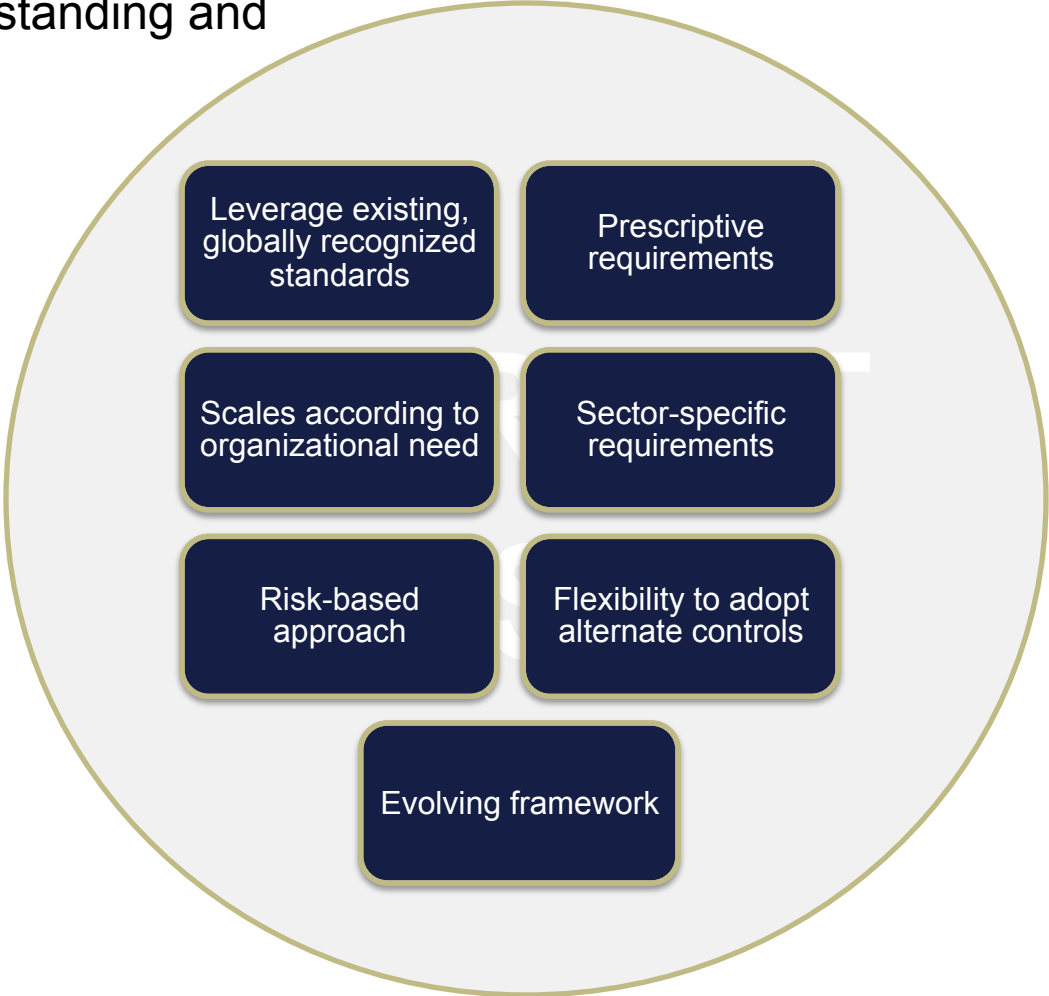


About HITRUST

- The Health Information Alliance (HITRUST) exists to ensure that information security becomes a core pillar of, rather than an obstacle to the broad adoption of health information systems and exchanges
- Formed in August 2007, began operating in October 2007
- Based in Frisco, Texas (suburb of Dallas)
- Legal structure is Limited Liability Company
- Formed as a For Profit, decision to change to Not-For Profit in December 2010
- 3rd major release of Common Security Framework (CSF) in Dec 2010
- First organization obtained CSF Certified status in May 2010

HITRUST Common Security Framework

Certifiable framework to enable common understanding and acceptance



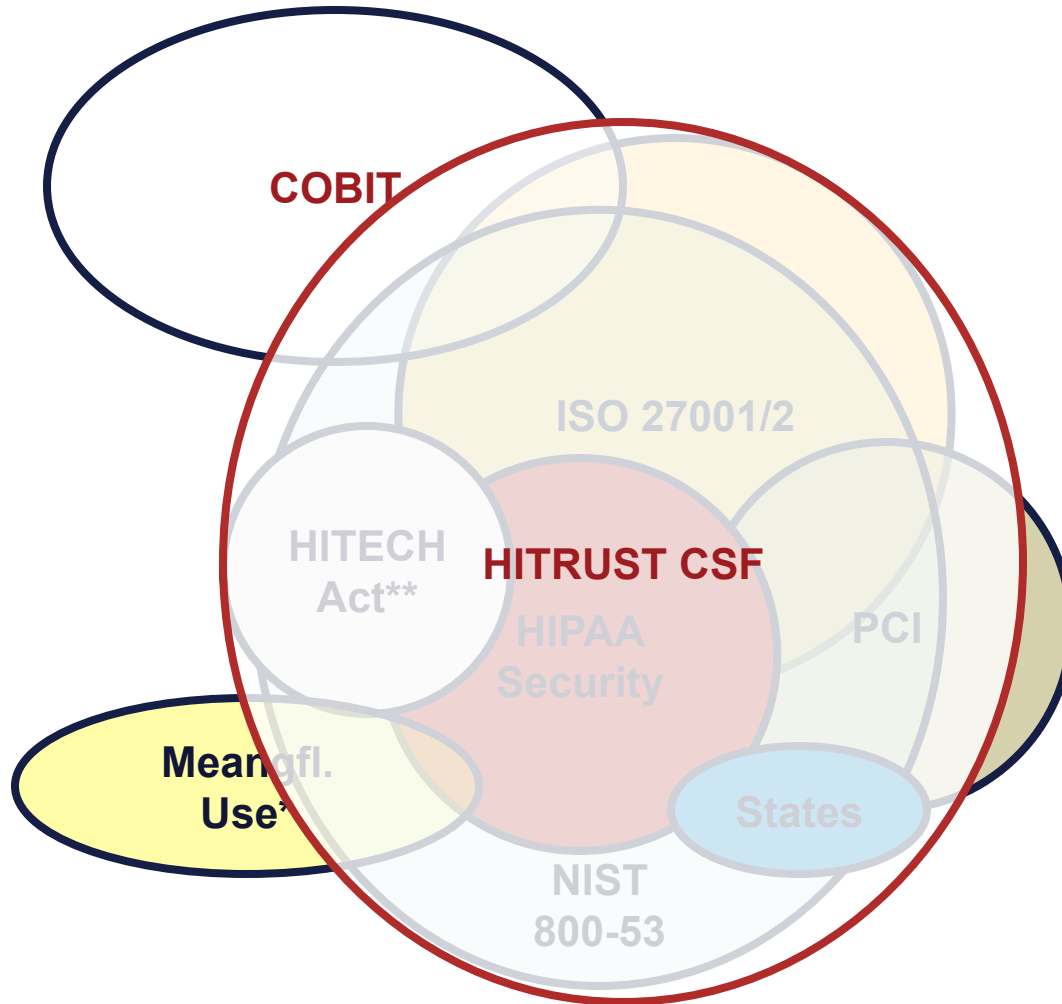
Risk Assessment Methodology (NIST, ISO)



- HITRUST Risk Areas
- Determined based upon analysis of breach data
- Significantly simplified for organizations

- HITRUST Common Security Framework
- Reasonable practice

CSF Standards and Regulations Coverage



CSF Compared with Other Standards

Requirement	CSF	COBIT	PCI	ISO	NIST	HIPAA
Comprehensive – general security	Yes	Yes	Yes	Yes	Yes	Partial
Comprehensive – regulatory, statutory, and business security requirements	Yes	No	No	No	No	No
Prescriptive	Yes	No	Yes	Partial	Yes	No
Practical and scalable	Yes	Yes	No	No	No	Yes
Audit or assessment guidelines	Yes	Yes	Yes	Yes	Yes	No
Certifiable	Yes	Yes	Yes	Yes	No*	No
Support for third-party assurance	Yes	Yes	Yes	Yes	No	No
Open and transparent update process	Yes	No	Yes	Yes	Yes	Yes
Cost	Free	Free	Free	Subsc.	Free	Free

Drivers for Adoption of the CSF

- Strengthening an organization's compliance posture
 - Created, maintained and vetted by experts in consultation with industry
 - Widely adopted
 - Incorporates third party, industry accepted, validation of your security program
- Efficiency of internal security program
 - Leverages globally recognized standards, including HIPAA, HITECH, NIST, ISO, PCI, FTC, COBIT, States and others
 - Lowers costs associated with monitoring and keeping pace with the evolving regulatory environment
- Management of business associates
 - Establishes a commercially reasonable approach to measuring business associates
 - Provides common security baseline and method for communicating security controls between parties

CSF Assurance Program Overview

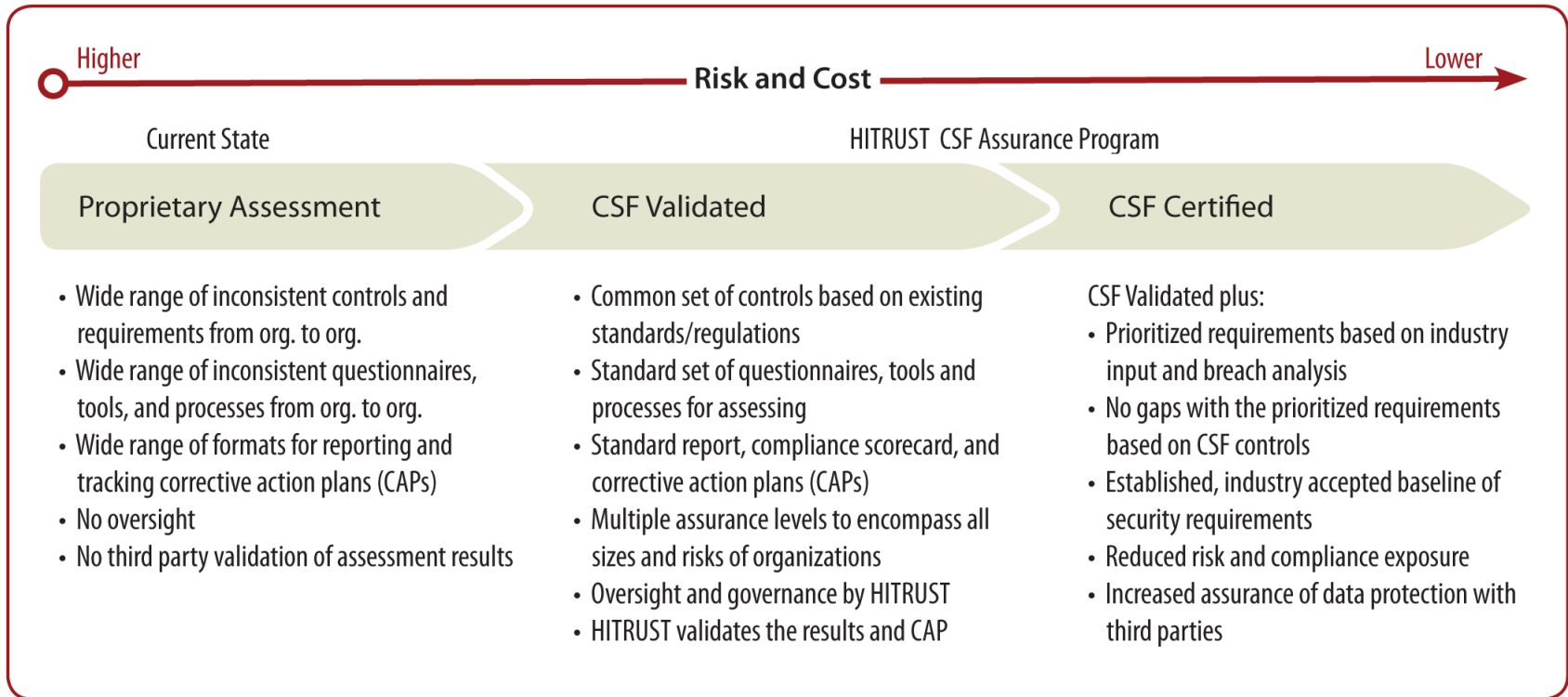
Overview of CSF Assurance Program

HITRUST CSF Assurance Program



- Utilizes a common set of information security requirements with standardized assessment and reporting processes accepted and adopted by healthcare organizations
- Through the program, healthcare organizations and their business associates can improve efficiencies and reduce the number and costs of security assessments
- The oversight and governance provided by HITRUST support a process whereby organizations can trust that their third parties have essential security controls in place

CSF Assurance Program – The Solution



Key Components of CSF Assurance Program

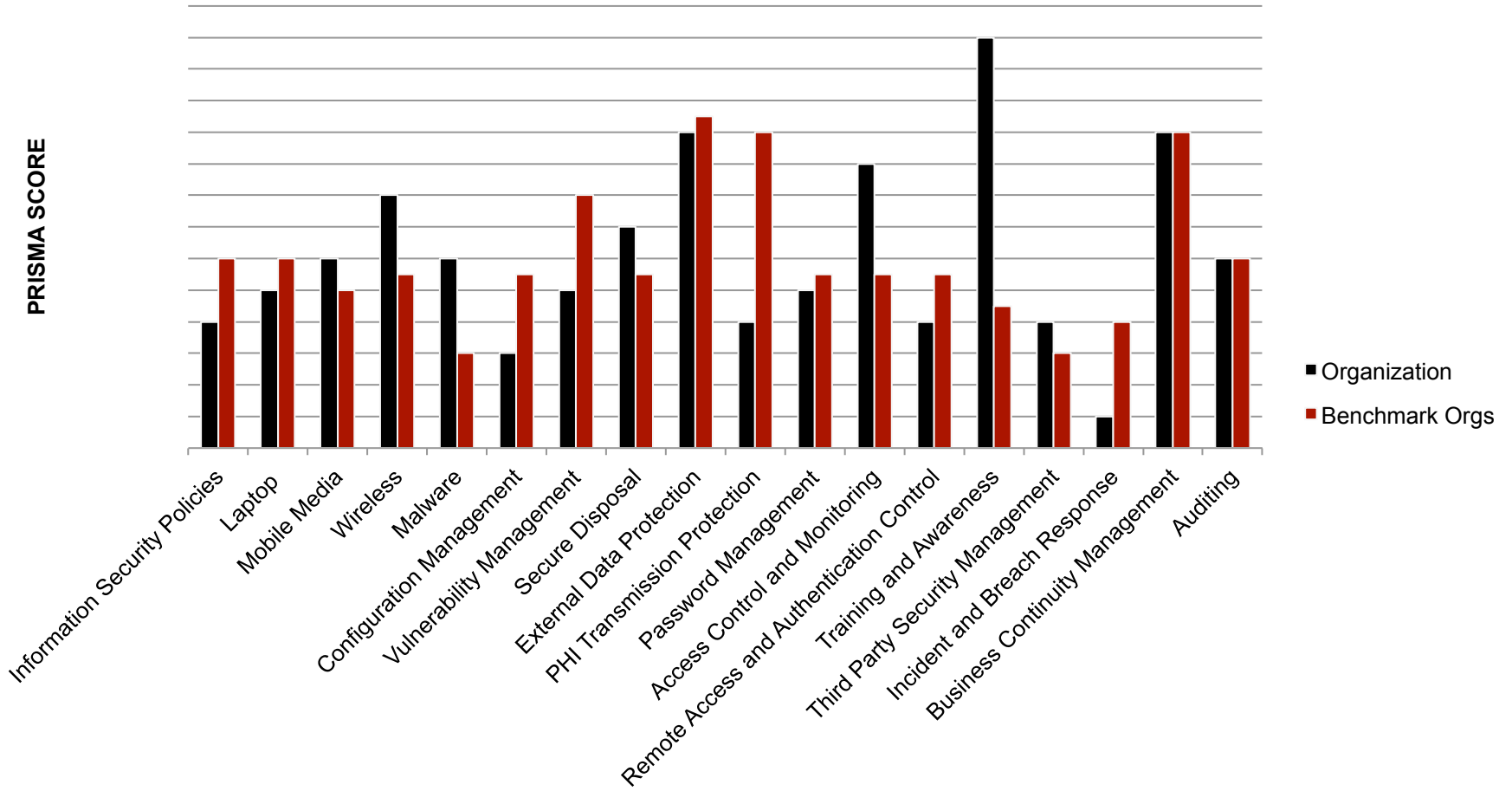
- Standardized tools and processes
 - Questionnaire
 - Worksheet for reporting compliance
 - Report
 - Output that is consistently interpreted across the industry
- Requires use of approved CSF Assessors
- Stringent CSF Assessor requirements
 - Vetting Process
 - Including compliance with our policies, processes and training
 - Ongoing review and oversight
- Cost effective and rigorous assurance
 - Multiple assurance options based on risk
 - Quality control processes to ensure consistent quality and output across CSF Assessors

CSF Assurance Program Deliverables

Table of Contents

1. HITRUST Background
2. Letter of Validation
3. Representation Letter from Management
4. Assessment Context
5. Scope of systems in the assessment
6. Security Program Analysis
7. Overall Security Program Summary
8. Breakdown by CSF Control Areas Required for Certification
9. Compliance Scorecards
10. HIPAA Security Rule
11. Appendix
 - A. Detailed Control Summary of Business Associate (ABC)
 - B. Testing Summary
 - C. Corrective Action Plan
 - D. Questionnaire Results
 - E. System Profile

Benchmark Data



HIPAA Compliance Scorecard

- Standardized output that is consistently interpreted across the industry
- Available for any standard or regulation the CSF maps to (e.g., HIPAA)

HIPAA Security Rule

E. Administrative Safeguard (164.308)	Assigned Security Responsibility	(a)(2) Authority and Responsibility for the Information Security Program	●
	Business Associate Contracts and Other Arrangements	(b)(1) Business associate contracts and other arrangements	●
		(b)(2)(i) Business associate contracts and other arrangements - Covered Entity Exception	●
		(b)(2)(ii) Business associate contracts and other arrangements - Group Health Plan or HMO Exception	●
		(b)(2)(iii) Business associate contracts and other arrangements - Service Agency Exception	●
		(b)(3) Business associate contracts and other arrangements	●
		(b)(4) Written contract or other arrangement (Required)	●
		Contingency Plan	(a)(7)(i) Emergency Response Policies and Procedures
		(a)(7)(ii)(A) Data backup plan (Required)	●
		(a)(7)(ii)(B) Disaster recovery plan (Required)	●
		(a)(7)(ii)(C) Emergency mode operation plan (Required)	●

* Circle is an indication of the level of testing performed.

Going Forward

HITRUST – Information Snap Shot

- Adoption of the CSF
 - Hospitals¹ **62%**
 - Health Plans² **74%**
- Adoption of the CSF Assurance Program
 - Assessments requested of Partners in 2011 **11,000**
- Regional User Group Chapters (monthly) **5**
- CSF Assessors **12**
- HITRUST Central Community Members **5,000+**
- Trained CSF Practitioners³ **200**

1 – Based on facilities in the 2009 AHA hospital and health system data as of Dec 2010

2 – Based on health plans with over 500,000 members as of Dec 2010

3 – Every training class (5 day class) is full through June 2011

Strategic Focus for HITRUST 2011 - 2013

- Continued enhancements to CSF and CSF Assurance Program
- Greater tools to streamline and simplify process
 - Such as CSF Assurance Self Assessment for SMB
- Broader adoption by all providers of CSF and CSF Assurance
 - Chronic, ambulatory, clinic, life sciences
- Greater education and competency of information security personnel
- Greater collaboration at federal and state levels
- Greater collaboration with security software and services vendors
- Analysis and release of summary information on industry progress and trouble areas