# HITRUST CSF Assurance Program

## Simplifying the information protection of healthcare data

May 2015

# Table of Contents







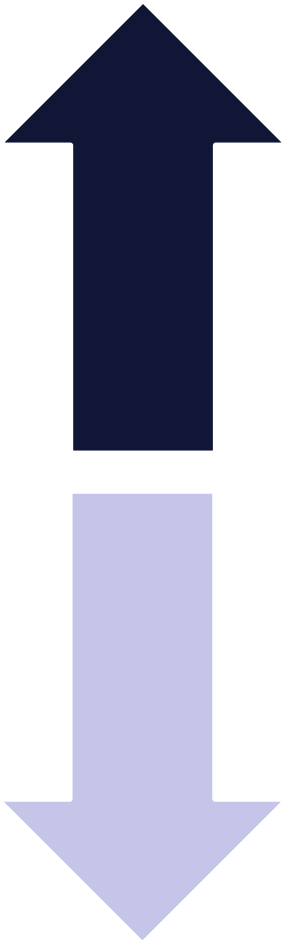
HITRUST
Health Information Trust Alliance

# Background

# Current Environment

Security and privacy challenges will hamper industry initiatives

- Cost and complexity of compliance
- Increasing threats locally and abroad
- Lack of progress made by the industry on addressing fundamental exposures



Industry objectives

- Broad adoption of health IT to improve healthcare quality and the efficiency of care provision

Security regulation and adoption

- Increasing costs around managing and reporting against compliance requirements
- Increasing exposure to broad scale and significant healthcare breaches





HITRUST
Health Information Trust Alliance

# Industry Challenges as Catalyst for HITRUST (Circa 2007)

In 2007, healthcare organizations faced multiple challenges with regards to information security:

- Costs and complexities of redundant and inconsistent requirements and standards
- Confusion around implementation and acceptable baseline controls
- Information security audits subject to different interpretations of control objectives and safeguards
- Increasing scrutiny and similar queries from regulators, auditors, underwriters, customers and business partners
- Growing risk and liability associated with information protection
- Lack of educational resources available to health information security professionals






HITRUST
Health Information Trust Alliance

# Confusion with Existing Standards (Circa 2007)

The multitude of standards and regulations in the healthcare industry introduces ambiguity, inefficiencies, cost and distraction from the complicated business of protecting healthcare organizations

The corresponding 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 administrator, 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 membership, 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. |



HITRUST
Health Information Trust Alliance

# HITRUST Mission and Objectives

In 2007, the Health Information Trust Alliance or HITRUST was formed by a group of concerned healthcare organizations out of the belief improvements in the state of information security and privacy in the industry are critical to the broad adoption, utilization and confidence in health information systems, medical technologies and electronic exchanges of health information, all of which are necessary to improve the quality of patient care while lowering the cost of healthcare delivery.

Key focus:

- Increase the protection of protected health and other sensitive information
- Mitigate and aid in the management of risk associated with health information
- Contain and manage costs associated with appropriately protecting sensitive information
- Increase consumer and governments' confidence in the industry's ability to safeguard health information
- Address increasing concerns associated with business associate and 3rd party privacy, security and compliance
- Work with federal and state governments and agencies and other oversight bodies to collaborate with industry on information protection
- Facilitate sharing and collaboration relating to information protection amongst and between healthcare organizations of varying types and sizes
- Enhance and mature the knowledge and competency of health information protection professionals

# HITRUST CSF

Framework that normalizes the security requirements of healthcare organizations, including federal (e.g., HITECH Act and HIPAA), state (e.g., MA 201 CMR 17.00), third party (e.g., PCI and COBIT) and government (e.g., NIST, FTC and CMS)

- HIPAA is not prescriptive, which makes it difficult to apply and open to interpretation. It is also not the only set of security requirements a healthcare organization will need to address (e.g., PCI, state or business partner requirements)
- Organizations will need to reference additional standards for specific guidance on requirements specified by HIPAA

Built to simplify these issues by providing direction for security tailored for the needs of the organization

The only framework that is built to provide scalable security requirements based on the different risks and exposures of organizations in the industry

Makes security manageable and practical by prioritizing one-third of the controls in the CSF as a starting point for organizations. Priorities are based on industry input and analysis of breach information in the industry

No other relevant resource for healthcare organizations to reference for prioritizing their initiatives and validating their investments in security

# CSF Assurance Program Overview

# Overview of CSF Assurance Program

Organizations face multiple and varied assurance requirements from a variety of parties, including increased pressure and penalties associated with HHS enforcement efforts and an inordinate level of effort on negotiation of requirements, data collection, assessment and reporting.


**The HITRUST CSF Assurance Program provides:**

- A risk-based approach to selecting controls for assessment and formal certification
- A common, standardized methodology to effectively and consistently measure compliance and risk
  - Simplified information collection and reporting
  - Consistent testing procedures and scoring
  - Demonstrable efficiencies and cost-containment
- Assessments performed by qualified professional services firms – CSF Assessors

# Strategic Objectives of CSF Assurance Program

Provide assurance that controls to limit the exposure of a breach are in place and operating effectively. Recipients of this assurance include:

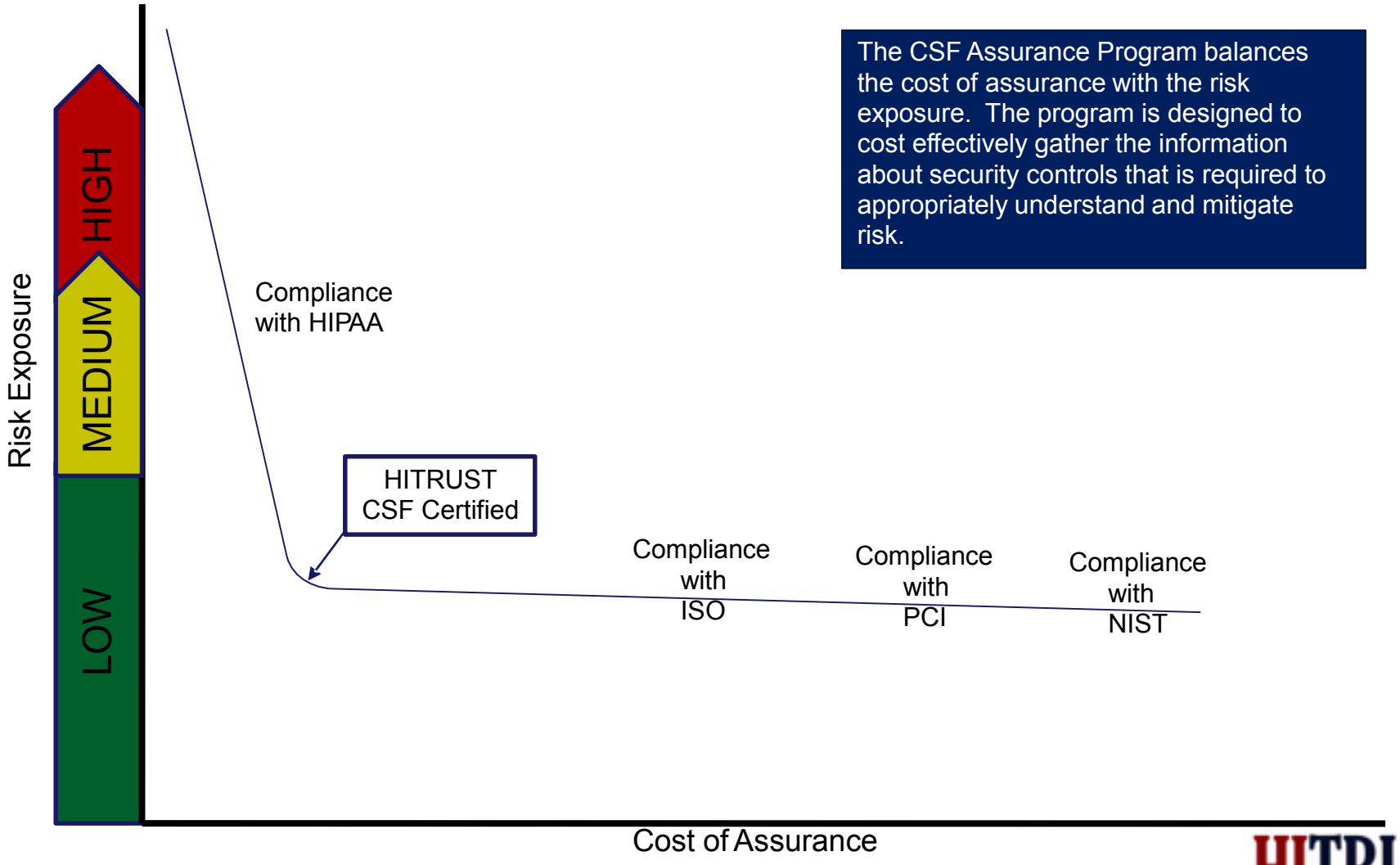
- Executive management
- Auditors
- Federal and state regulators
- Customers of business associates

Simplify compliance efforts for organizations

- Assess once and report to many constituents:
  - Federal (e.g., HIPAA/HITECH or meaningful use information) and state regulators
  - Credit card companies (i.e., PCI requirements)
  - CMS (i.e., Core Security Requirements)
  - Internal or external auditors
- Comprehensively leverage assessments (i.e., internal audit work, other certifications such as PCI and SOC 1/2 reports to streamline audits and testing)

Provide this assurance in a more cost-effective manner with additional rigor than existing processes

# Varying Costs of Assurance




The CSF Assurance Program balances the cost of assurance with the risk exposure. The program is designed to cost effectively gather the information about security controls that is required to appropriately understand and mitigate risk.

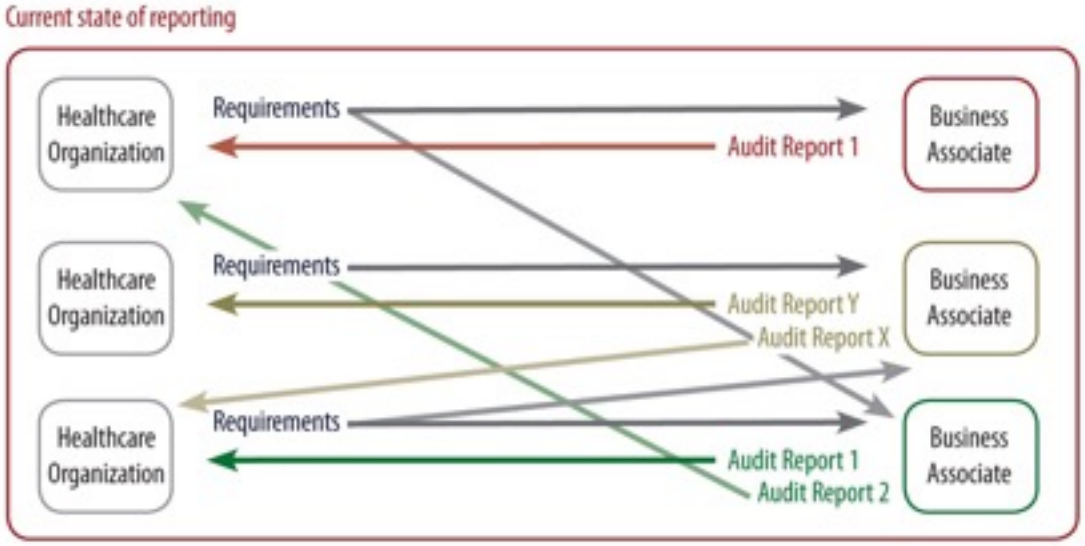




HITRUST
Health Information Trust Alliance

# HITRUST CSF Assurance Program – The Need

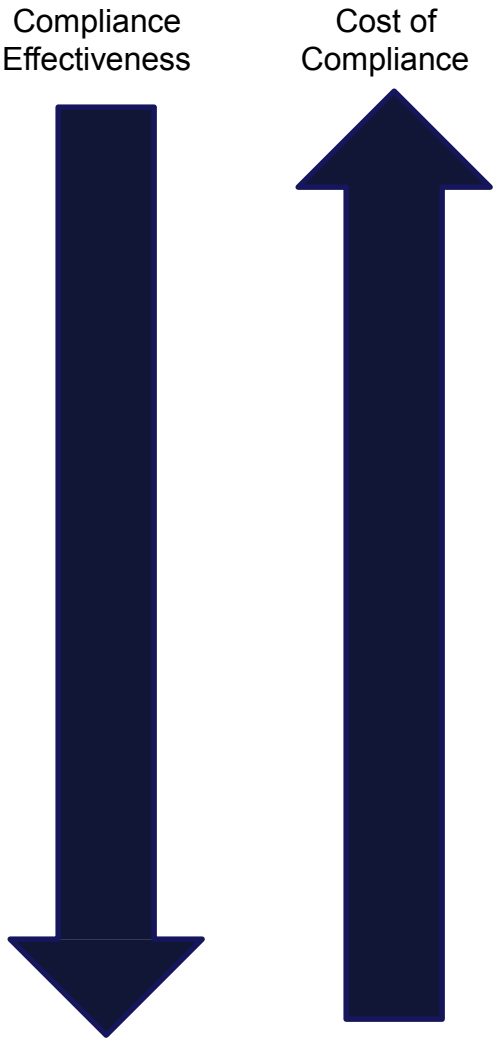
- Organizations facing multiple and varied assurance requirements from a variety of parties
- Increasing pressure and penalties associated with enforcement efforts of HIPAA/HITECH
- Inordinate level of effort being spent on the negotiation of requirements, data collection, assessment and reporting



# Compliance Challenges

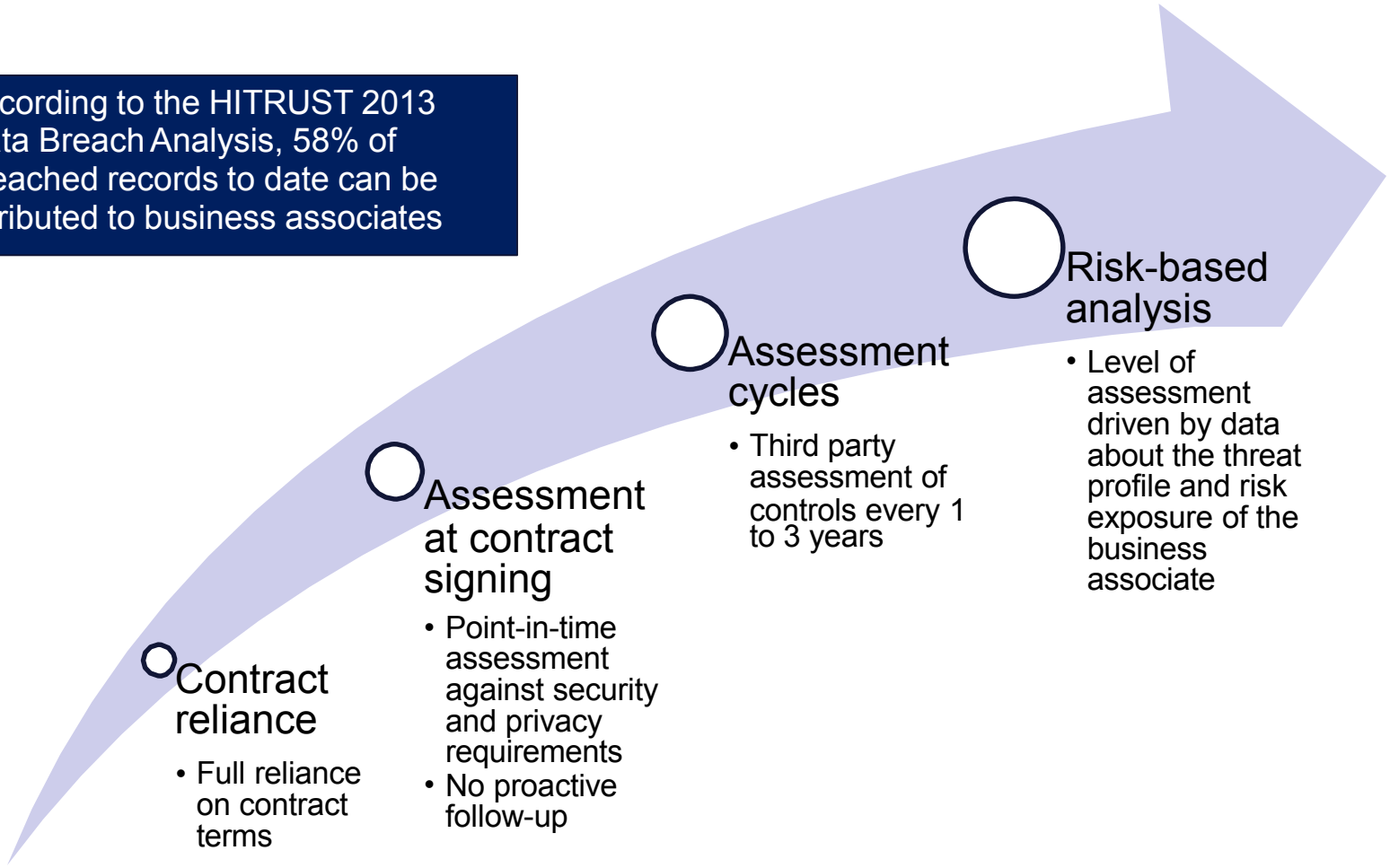
# Compliance Challenges

- Organizations have a responsibility to ensure information shared with business associates (BAs) is appropriately protected
- Organizations in healthcare are spending increasingly more on BA compliance while overall confidence in the effectiveness of these compliance efforts is decreasing
- Increased organizational exposure to breaches or data leaks originating with BA
  - Emergence of health information exchanges and evolving business relationships globally is increasing the number of BAs and volume of shared data
  - BA downstream relationships increase complexity and risk
  - Greater regulatory requirements and scrutiny
  - Inadequate organizational resources
  - Lack of a standard industry approach



# Broad Spectrum of Industry Practices

According to the HITRUST 2013 Data Breach Analysis, 58% of breached records to date can be attributed to business associates








HITRUST
Health Information Trust Alliance

# Existing Issues for Covered Entities

- Complex contracting process due to unique security requirements
- Low response rate of questionnaires
- Inaccurate and incomplete responses
- Inadequate due diligence of questionnaires
- Difficulty monitoring the status and effectiveness of corrective action plans
- Difficulty tracking down appropriate contacts at business associate
- Costly and time-intensive data collection, assessment and reporting processes
- Inability to proactively identify and track risk exposures at business associate
- Lack of visibility into downstream risks related to business associate (i.e., business associate's own business partners)
- Lack of consistent reporting to management on business associate risks

# Existing Issues for Business Associates

- Complex contracting process due to unique security requirements
- Broad range and inconsistent expectations for responses to questionnaires – inability to effectively leverage responses across organizations
- Complex processes:
  - Maintaining broad range of reporting requirements
  - Tracking to varied expectations around corrective action plans
  - Tracking down appropriate contacts at customers
  - Expensive and time-intensive audits by customers
  - Inability to consistently and effectively report to and communicate with customers
  - Risk exposure to inconsistent responses from different business units of the business associate

# 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

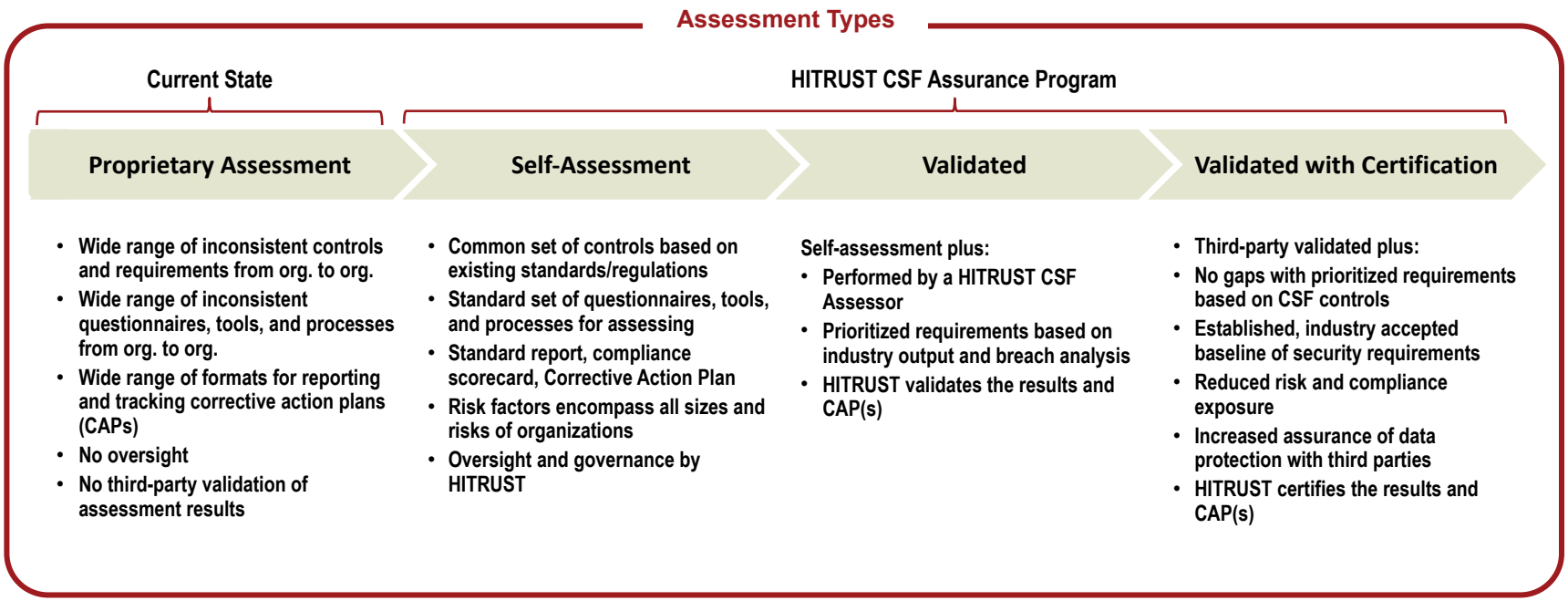
- Leverages globally recognized standards, including HIPAA, HITECH, NIST, ISO, PCI, FTC , COBIT, States and others
- Lowers costs associated with monitoring and keeping pace with the evolving regulatory environment

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

# Key Components of the CSF Assurance Program

# CSF Assurance Program – The Solution



# Key Components of CSF Assurance Program

Standardized tools and processes

- Questionnaire
  - Focus assurance dollars to efficiently assess risk exposure
  - Measured approach based on risk and compliance
  - Ability to escalate assurance level based on risk
- Report
  - Output that is consistently interpreted across the industry

Cost effective and rigorous assurance

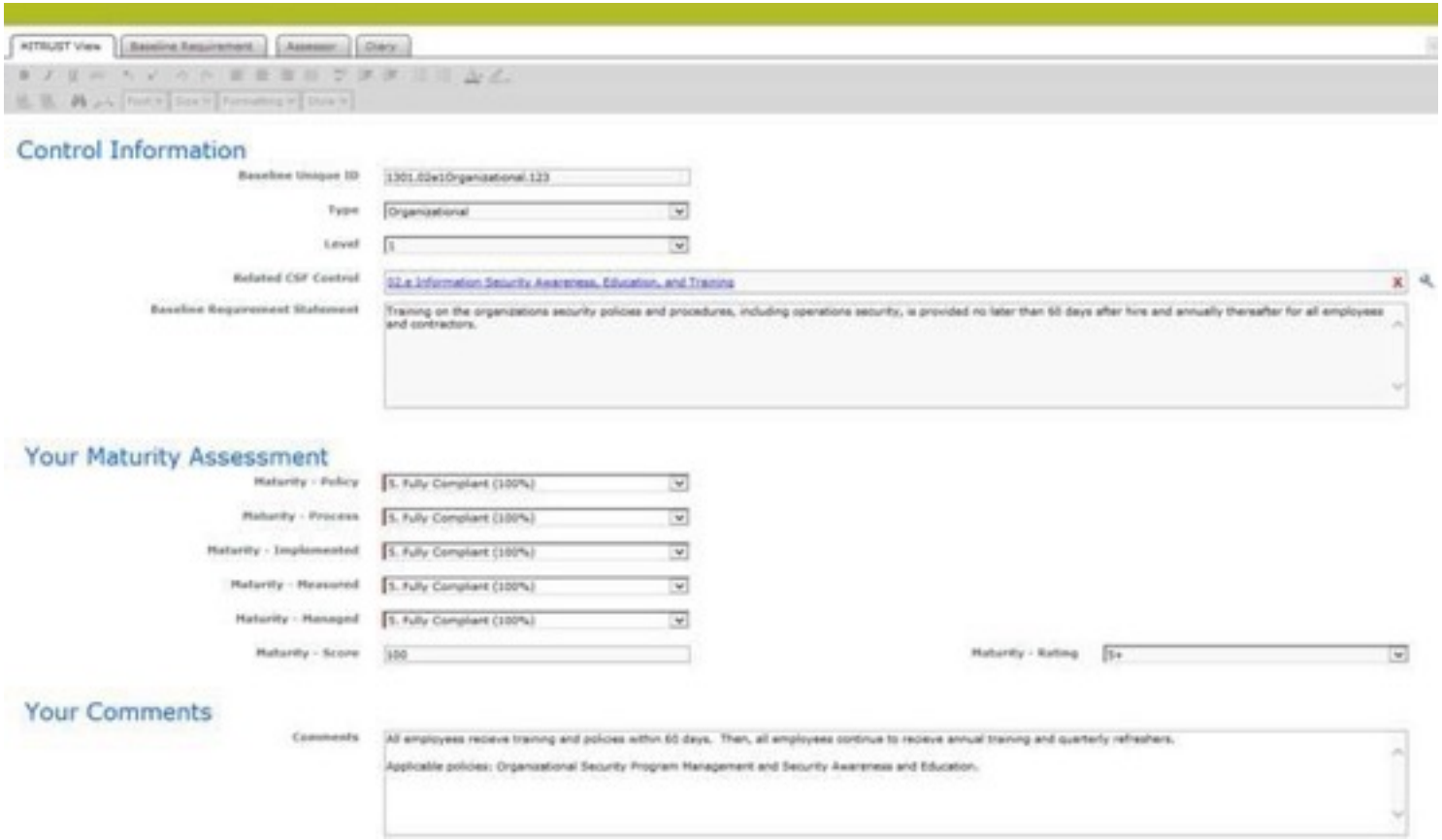
- Multiple assurance options based on risk
- Quality control processes to ensure consistent quality and output across CSF Assessors

# Questionnaire

Assessment Questionnaire:

- Innovative approach to assess the quality of information protection practices in an efficient manner
- Focus on the security capabilities and outcomes of an organization
- Leverages key measures and benchmarking
- Structured according to the high-risk areas identified in the CSF, which reflect the controls required to mitigate the most common sources of breaches for the industry

# Questionnaire








HITRUST
Health Information Trust Alliance

# Report

Standardized output that is consistently interpreted across the industry

Characteristics of HITRUST reporting:

- Consistent representation of risk exposure, compliance posture and corrective actions
- Benchmarking of results against security practices at similar organizations in the industry

| | | | |
|---|---|---|---|
| Security Awareness and Training | (a)(5)(i) Security Awareness Program | 3 | ○ |
| | (a)(5)(ii)(A) Security reminders (Addressable) | 3 | ○ |
| | (a)(5)(ii)(B) Protection from malicious software (Addressable) | 3 | ○ |
| | (a)(5)(ii)(C) Log-in monitoring (Addressable) | 3 | ○ |
| | (a)(5)(ii)(D) Password management (Addressable) | 3 | ○ |
| Security Incident Procedures | (a)(6)(i) Incident Response Policies and Procedures | 3 | ○ |
| | (a)(6)(ii) Response and Reporting (Required) | 3+ | ○ |
| Security Management process | (a)(1)(i) Security Policy Implementation | 3 | ● |
| | (a)(1)(ii)(A) Risk analysis (Required) | 3 | ● |
| | (a)(1)(ii)(B) Risk management (Required) | 3 | ○ |
| | (a)(1)(ii)(C) Sanction policy (Required) | 3+ | ● |
| | (a)(1)(ii)(D) Information system activity review (Required) | 3- | ○ |
| Workforce Security | (a)(3)(i) Access Control Policies and Procedures | 3 | ○ |
| | (a)(3)(ii)(A) Authorization and/or supervision (Addressable) | 3 | ○ |





HITRUST
Health Information Trust Alliance

# Assurance

Multiple assurance options based on risk:

- Self Assessment
- On-site assessment conducted by a CSF Assessor that includes testing and the review of system configurations, physical walk-throughs, interviews with key personnel, and the review of organization charts, policies, procedures and other third-party testing that may have recently been conducted at the organization

# Assurance

HITRUST quality control:

- Stringent approval process for CSF Assessor organization and regular reviews
- CSF Assessor training requirements
- Experienced HITRUST reviewers
  - Conduct review of CSF submission package
  - Prepare and issue report

# Participating in the CSF Assurance Program

# Participating in the CSF Assurance Program – Organizations/Covered Entities

Four steps to getting started with the CSF Assurance program:

1. Select “publicly available downloads” under the “Downloads” tab on the HITRUST website and click the “CSF Assurance & Related Programs” icon for more detailed information
2. Insert language into your business associate contracts that requires assurance around information protection
3. Require your business associates to provide you with a Self Assessment, CSF Validated, or CSF Certified Assessment Report
4. Make known publicly your participation in CSF Assurance program so as to help drive down compliance costs for the industry

# Participating in the CSF Assurance Program – Internally or to share with Customers as a BA

Three steps to getting started with the CSF Assurance program:

1. Download the CSF and understand the requirements

2. Perform a readiness assessment and consider:
   a. Licensing MyCSF to help with the assessment,
   b. Attending HITRUST CSF training
   c. Using a CSF Practitioner to assist with fixing any gaps

3. Engage a CSF Assessor Organization to perform a Validated Assessment

# CSF Assurance Related Costs

- Program related costs are a function of assessment fees
- No remediation is required for CSF Validated
- Costs for remediating control weaknesses related to CSF Certified will vary based on each organization's circumstances
- Assessments costs:
  - Validated Assessment Processing fee $3,750 - $7,500 (sliding scale based on total organization revenue)
  - Third-party on-site assessment of controls – varies based on size and complexity
  - Optional MyCSF subscription starting at $10K per year

# For More Information

**For more information on the CSF Assurance Program visit:**
www.HITRUSTAlliance.net/csf-assurance/

**For a list of HITRUST CSF Assessors visit:**
http://www.hitrustalliance.net/csf-assessors/

**For assistance, contact:**
info@HITRUSTalliance.net