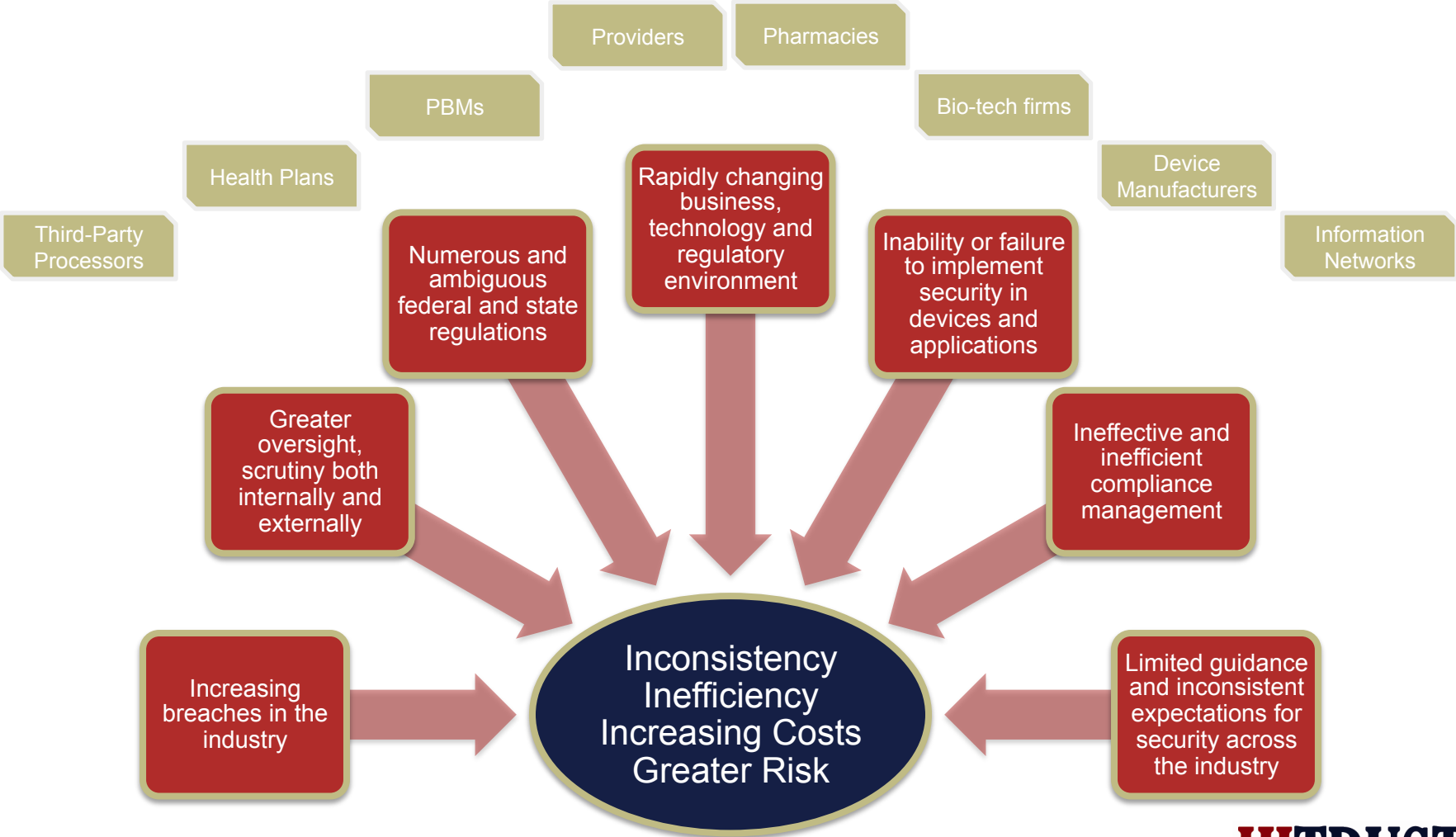


Background

Healthcare Challenges



Confusion with Existing Standards

- The variety of standards and regulations in the healthcare industry introduces ambiguity, inefficiencies, cost and distraction from the complicated business of protecting healthcare organizations.
- The below table denotes how a variety of standards address Access Control.



Standard	Access Control Variations
CPA Firm (SAS 70, SysTrust, SoX)	The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication and authorization mechanisms, linking users and resources with access rules. Such mechanisms should prevent unauthorized personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimize the need for authorized users to use multiple sign-ons. Procedures should also be in place to keep authentication and access mechanisms effective (e.g., regular password changes.)
PCI	Limit access to computing resources and cardholder information to only those individuals whose job requires such access. Identify all users with a unique username before allowing them to access system components or cardholder data.
CCHIT	The system shall enforce the most restrictive set of rights/privileges or accesses needed by users/groups (e.g. System administration, Clerical, Nurse, Doctor, etc.), or processes acting on behalf of users, for the performance of specified tasks.
ISO	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. The allocation and use of privileges shall be restricted and controlled.
URAC	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.
HITSP	Access Control is managed (created, modified, deleted, suspended, or restored, and provisioned based on defined rules and attributes). Data access policy is enforced. User data are located by an entity with the ability (privileges) to search across systems. Protected data are accessed based on access control decisions information attributes for data access. Select protected data are blocked from users otherwise authorized to access the information resource.
NIST	A subject can execute a transaction only if the subject has selected or been assigned a role. The identification and authentication process (e.g. login) is not considered a transaction. All other user activities on the system are conducted through transactions. Thus all active users are required to have some active role. A subject's active role must be authorized for the subject. With (1) above, this rule ensures that users can take on only roles for which they are authorized. A subject can execute a transaction only if the transaction is authorized through the subject's role memberships, and subject to any constraints that may be applied across users, roles, and permissions. This rule ensures that users can execute only transactions for which they are authorized.
COBIT	The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication and authorization mechanisms, linking users and resources with access rules. Such mechanisms should prevent unauthorized personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimize the need for authorized users to use multiple sign-ons. Procedures should also be in place to keep authentication and access mechanisms effective (e.g., regular password changes).
ITIL	Access Management is effectively the execution of both Availability and Information Security Management, in that it enables the organization to manage the confidentiality, availability and integrity of the organization's data and intellectual property. Access Management ensures that users are given the right to use a service, but it does not ensure that this access is available at all agreed times - this is provided by Availability Management.
HIPAA	Implement policies and procedures for granting access to electronic PHI through access to a workstation, transaction, program, process or other mechanism. Implement policies and procedures that based upon the entity's access authorization policies, establish, document, review, and modify a user right of access to a workstation, transaction, program or process.

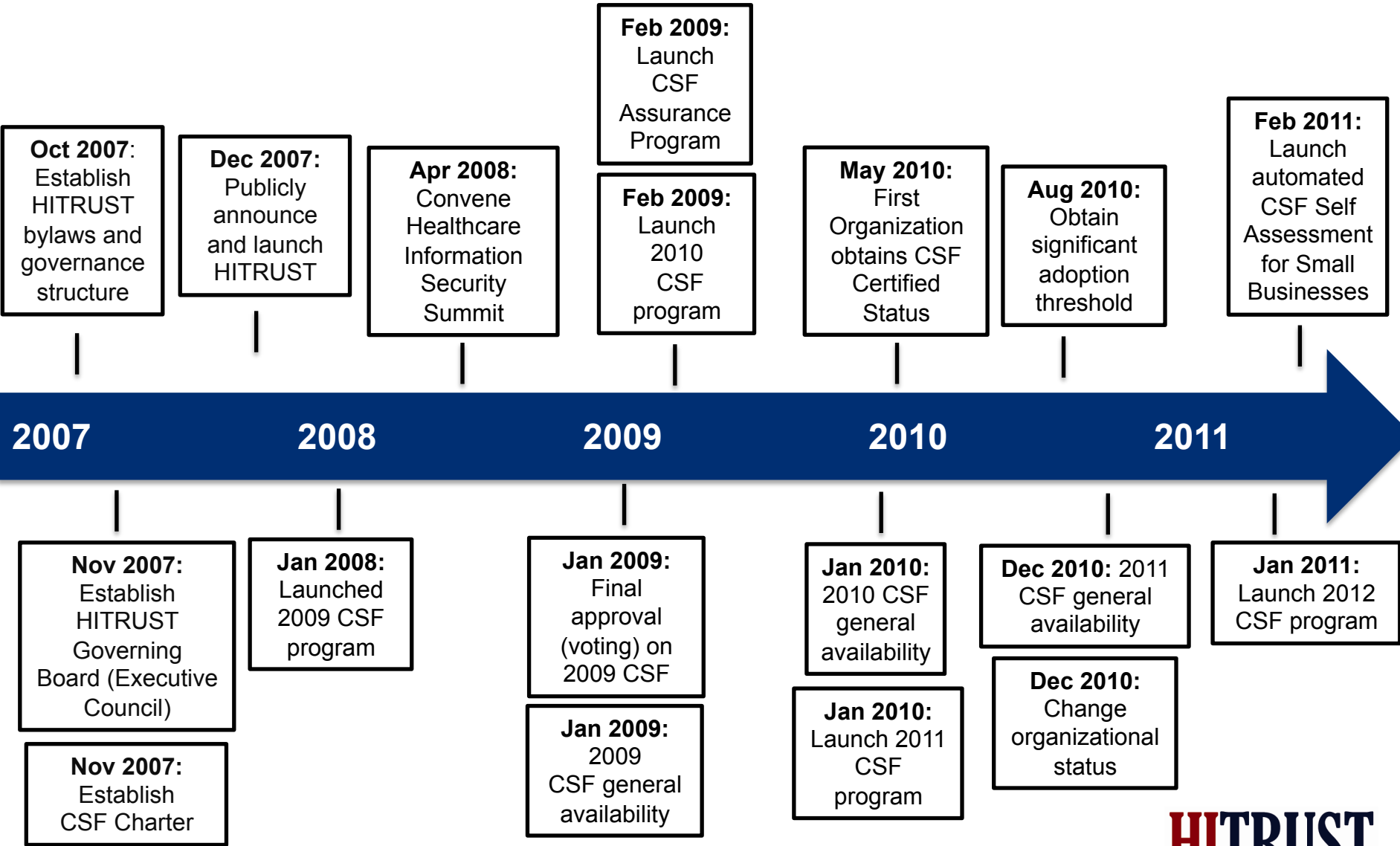
About HITRUST

- 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—Mission and Goals

- To collaborate with healthcare, business, technology and information security leaders, who are united by the belief that standardizing a higher level of security will build greater trust in the electronic flow of information through the healthcare system
- To increase trust in the way health information is safeguarded, while reducing the complexities and managing the costs
 - Lower costs
 - Reduce risk
 - Increase efficiency
 - Reduce complexity
- Establish a fundamental and holistic change in the way the healthcare industry manages information security risks
- Enhance the competency and role of information security professionals

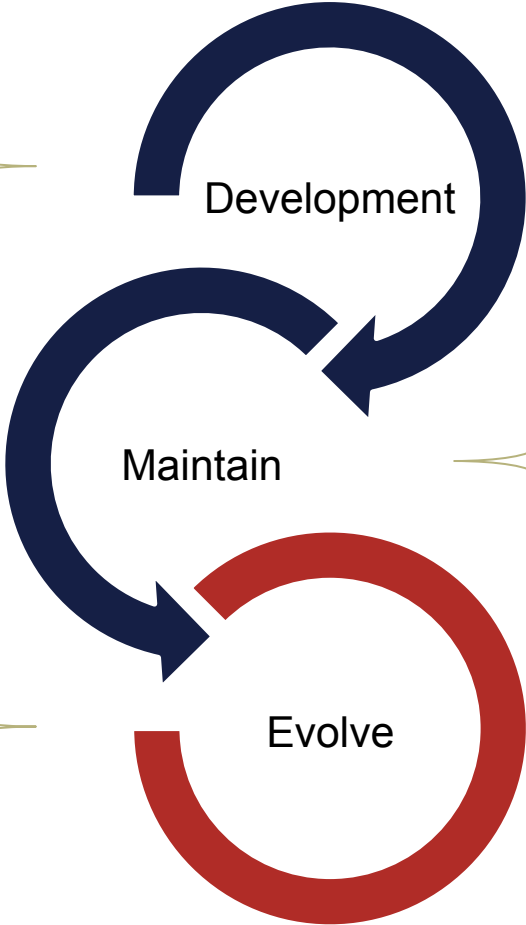
Major Organizational Milestones and Accomplishments



HITRUST – Continuously Evolving

- CSF
- CSF Assurance Program
- CSF Toolkit
- CSF Training program
- CSF Small Practice Assessment

- Address evolving topics such as portable devices, cloud computing and HIEs
- Add new technical functionality to on-line CSF version
- Adjust CSF based on analysis of breach data for the industry
- Adjust CSF based on industry feedback
- Annual updates of significant content changes (e.g., CMS requirements)
- Support for additional sectors (e.g., home health and life sciences)



- Quarterly updates based on regulatory changes
- Over 150 experienced security professionals trained in CSF and healthcare security
- Benchmark data

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

CSF Overview

HITRUST Common Security Framework

Certifiable framework to enable common understanding and acceptance



Risk Assessment Methodology (NIST, ISO)



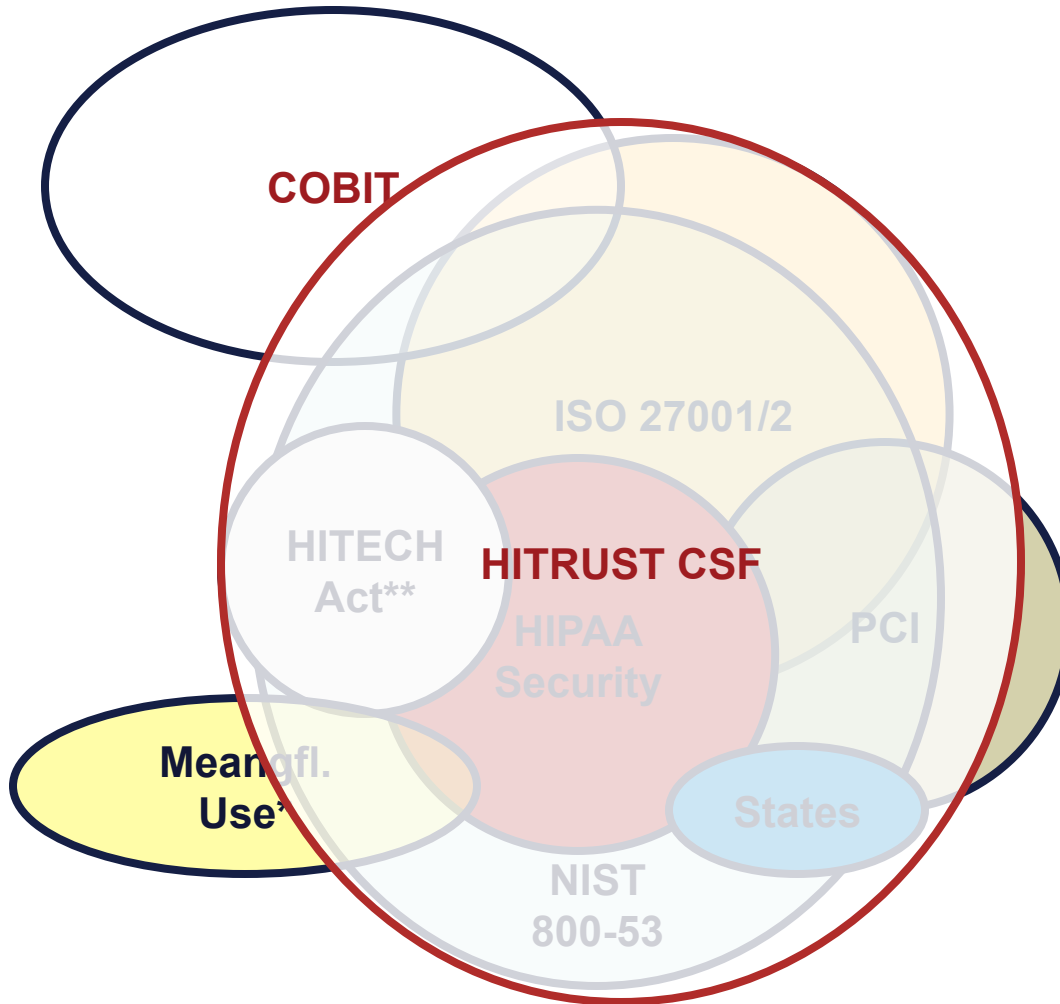
- HITRUST Risk Areas
- Determined based upon analysis of breach data
- Significantly simplified for organizations

- HITRUST Common Security Framework
- Reasonable practice

CSF – Leverages Federal Standards

Federally Recognized Guidance	HITRUST CSF 2011
<p>NIST SP 800-53: Recommended Security Controls for Federal Information Systems</p>	<p>Controls of NIST SP 800-53 are cross-referenced with the CSF.</p> <p>HITRUST CSF’s implementation requirements address those of NIST SP 800-53.</p>
<p>FIPS 199: Standards for Security Categorization of Federal Information and Information Systems</p>	<p>Risk-based approach by applying security controls and requirements based on defined risk factors specific to the organization or system</p>
<p>NIST SP 800-30: Risk Management Guide for Information Technology Systems</p>	<p>CSF leverages the key concepts using differing levels of requirements: FIPS (NIST) specifies LOW, MOD, HIGH; CSF specifies Levels 1, 2, and 3.</p>
<p>NISTIR 7358 standard - Program Review for Information Security Management Assistance (PRISMA)</p>	<p>HITRUST CSF Assurance Program leverages the concepts and rating scheme of PRISMA, which serves an indicator of an organization’s ability to protect information in a sustainable manner.</p>
<p>SANS Top 20 Critical Security Controls</p>	<p>The CSF Assurance Program including our Validation/Certification assessment designations follow a phased approach. The initial requirements are a subset of the CSF’s security control requirements that relate to the greatest number of breaches or greatest loss of PHI. These requirements are based on actual breach data supplemented by expert opinion.</p>

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

Spectrum of CSF Adopters

Minimum Compliance Requirements

HIPAA, HITECH

Example Entity Types

- Physician practice
- Hospital
- Transcription company
- Home health

Moderate Compliance Requirements

HIPAA, HITECH, PCI, Non-healthcare customers

Example Entity Types

- Health Plans
- PBMs
- Multi-state health systems

Complex Compliance Requirements

HIPAA, HITECH, PCI, SOX, International Operations, CMS, FISMA

Example Entity Types

- Large for profit health systems
- Medicare Contractors
- PBM for Federal Agencies

Drivers for Adoption of the CSF

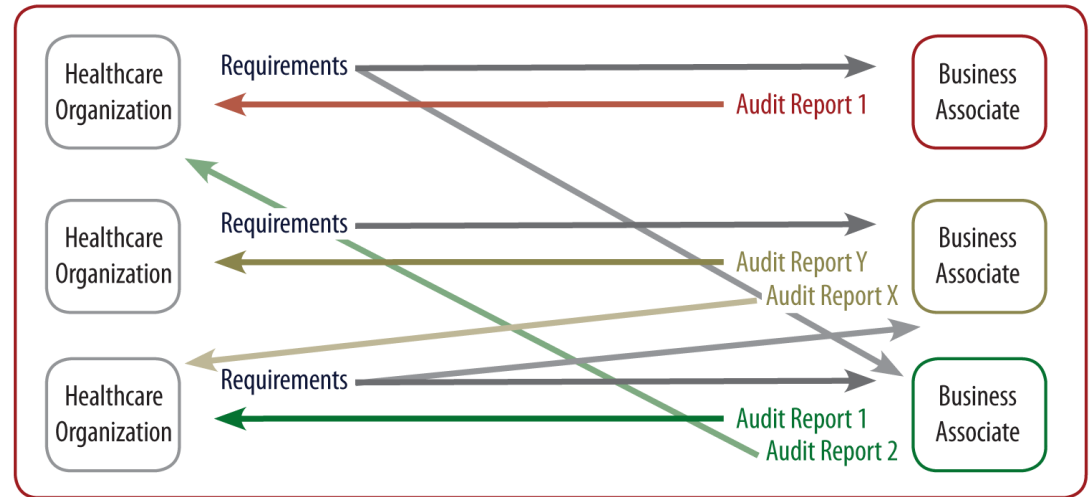
- Strengthening an organization's compliance posture
 - Created, maintained and vetted by experts in consultation with industry
 - Widely adopted
 - Incorporates third party, industry accepted, validation of your security program
- Efficiency of internal security program
 - Leverages globally recognized 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

HITRUST CSF Assurance Program – The Need

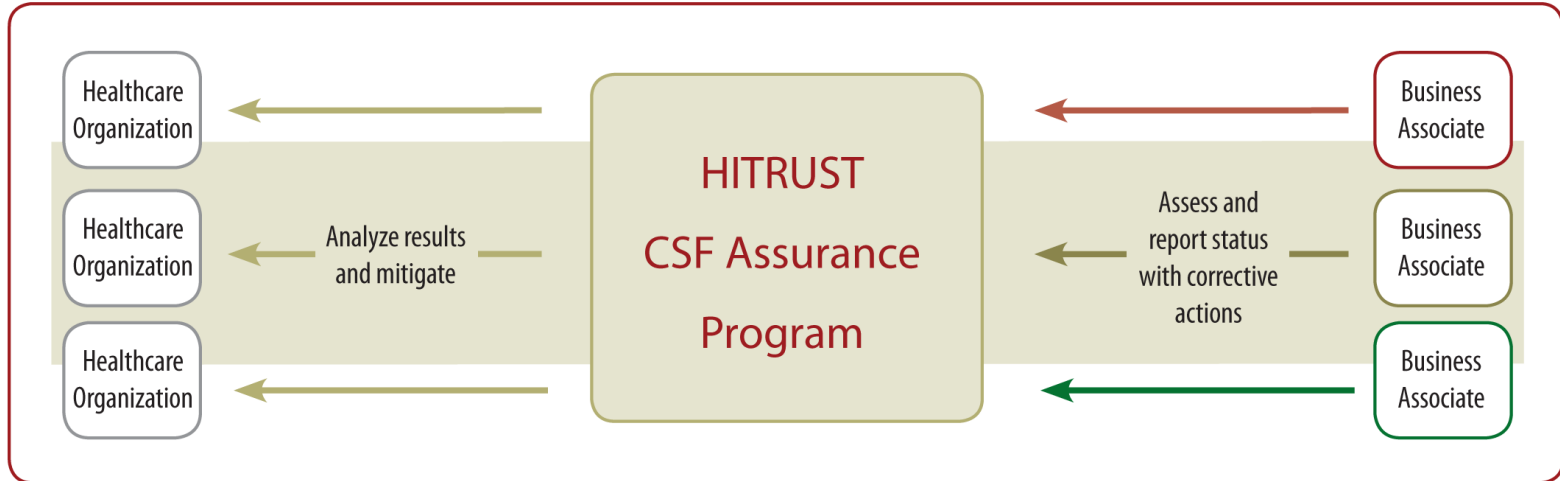
- Organizations facing multiple and varied assurance requirements from a variety of parties
- Increasing pressure and penalties associated with enforcement efforts of HIPAA/HITECH
- Inordinate level of effort being spent on the negotiation of requirements, data collection, assessment and reporting

Current state of reporting



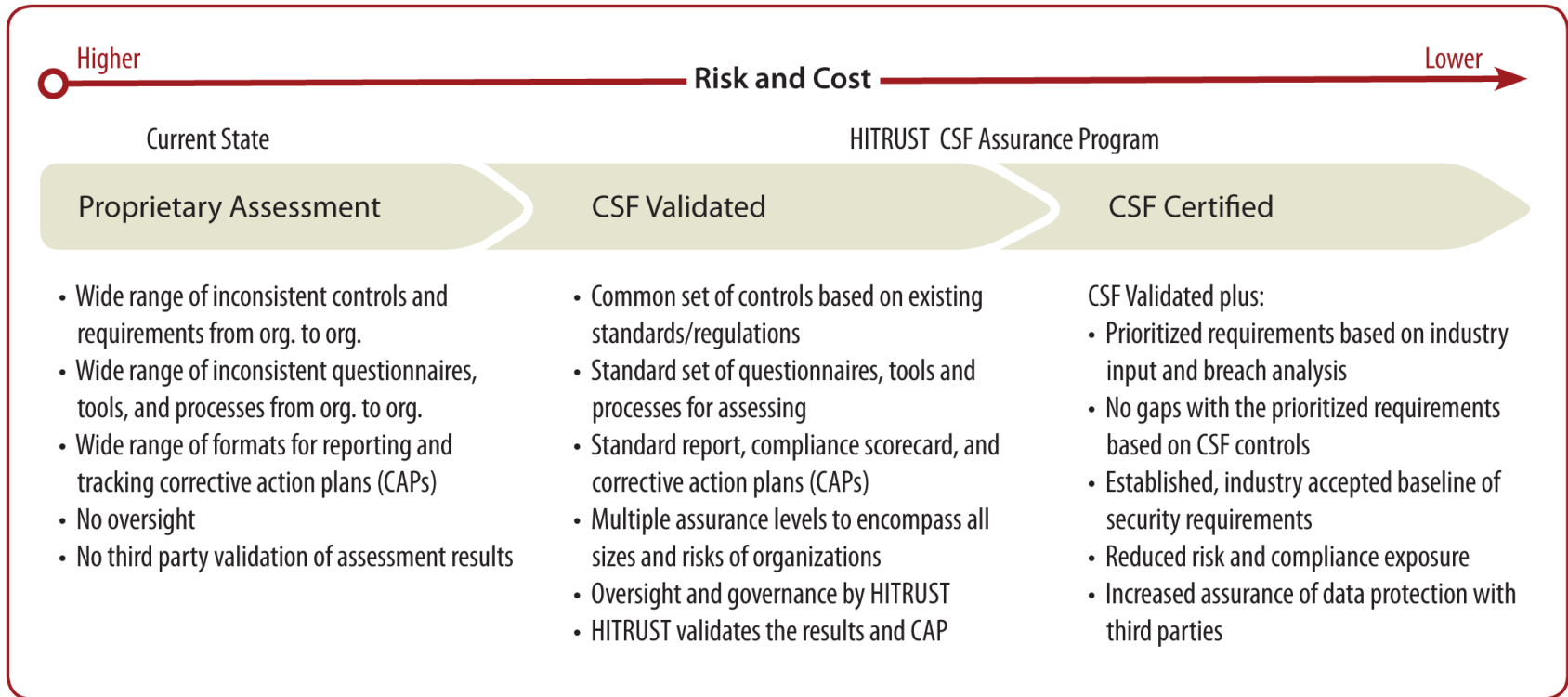
Overview of CSF Assurance Program

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

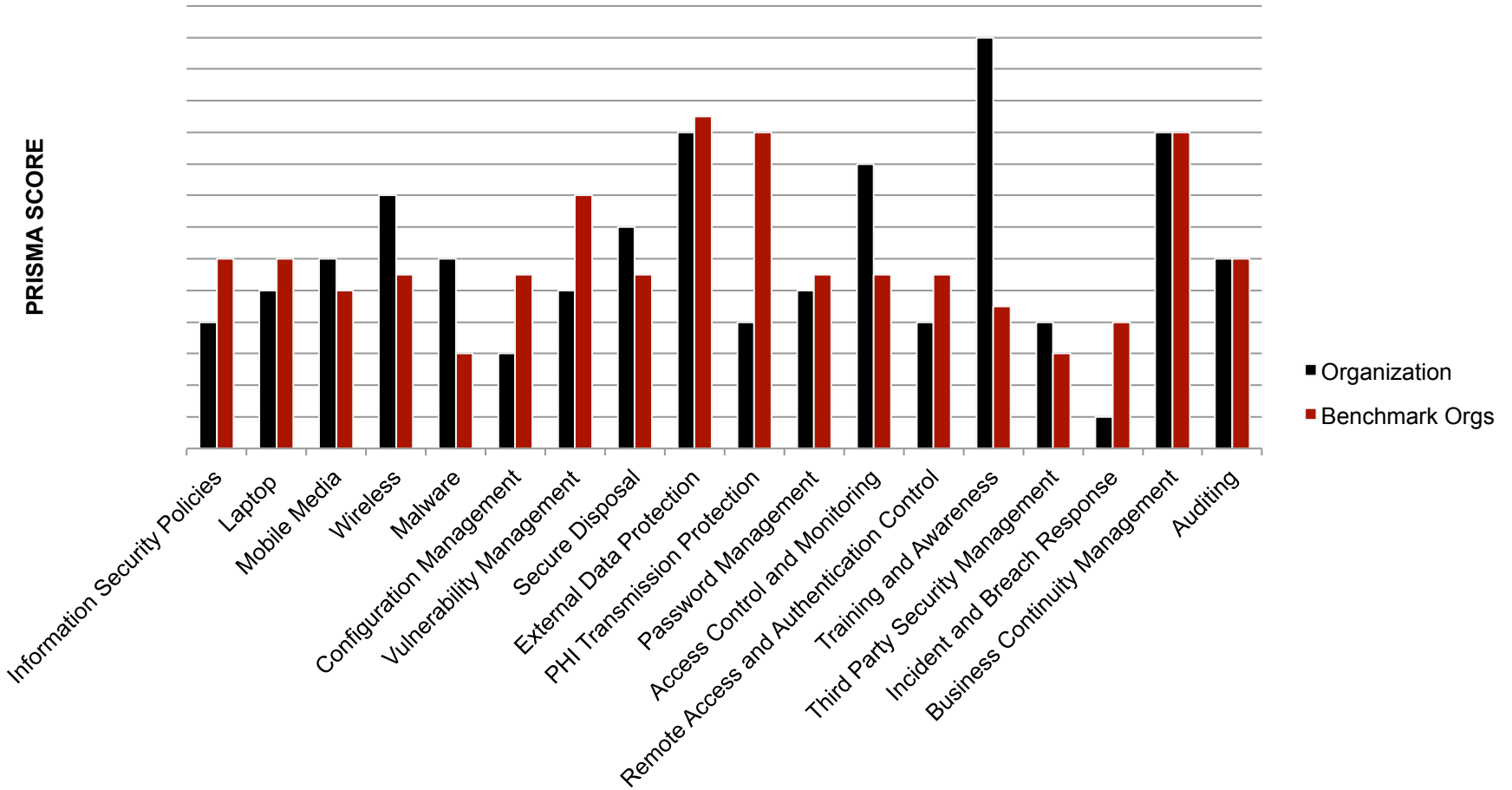
- Standardized tools and processes
 - Questionnaire
 - Worksheet for reporting compliance
 - Report
 - Output that is consistently interpreted across the industry
- Requires use of approved CSF Assessors
- Stringent CSF Assessor requirements
 - Vetting Process
 - Including compliance with our policies, 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

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