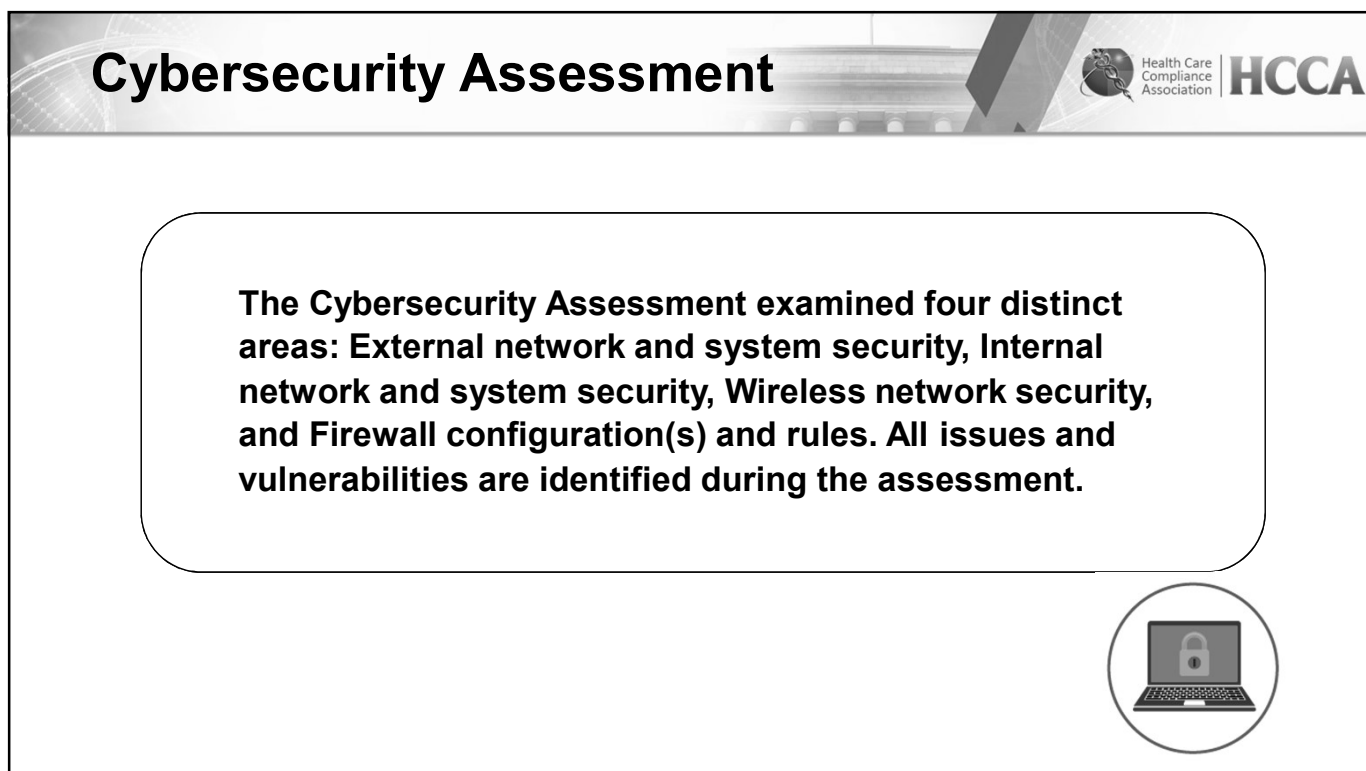


16





17



18

## Risk Summary



### Determined risk status:

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

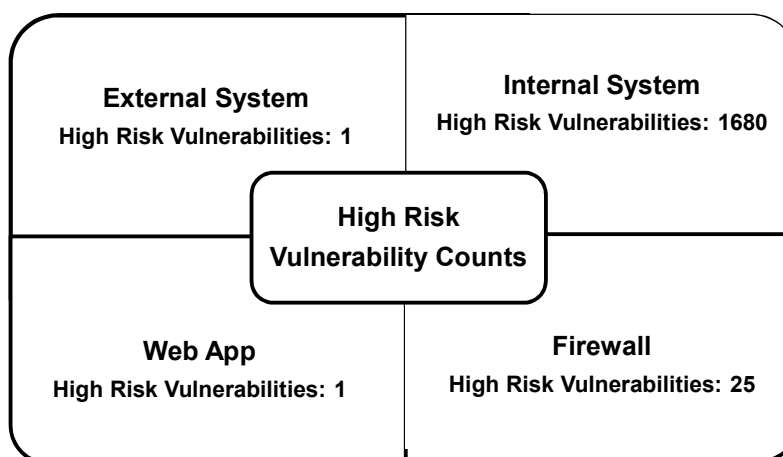
### Based on the following major issues:

- Sensitive information contained in publicly accessible documents
- IAM doesn't follow best practice
- Password policies don't follow best practice
- Weak credentials in use
- Out-of-date and unsupported software in use
- Insecure system configurations
- Number of open SQL servers
- Large number of potentially rogue wireless networks identified



19

## Significant Findings



20

## Cybersecurity Assessment: Grade



Grade	Disposition
<b>A</b>	Overall, the organization is above average in relation to the security controls and practices implemented.
<b>B</b>	Overall, the organization is average in relation to the security controls and practices implemented. Minor updates or changes will help to increase overall security.
<b>C</b>	Overall, the organization slightly below average in relation to the security controls and practices implemented. A number of updates or changes are required to bring the state of security to an acceptable level.
<b>D</b>	Overall, the organization is below average in relation to the security controls and practices implemented. A significant amount of updates or changes are required to bring the state of security to an acceptable level.
<b>F</b>	Overall, the organization is far below average in relation to the security controls and practices implemented. Basic security controls and practices need to be implemented to bring the state of security to a minimum level.

21

## Cybersecurity Assessment: Rating



Risk Rating	Impact
<b>High</b>	<p>Highly likely a malicious event will occur and could be expected to have a severe or catastrophic adverse effect on organizational operations or organizational assets.</p> <ul style="list-style-type: none"> <li>• Cause a severe degradation in, or loss of, mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions</li> <li>• Result in major damage to organizational assets</li> <li>• Result in major financial loss</li> </ul>
<b>Medium</b>	<p>Somewhat likely a malicious event may occur and could be expected to have a serious adverse effect on organizational operations or organizational assets.</p> <ul style="list-style-type: none"> <li>• Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced</li> <li>• Result in significant damage to organizational assets</li> <li>• Result in significant financial loss</li> </ul>
<b>Low</b>	<p>Unlikely a malicious event may occur, but if it were to happen could be expected to have a limited adverse effect on organizational operations or organizational assets.</p> <ul style="list-style-type: none"> <li>• Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced</li> <li>• Result in minor damage to organizational assets</li> <li>• Result in minor financial loss</li> </ul>

22

## Report Card



### Cybersecurity Assessment Report Card

Area	2018	2019
External Network	B	B-
Internal Network	D	D
Wireless Network	B-	B+
Firewall Configuration	B-	B-
<b>Overall Cybersecurity Grade</b>	<b>C-</b>	<b>C</b>

23

## External Assessment



External	Issues	Overall Risk
High Risk System Vulnerabilities	1	High
Medium Risk System Vulnerabilities	52	Medium
Low Risk System Vulnerabilities	32	Low
Positive Google Hacking Database Queries	1	Low
Documents containing Metadata	56	Low
DNS Assessment	3	Low

Web App Assessment	Issues	Overall Risk
High Risk Web Site/App Vulnerabilities	1	High
Medium Risk Web Site/App Vulnerabilities	2	Medium
Low Risk Web Site/App Vulnerabilities	10	Low

24

## Internal Assessment



Internal	Issues	Overall Risk
High Risk System Vulnerabilities	1,680	High
Medium Risk System Vulnerabilities	2,321	Medium
Low Risk System Vulnerabilities	391	Low
Endpoint Assessment - USB Storage Devices	13,108	High
Endpoint Assessment - USB Communication Devices	128	Low
Insecure SNMP Community Strings	6	Low
Open SQL Servers / Weak Credentials In Use	9 / 0	High

25

## Wireless Network Assessment



Wireless	Issues	Overall Risk
Open/Unsecured Access Points/SSID's	197	Medium
Access Points/SSID's using Pre-shared Keys	58	Low
Hidden Access Points/SSID's	624	Medium
Potentially Rogue Access Points/SSID's	209	Medium

26

## Firewall Assessment



Internal	Issues	Overall Risk
High Risk Vulnerabilities	25	High
Medium Risk Vulnerabilities	26	Medium
Low Risk Vulnerabilities	25	Low

27

## Cybersecurity Assessment CAP: Next Steps



### Recommended to be addressed within 30 days

- 🔗 Upgrade all software in use to the most current version on all systems.
- 🔗 Update Firewall configurations to be as restrictive as possible.
- 🔗 Install missing Microsoft patches on all applicable systems.
- 🔗 Configure Firewall rules to be as restrictive as possible.

28

## Cybersecurity Assessment CAP: Next Steps



### Recommended to be addressed within 90 days

- 🔗 Develop (or update as applicable) and implement a Patching policy & procedures for systems.
- 🔗 Develop (or update as applicable) and implement an Account Management policy & procedures for Active Directory.
- 🔗 Develop (or update as applicable) and implement a Secure Password policy & procedures.
- 🔗 Investigate potentially rogue Access Points identified.
- 🔗 Perform a Firewall Rule Review to ensure a business justification for all rules is formally documented.
- 🔗 Change default SNMP Community Strings and account credentials in use.
- 🔗 Remediate or accept Risk for all **High** and **Medium** severity vulnerabilities.
  - 🔗 Review remediation activities weekly

29

## Cybersecurity Assessment CAP: Next Steps



### Recommended to be addressed within 180 days

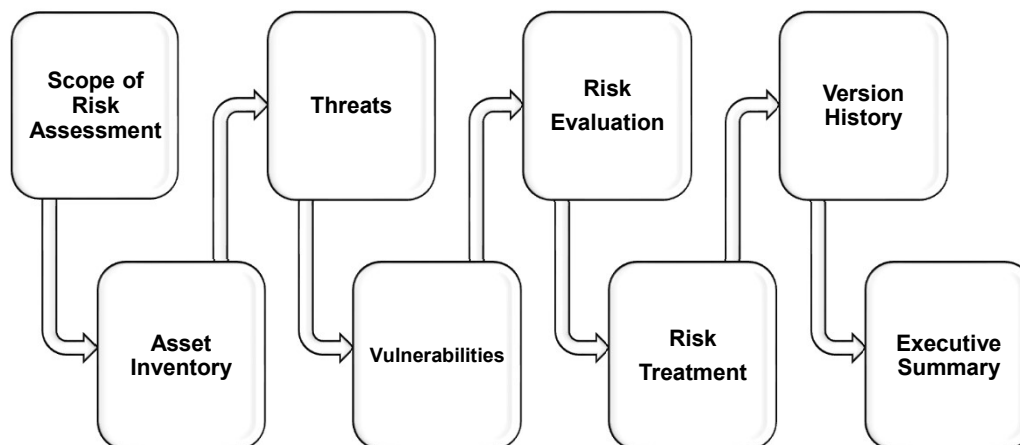
- 🔗 Develop (or update as applicable) and implement Baseline Configuration Standards for systems.
- 🔗 Develop and implement a Web Application Secure Development Life Cycle.
- 🔗 Develop (or update as applicable) and implement a Data Security policy & procedures to protect the CIA of sensitive data; consider the use of a Data Loss Prevention (DLP) system.
- 🔗 Ensure External DNS systems and records are configured following best practices.
- 🔗 Finalize remediation tasks including remediating or accepting the Risk for **Low** severity vulnerabilities.
  - 🔗 Review remediation activities weekly
- 🔗 Implement 802.1x authentication for wireless networks.
- 🔗 Schedule a Titanium Cybersecurity Assessment.
- 🔗 Perform periodic vulnerability scans.

30



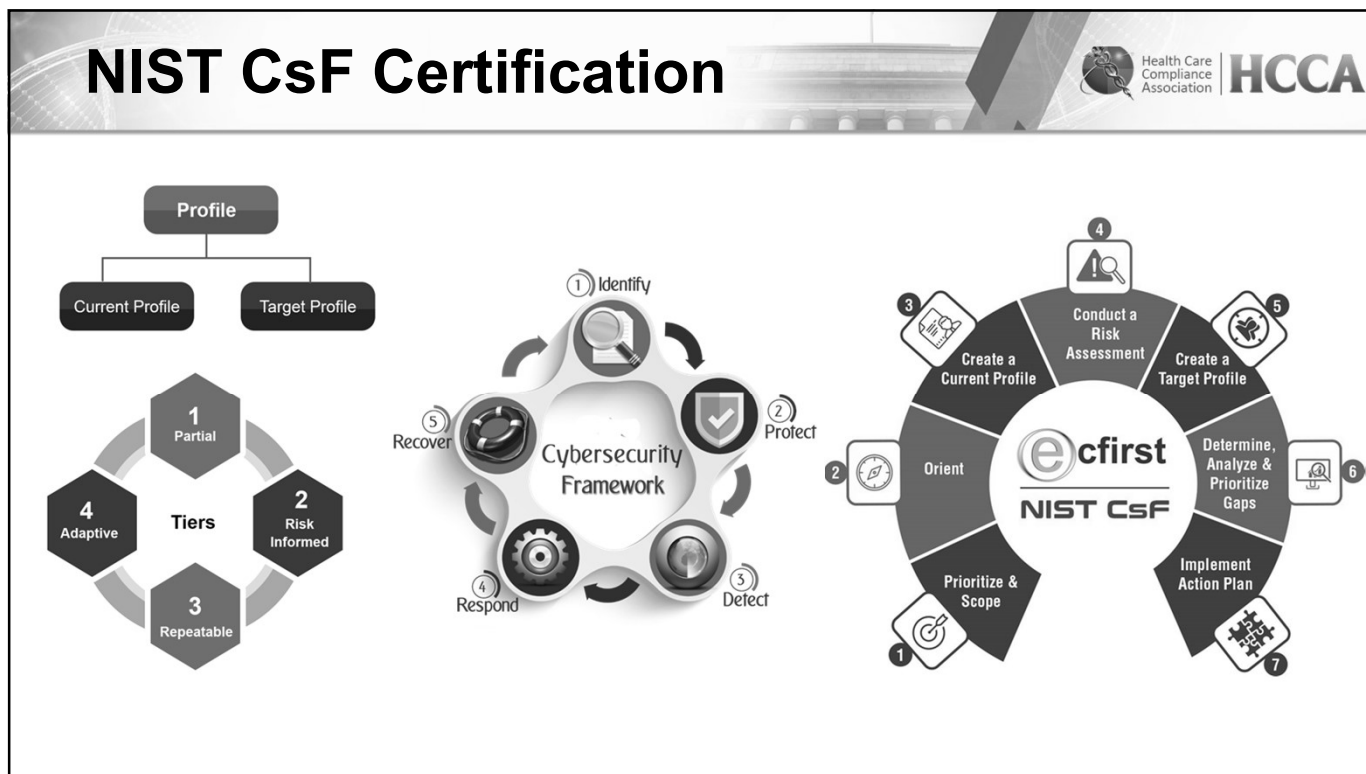
31

## NIST CsF Credible Reference for Risk Assessment



32





33

## Function and Category Unique Identifiers

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
ID	Protect	PR.AC	Identify Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.JP	Information Protection Processes and Procedures
		PR.MA	Maintenance
DE	Detect	PR.PT	Protective Technology
		DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
RS	Respond	DE.DP	Detection Processes
		RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
RC	Recover	RS.IM	Improvements
		RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

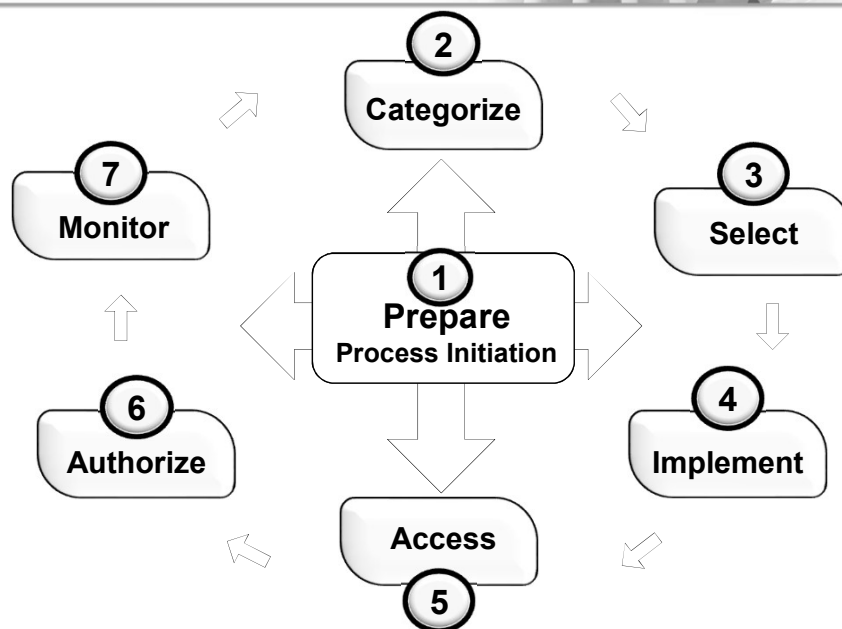
34

## Organization-Wide Risk Management Approach



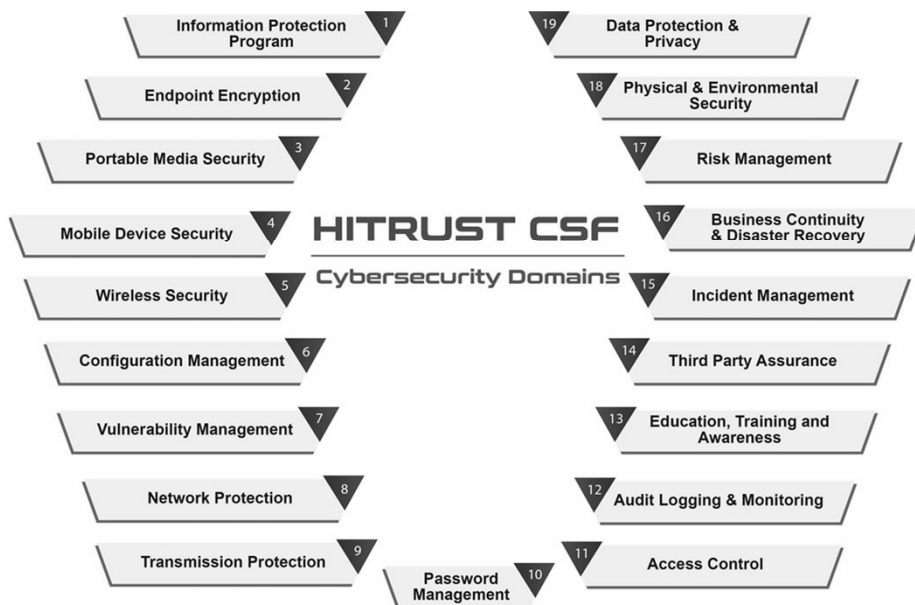
35

## Risk Management Framework



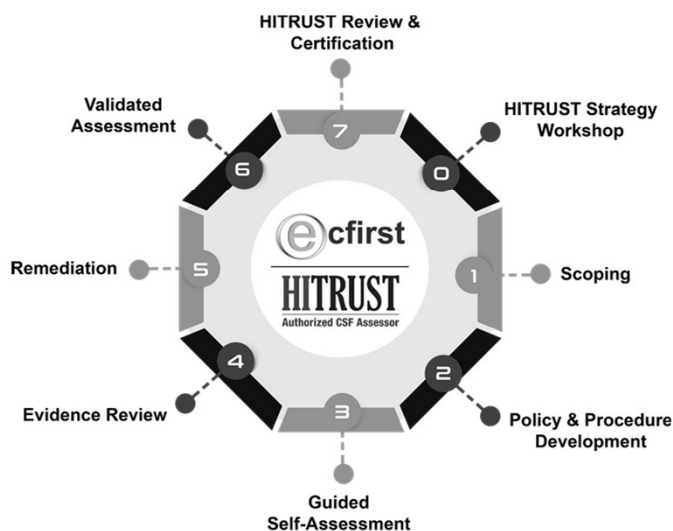
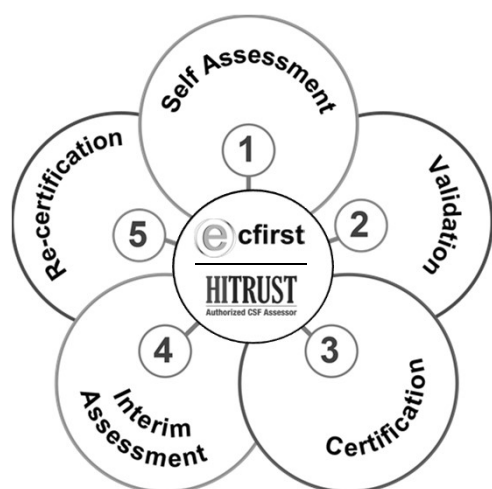
36

## Mission Critical Assets! HITRUST CSF Certification

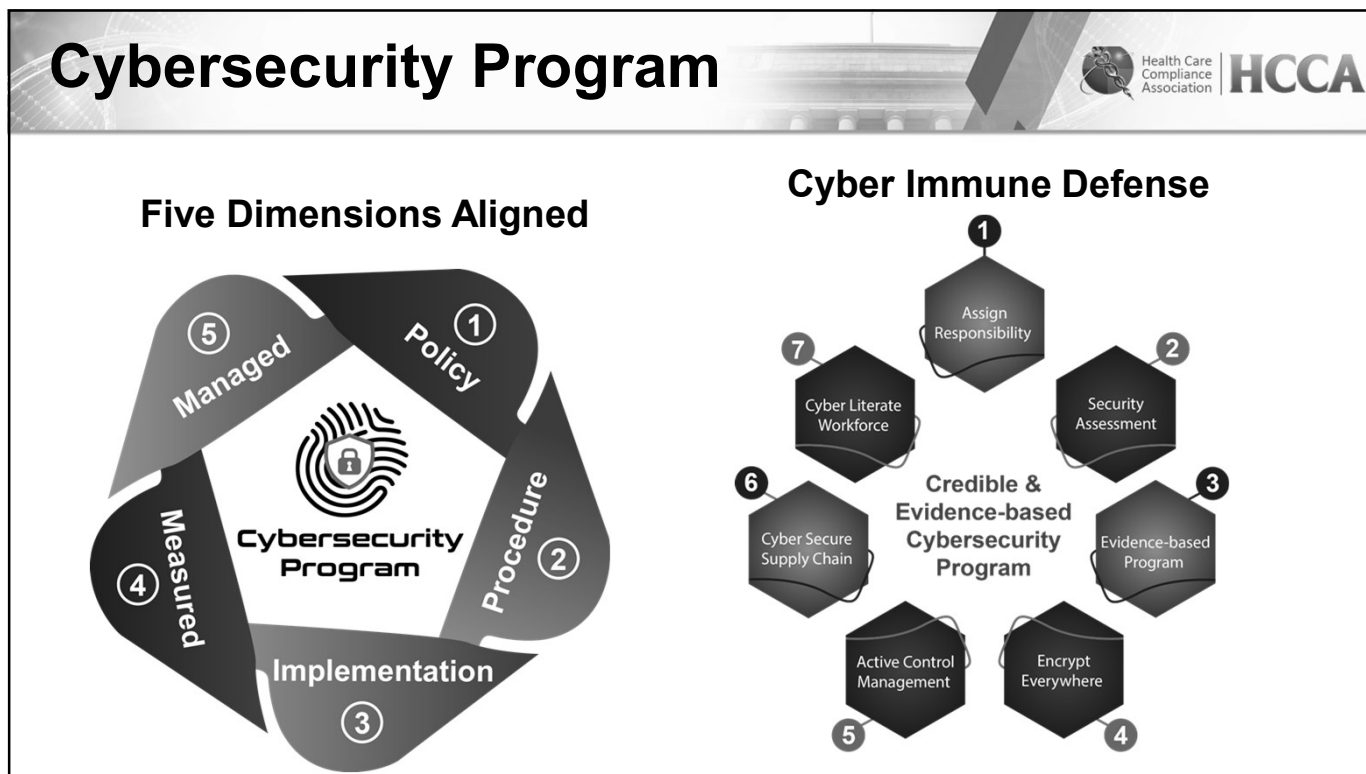


37

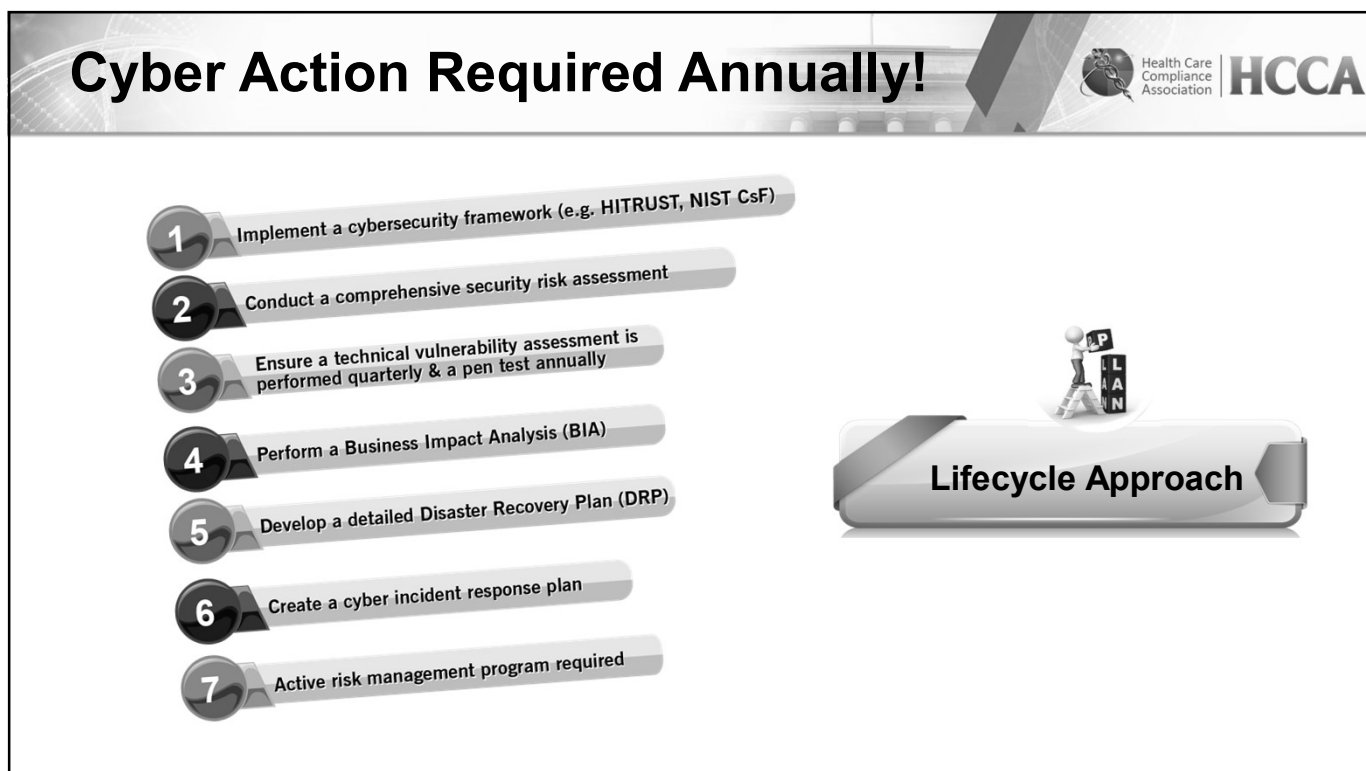
## HITRUST CSF Certification



38

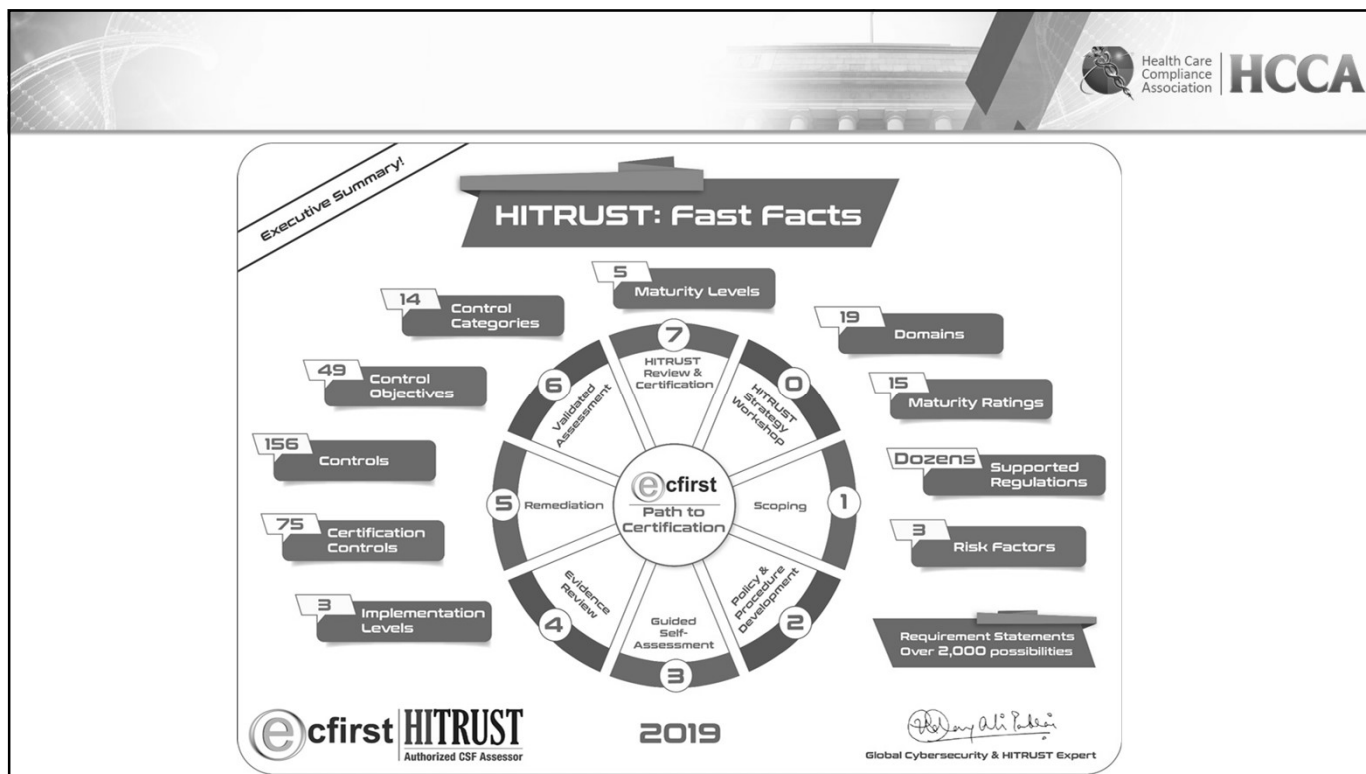


39

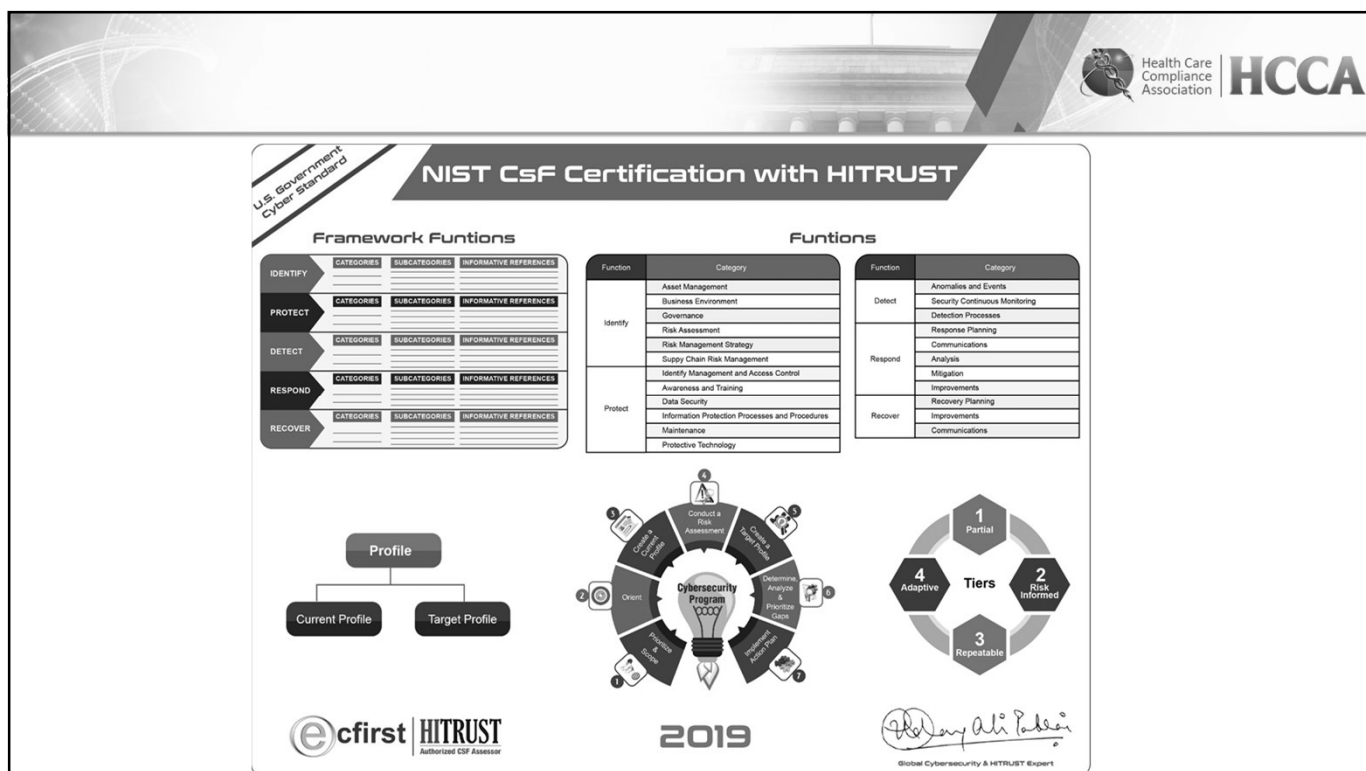


40

# Applying HITRUST to Address NIST CsF, GDPR & More

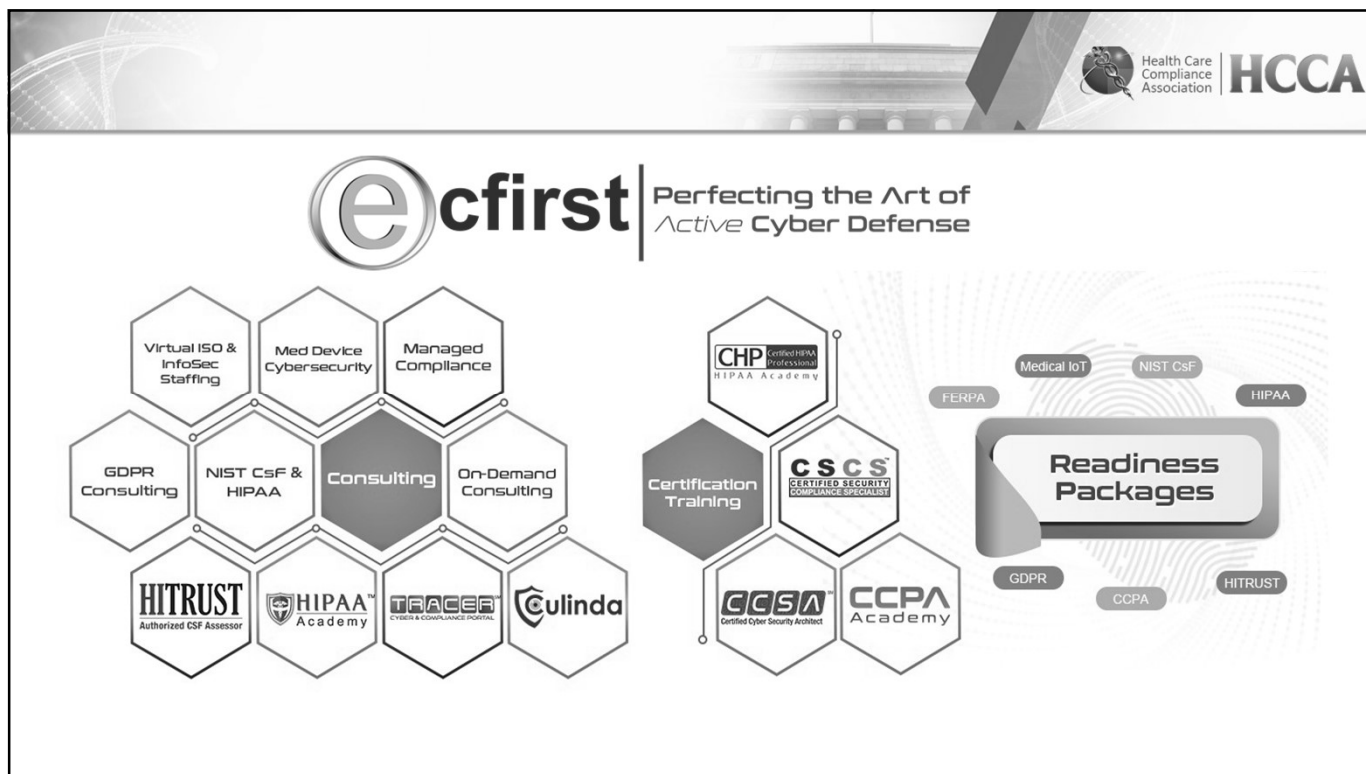


41



42

# Applying HITRUST to Address NIST CsF, GDPR & More



43

This slide is a "Thank You!" message from ecfirst and HITRUST. It features the Health Care Compliance Association (HCCA) logo at the top left. The text "Thank You!" is prominently displayed in the center. To the right, a cluster of hexagons contains the terms: Vulnerability, HITRUST, Risk, Cybersecurity, Compliance, NIST CsF, and Assessment. At the bottom, a contact box provides the following information:

Marcie Swenson | MarcieS@MySkyda.com | +1.801.830.9113  
Ali Pabrai | Ali.Pabrai@ecfirst.com | +1.949.528.5224

The ecfirst logo and HITRUST Authorized CSF Assessor logo are located at the bottom right. The background shows a stylized image of a classical building with columns.

44