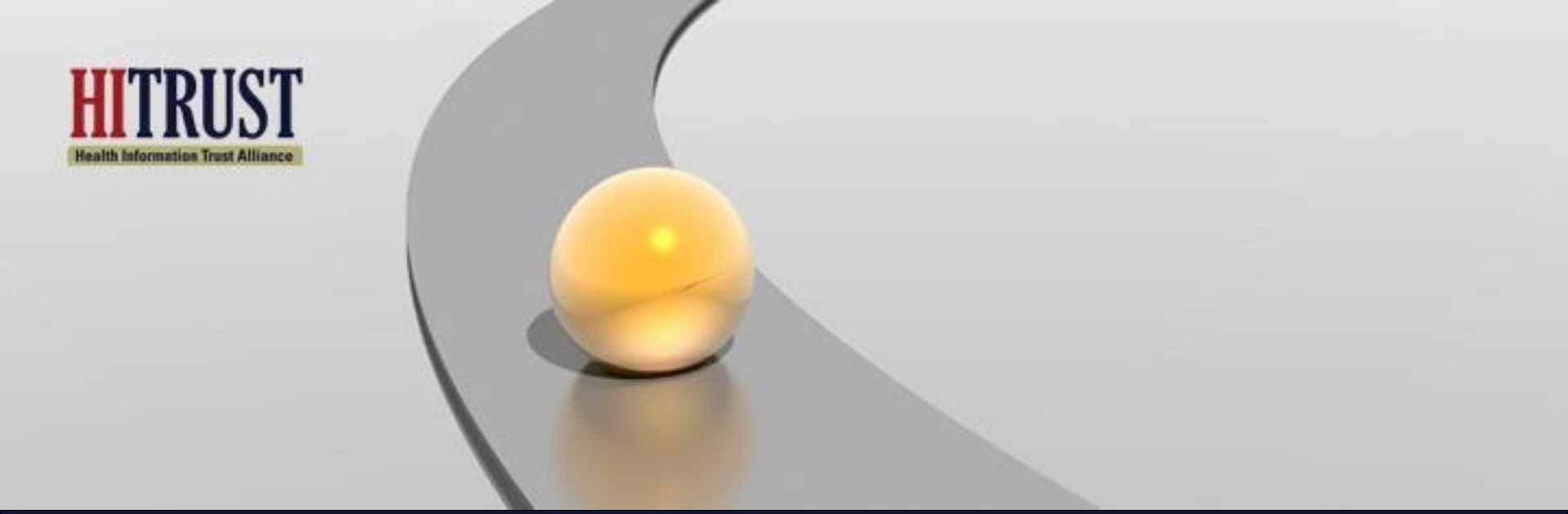


HITRUST CSF Assurance Program

You Need a HITRUST CSF Assessment – Now What?

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

Introduction

- This material is designed to answer some of the commonly asked questions by business associates and other organizations that need a CSF Assessment
- It is intended to:
  - Provide some background and context on issues and challenges related to 3rd party assurance
  - Present an overview of the CSF Assurance program
  - Answer common questions about the program
  - Help organizations get started
  - Identify how and where to get additional help

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

OVERVIEW

Background and overview of the CSF Assurance Program

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

Background- Regulatory Landscape

- Organizations have a responsibility to ensure information shared with business associates (BAs) is appropriately protected
- Under HIPAA:
  - When a covered entity uses a contractor or other non-workforce member to perform “business associate” services or activities, the rule requires that the covered entity include certain protections for the information in a business associate agreement
  - In the business associate contract, a covered entity must impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

Background - Regulatory Landscape

- Under HITECH:
  - The HIPAA Privacy, Security and Breach Notification laws **apply directly to BAs** of covered entities (health care providers, plans, clearinghouses).
  - BAs are now regulated and subject to OCR audits
  - BAs are subject to civil and criminal penalties under certain conditions
  - BAs must report security breaches to covered entities consistent with the Act's notification requirements
  - Non-covered HIPAA entities, such as Health Information Exchanges (HIE), Regional Health Information Organizations (RHIO), e-Prescribing Gateways, and personal health record (PHR) vendors are now required to have BA agreements with covered entities (including physicians) for the exchange of ePHI

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

Background - Regulatory Landscape

- Under HIPAA Omnibus (Final) Rule:
  - Expands definition of BA to include entities that transmit and need routine access to PHI (e.g., Health Information Organizations, e-Prescribing Gateways)
  - Requires BAs to:
    - Use and disclose PHI only as permitted or required by their BAA or by law
    - Prohibit the use or disclosure of PHI in a manner that would violate the Rule
    - Use, request, or disclose only the minimum PHI necessary
    - Take reasonable steps to cure a subcontractor's breach or end a subcontractor's violation of the subcontractor's obligations under its contract or arrangement with the business associate and to terminate the contract or arrangement if the business associate's steps are unsuccessful
  - Applies the Rule's enforcement provisions directly to BAs

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

Background - Regulatory Landscape

- Summary:
  - Ever increasing regulation, enforcement and scope
  - HIPAA Rules applied only to covered entities
    - Extended to BAs thru contractual obligations
  - HITECH Act extended certain HIPAA provisions to BAs
    - BAs subject to regulatory oversight (audits, fines)
  - HIPAA Omnibus (Final Rule) … the “Great Equalizer”
    - Expanded definition of BAs to generally cover any entity with access to PHI
    - Directly applies all provisions, including enforcement to BAs
    - Places obligations on BAs for a subcontractor-compliance with the Rule

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

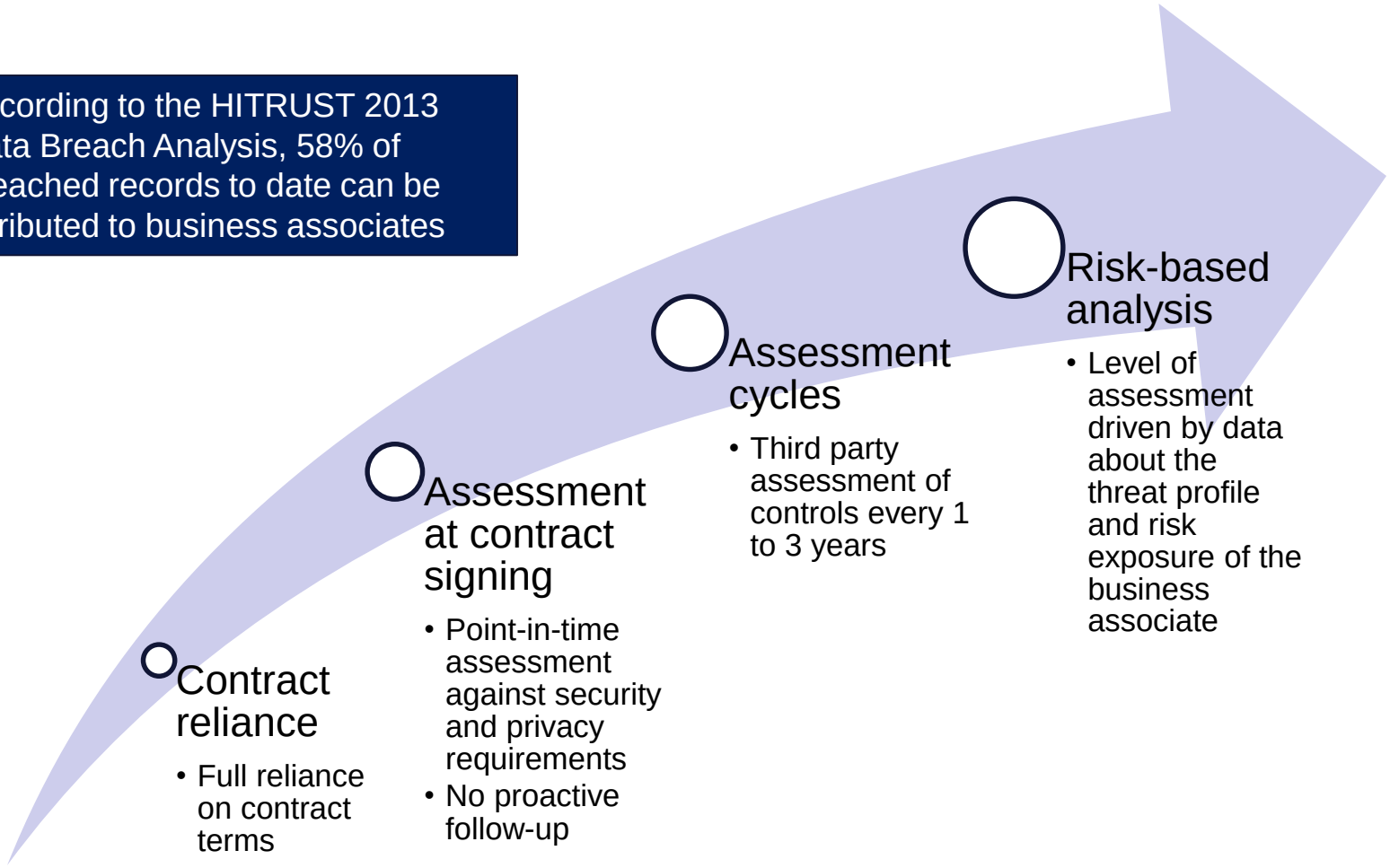
Background - Compliance Challenges

- Organizations are feeling exposed to breaches or data leaks originating with business partners:
  - Increasingly more data shared with business partners
  - Organizations rapidly establishing or evolving business relationships
  - Government/HITECH strongly promoting health information exchanges (HIE)
  - Data dispersed through a complicated web of business partner relationships
  - Greater regulatory requirements and scrutiny
  - Increasing costs shouldered individually by organizations and their business partners due to a lack of a standard industry approach

© 2013 HITRUST, Frisco, TX. All Rights Reserved.
HITRUST
Health Information Trust Alliance

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



© 2013 HITRUST, Frisco, TX. All Rights Reserved.

HITRUST
Health Information Trust Alliance

Background - Covered Entity Issues

- Complex contracting process due to unique security requirements
- Low response rate of questionnaires
- Inaccurate and incomplete responses
- Inadequate due diligence of questionnaires
- Costly and time-intensive data collection, assessment and reporting processes
- Inability to proactively identify and track risk exposures at BA
- Lack of visibility into downstream risks related to BA (i.e., BAs own business partners and sub-contractors)
- Lack of consistent reporting to management on BA risks

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

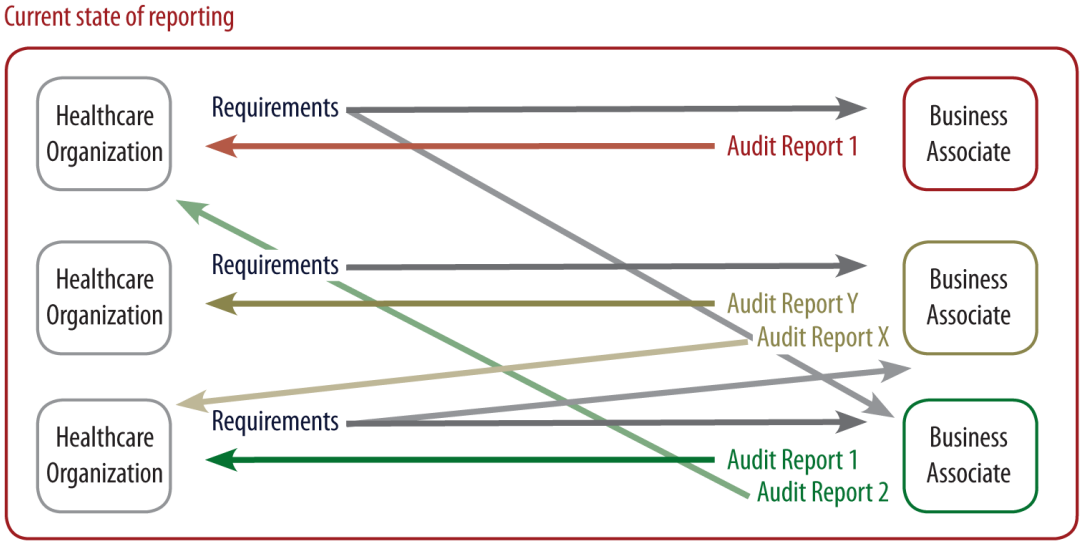
Background - Business Associate Issues

- Complex contracting process due to unique security requirements
- Broad range and inconsistent expectations for responses to questionnaires – cannot effectively leverage responses between organizations
- Complexity with:
  - Maintaining broad range of reporting requirements
  - Expensive and time-intensive audits by organizations
  - Inability to consistently and effectively report to and communicate with organizations
  - Lack of focus on high risk issues and actual remediation

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

HITRUST CSF Assurance Program – The Need

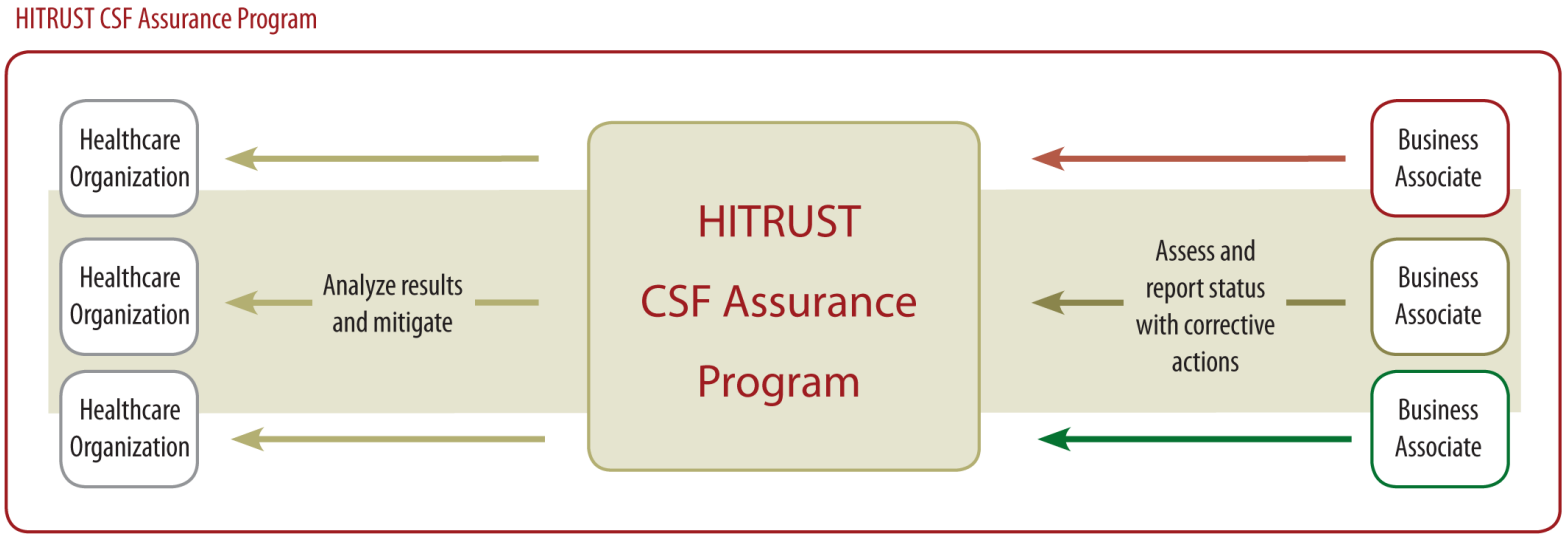
- Organizations facing multiple and varied assurance requirements from a variety of parties
- Increasing pressure and penalties associated with enforcement efforts of HIPAA/HITECH



- Inordinate level of effort being spent on the negotiation of requirements, data collection, assessment and reporting

© 2013 HITRUST, Frisco, TX. All Rights Reserved.
HITRUST Health Information Trust Alliance

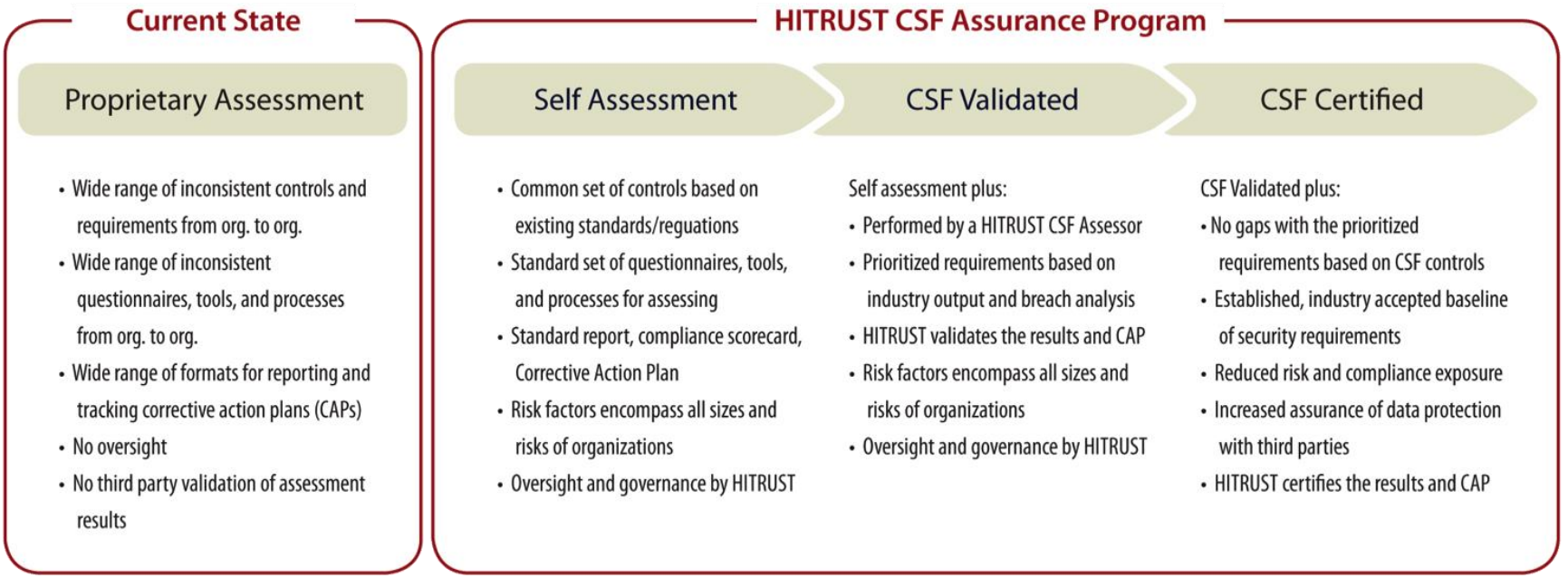
CSF Assurance Program



- Provides a common set of information security requirements, assessment tools and reporting processes
- Reduces the number and costs of business partner security assessments
- HITRUST governance and quality control enable trust between third parties

© 2013 HITRUST, Frisco, TX. All Rights Reserved.
HITRUST Health Information Trust Alliance

CSF Assurance Program - Degrees of Assurance



- CSF Self Assessments can be conducted by business associate
- CSF Validated or Certified requires third party engagement

© 2013 HITRUST, Frisco, TX. All Rights Reserved.
HITRUST
Health Information Trust Alliance

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

"Assess once report many approach"

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

CSF Assurance Program: CSF Validated - Self Assessment

- Assessed entity completes a baseline assessment questionnaire within MyCSF tool
  - Focuses on key areas of security and the use of technology (e.g., firewalls, A/V)
- HITRUST performs limited consistency check and review on the results and issues a CSF Self Assessment report

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

CSF Assurance Program: CSF Validated - Third Party

- Assessed entity completes a baseline assessment questionnaire within MyCSF tool
- Additional on-site testing is performed by a third party CSF Assessor
  - Onsite interviews
  - Review documentation (policies, procedures, previous assessments)
  - Walkthroughs
  - Technical configuration testing
- The completed questionnaire and supporting documentation are sent to HITRUST for review
  - HITRUST issues CSF Validated report

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

CSF Assurance Program: CSF Certified

- CSF Certified designates that an organization **meets all of the certification requirements of the CSF**
- Same components and process as CSF Validated under the CSF Assurance program
- Must engage a qualified third party CSF Assessor to perform onsite testing
- HITRUST reviews and grants certification to the assessed entity
  - Valid for two years from the certification date

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

CSF Assurance Program - Areas Evaluated

- Information Protection Program
- Endpoint Protection
- Portable Media Security
- Mobile Device Security
- Wireless Protection
- Configuration Management
- Vulnerability Management
- Network Protection
- Transmission Protection
- Password Management
- Access Control
- Audit Logging & Monitoring
- Education, Training & Awareness
- Third Party Security
- Incident Management
- Business Continuity & Disaster Recovery
- Risk Management
- Physical & Environmental Security
- Data Protection & Privacy

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

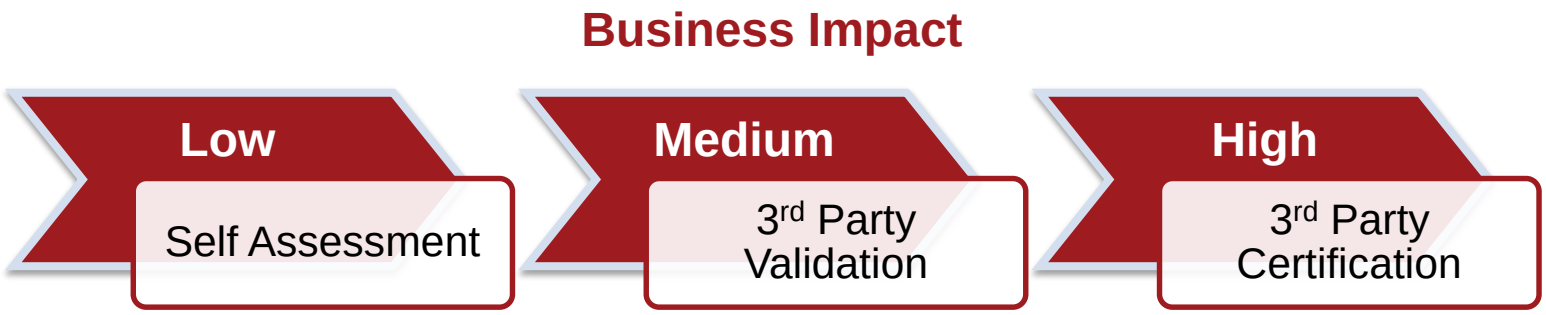
GETTING STARTED

Process and tools to get started

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

Assessment Process - Identify Assurance Requirements

- Coordinate with your business partners that require information about your organization's security program to identify the type of assessment needed



- Increasing the level of assessment will satisfy more business partners

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

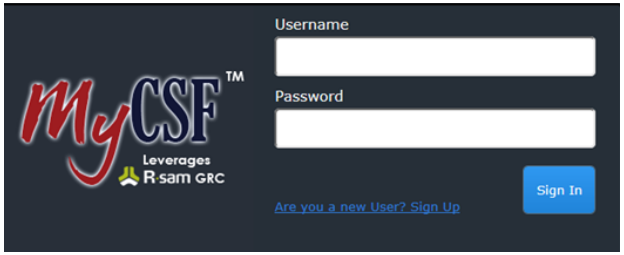
Assessment Process - Define Scope

- The assessment scope gives context to the security controls and those organizations and individuals relying on the results
  - Organization scope defines the facilities, business units or subsidiaries reviewed and covered by the controls
  - System scope defines the “systems” reviewed and covered by the controls - systems are generally applications; however, they could also be hardware (e.g., medical devices) or enterprise-wide platforms (e.g., electronic health records system)
- Increasing the organization and system scope will satisfy more business partners, but also increases complexity

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

Assessment Process – Generate and Complete the Baseline Assessment

- The Baseline Assessment is designed to:
  - Identify general controls, security resources and tools utilized
  - Evaluate the maturity of the organization's security management program
  - Identify documents, interviews and tests to perform as necessary
- There are typically 150-200 questions in the Baseline Assessment
  - Best to work through with the individual(s) who have the most knowledge of the overall security program and controls
- Assessment workflow may be managed in MyCSF
  - Questions may be assigned to specific individuals
  - Notifications and reminders can be automated
  - Status of the assessment can be monitored and reported to management



Access MyCSF at
https://app.mycsf.net/mycsf

© 2013 HITRUST, Frisco, TX. All Rights Reserved.
HITRUST
Health Information Trust Alliance

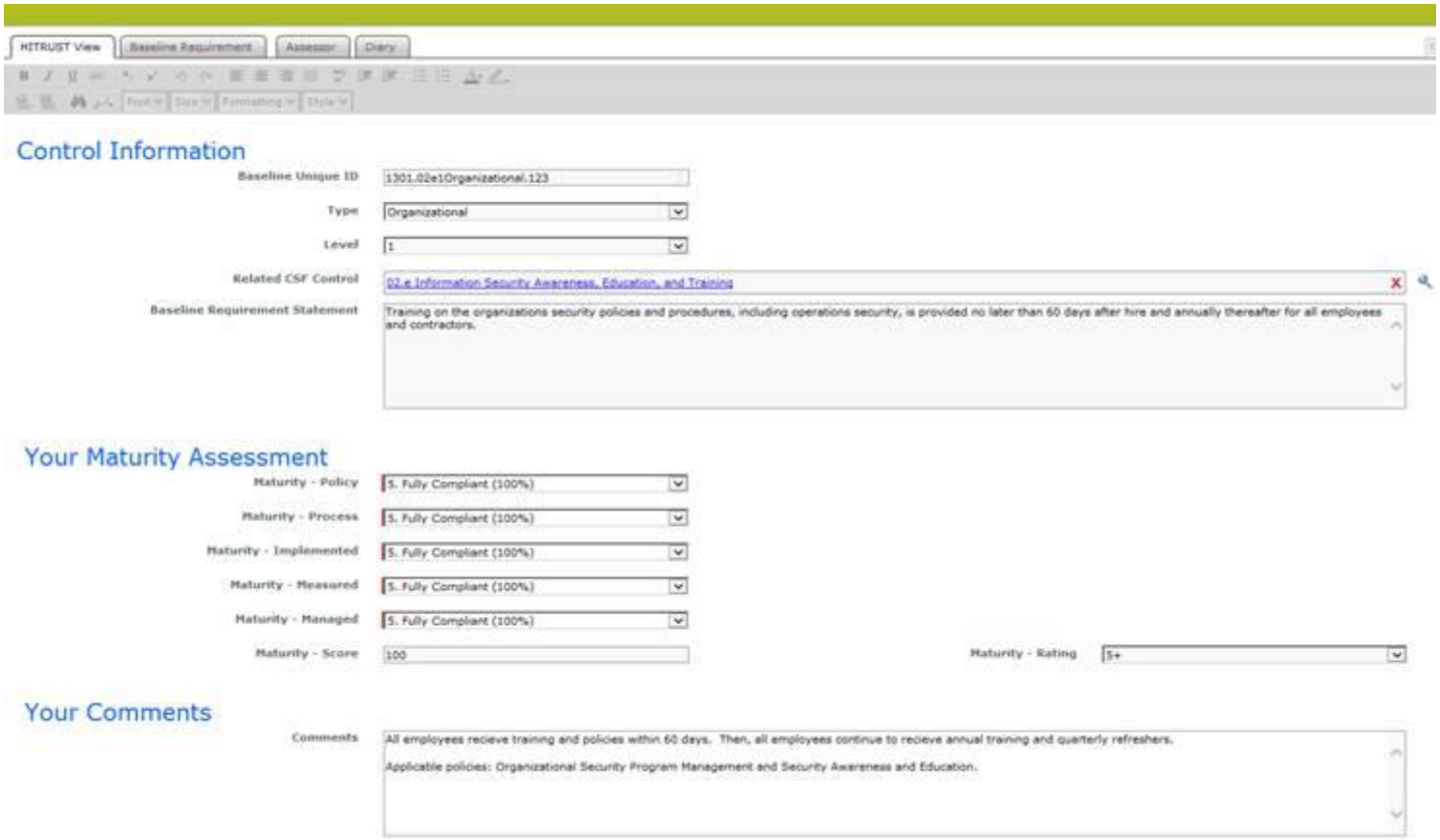
Questionnaire

Baseline 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
- Ensures all HIPAA Security Rule implementation specifications are addressed

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

Questionnaire



© 2013 HITRUST, Frisco, TX. All Rights Reserved.

HITRUST
Health Information Trust Alliance

Examples of Domain Questions/Requirements Statement

- The organization has a formal information protection program based on an accepted industry framework that is reviewed and updated as needed.
- The security policies are regularly reviewed, updated and communicated throughout the organization.
- Firewalls are configured to deny or control any traffic from a wireless environment into the covered data environment.
- The access authorization process addresses requests for access, changes to access, removal of access, and emergency access.
- The organization maintains and updates a formal, comprehensive program to manage the risk associated with the use of information assets.
- The organization has formally appointed a data protection officer responsible for the privacy of covered information.

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

HITRUST
Health Information Trust Alliance

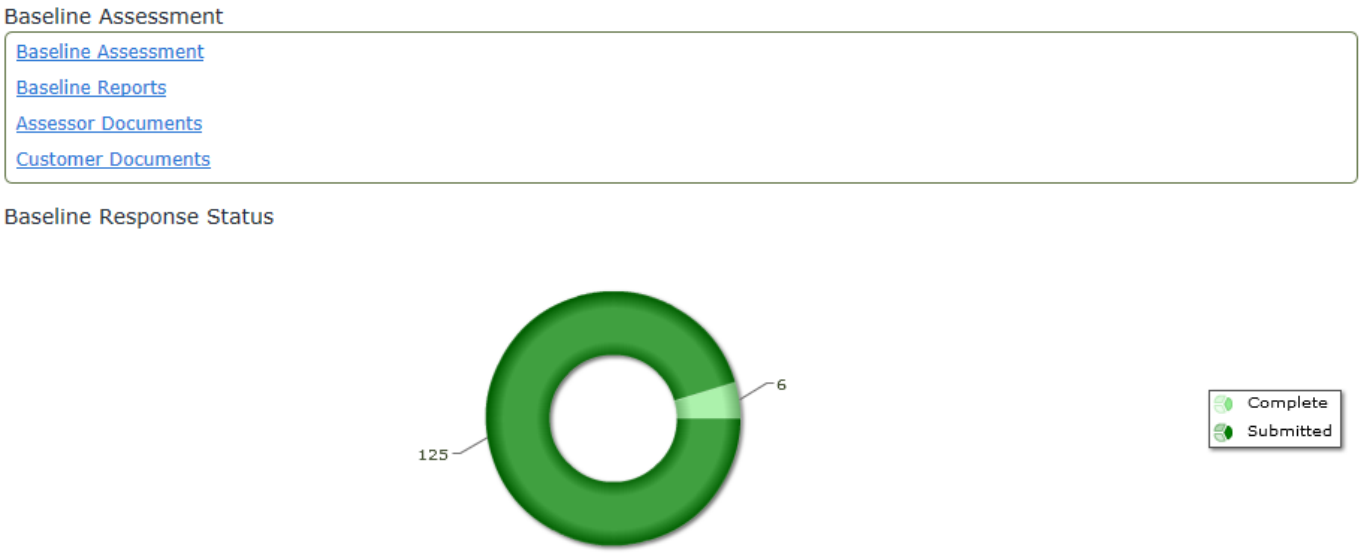
Assessment Process - Conduct Testing

- For third party assessment (CSF Validated or CSF Certified), testing of the controls is required
- Testing is performed by a qualified CSF Assessor organization and may include
  - Documentation review
  - Interviews
  - System configuration Objective of tests is to validate the metrics and controls captured in the Baseline Assessment
  - Gather enough information to be able to allow HITRUST to formulate a rating
  - Address compliance requirements if applicable
  - The CSF serves as the reference source for what to test
  - CSF detailed illustrative procedures serve as a guide on how to test

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

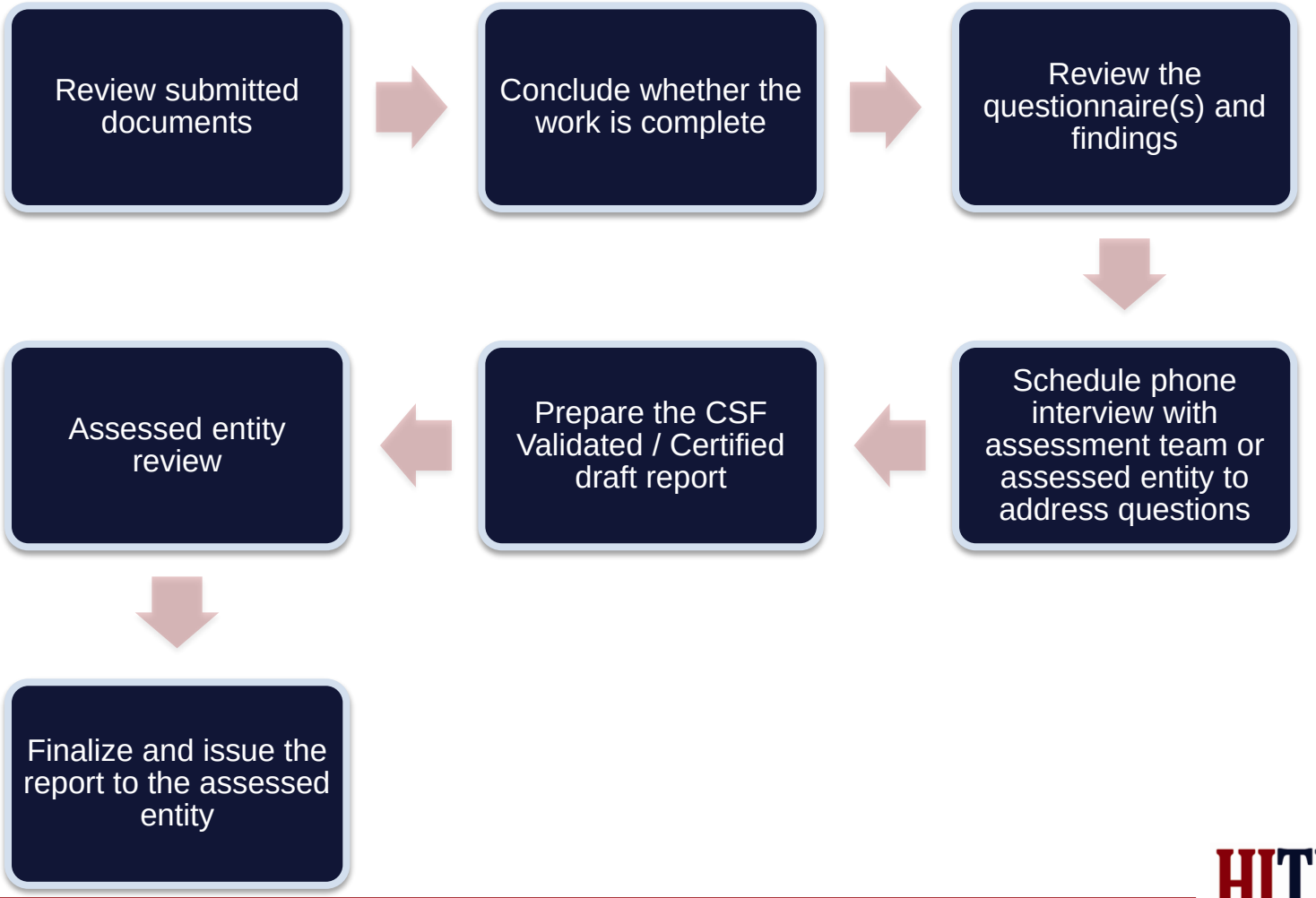
Assessment Process - Submit to HITRUST

- After completing the Baseline Assessment and other materials as necessary submit them to HITRUST.



© 2013 HITRUST, Frisco, TX. All Rights Reserved.

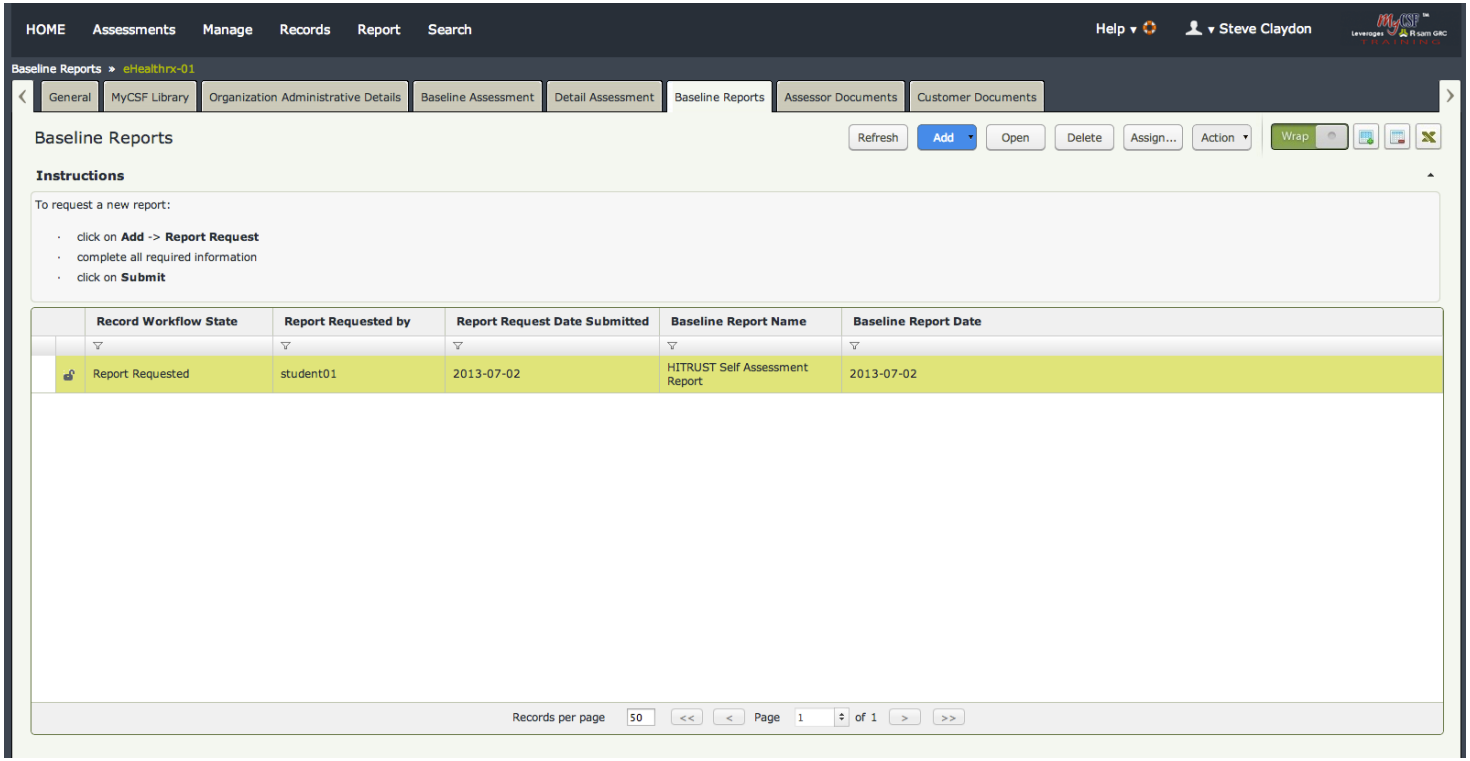
Assessment Process - HITRUST Quality Review



© 2013 HITRUST, Frisco, TX. All Rights Reserved.

Assessment Process - Review Report

- You will be notified when your draft and final reports are ready and you can download them from MyCSF when they are available

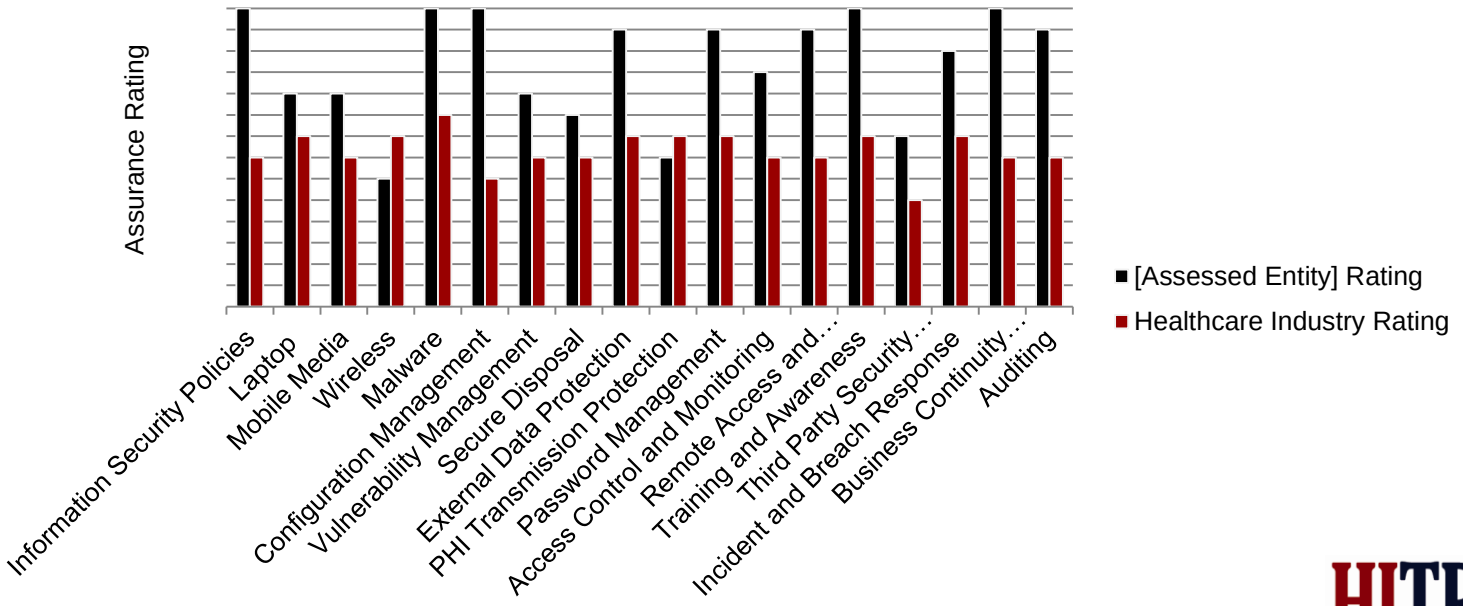


© 2013 HITRUST, Frisco, TX. All Rights Reserved.

HITRUST
Health Information Trust Alliance

CSF Assurance Report

- HITRUST leverages the concepts and rating scheme of the NISTIR 7358 standard - Program Review for Information Security Management Assistance (PRISMA) to rate an organization's security management program
  - The rating is an indicator of an organization's ability to protect information in a sustainable manner.



© 2013 HITRUST, Frisco, TX. All Rights Reserved.
HITRUST Health Information Trust Alliance

CSF Assurance Report

Network Protection	**2+**	Higher ratings can be achieved by: • Developing a policy that defines acceptable use of network services. • Deploying firewalls to segregate internal wired from wireless networks as well as internal from external networks. • Deploying application level firewalls on all public facing web applications. • Appropriately restricting the ability to connect to the internal network based on access control policy. • Reviewing the organization's network, including components and connections, documenting and updating the current network configuration.
Transmission Protection	**2-**	Higher ratings can be achieved by: • Developing policies supported by detailed procedures for the secure transmission of PHI and other sensitive information over open, public networks (e.g., the internet). • Standardize the organization's web infrastructure where PHI is transmitted on SSL/TLS. • Enabling the automatic detection and block/encryption of email messages containing PHI and other sensitive information. • Defining metrics for PHI transmission protection and monitoring and tracking deployment and operating effectiveness.
Password Management	**2+**	Higher ratings can be achieved by: • Developing policies supported by detailed procedures for configuring and maintaining complex passwords on all workstations, servers, databases, and

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

Assessment Process – Scoring

- Customers and covered entities have established various approaches to determine not just assurance level requirements but acceptable scores for each control area (domain)
  - These can take multiple factors into account, such as criticality of control, volume of PHI, and other business and clinical risks
  - Examples:
    - A large health system may require a cloud-based EHR provider to provide a CSF Certified report due to the extensive amount of ePHI handled and criticality of the system to the business
    - An HIE may require all participants to have a CSF Validated third party report indicating no less than a “2” in a maximum of 3 domains with CAPs remediating deficiencies within 1 year; otherwise no less than a “3-” for all remaining domains with CAPs addressing remediation within 3 years
    - A community hospital may require a small 3-person medical transcription company to provide a CSF Validated self-assessment report with minimum domain scores of “3+” for laptops, mobile media, wireless, malware, secure disposal, remote access, access control and education and training

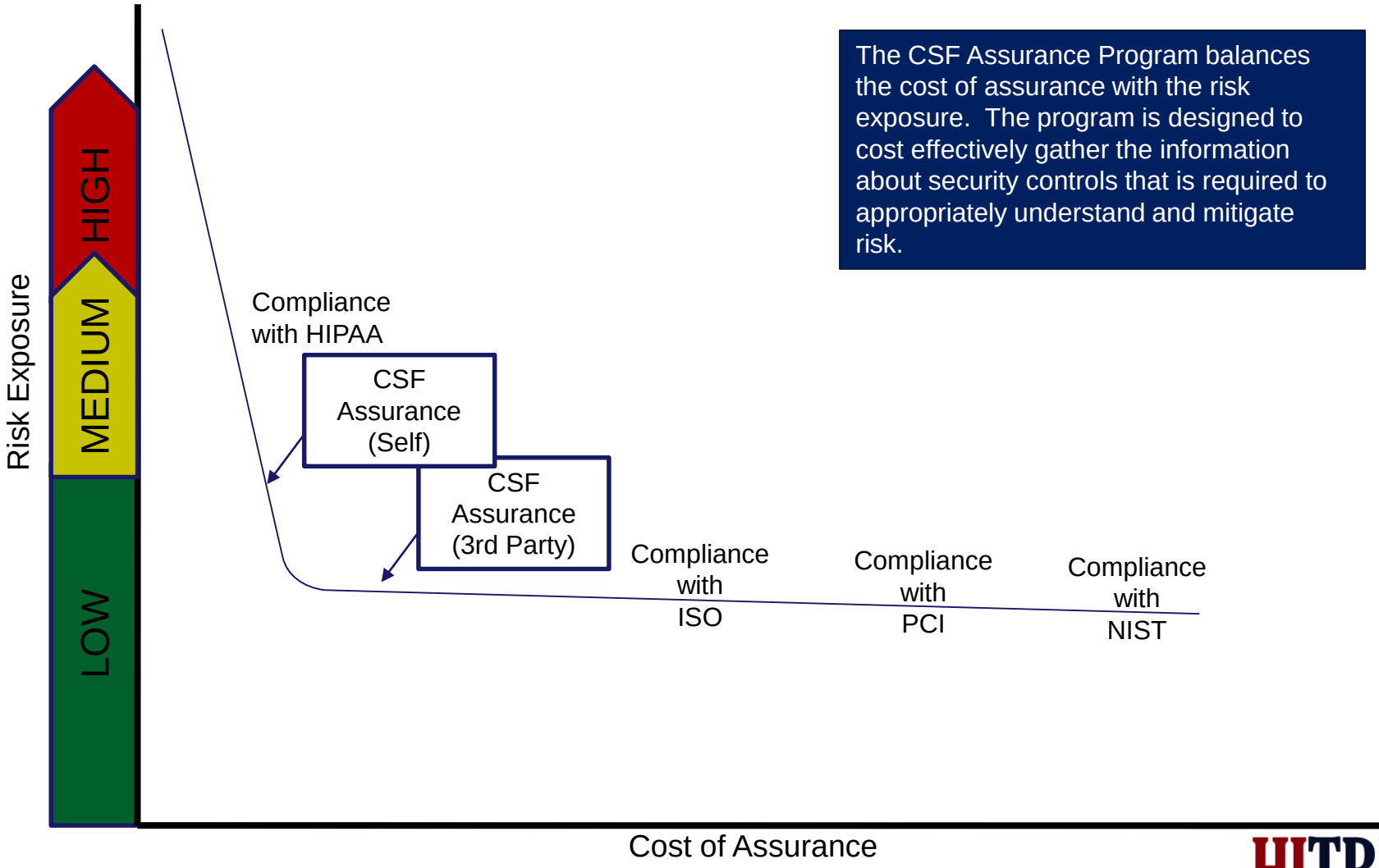
© 2013 HITRUST, Frisco, TX. All Rights Reserved.

Time and Cost

Type of Assessment	Time to Complete	CSF Assessor Involved	Cost
Self Assessment	<1 month	No	$2,500
Third Party Onsite Assessment	~3 months	Yes	$25,000+ depending on scope and complexity

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

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.

© 2013 HITRUST, Frisco, TX. All Rights Reserved.
HITRUST
Health Information Trust Alliance

Commonly Asked Questions

Questions and Answers

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

Questions and Answers

- How does the CSF and CSF Assurance programs relate?
  - **Answer: The CSF Assurance Program addresses the assessment and reporting of compliance with CSF requirements**
- How does the CSF Assurance program and CSF Assessment relate?
  - **Answer: CSF assessment methodologies are an integral component of the CSF Assurance program, which is why CSF assessors are certified to conduct assessments based on multiple criteria to ensure consistency and repeatability**
- When I have a questions about the CSF Assessment process, who do I contact?
  - **Answer: Organizations can contact HITRUST with any questions regarding the CSF Assessment process**
- How is HITRUST getting more organizations to accept the CSF Assessment reports?
  - **Answer: By encouraging organizations to accept if not mandate the use of CSF Validated and Certified reports for the sharing of information protection assurances and through general outreach to the healthcare community**

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

For More Information

www.hitrustalliance.net

469-269-1110

© 2013 HITRUST, Frisco, TX. All Rights Reserved.

HITRUST
Health Information Trust Alliance