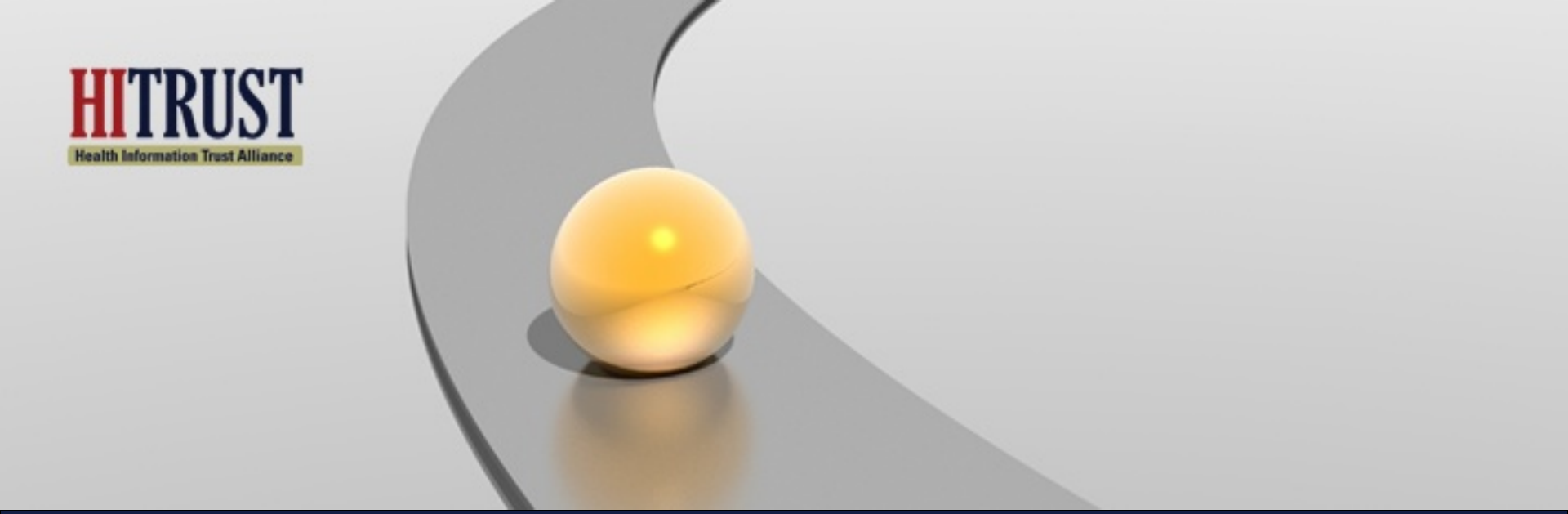


HITRUST
Health Information Trust Alliance

HITRUST CSF Assessment Process

June 2015

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

Assessment Process – Generate and Complete a HITRUST CSF Assessment

The HITRUST CSF 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 120-328 questions in a HITRUST CSF 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

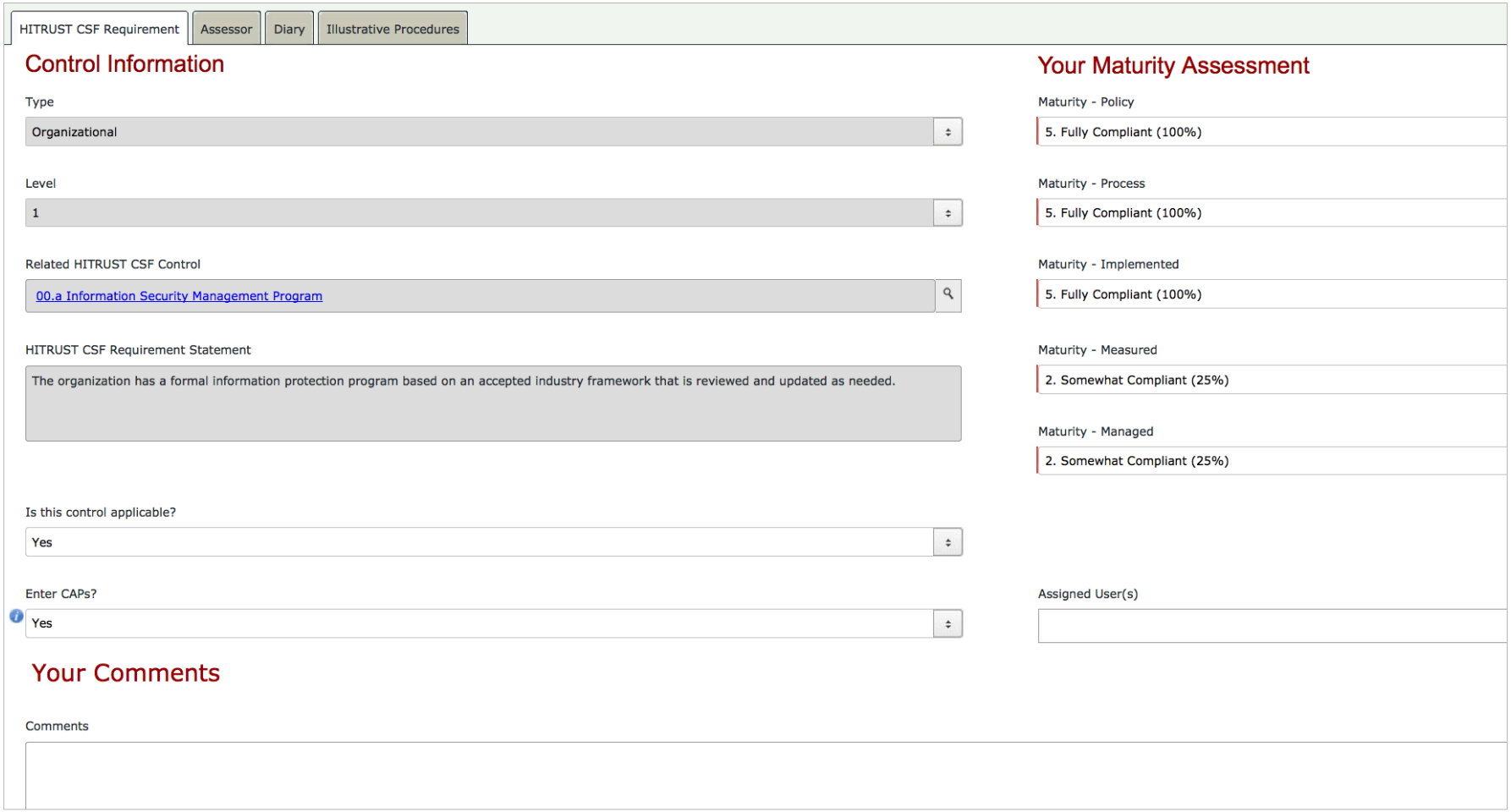
Access MyCSF at hitrustalliance.net/mycsf

Questionnaire

HITRUST CSF 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 HITRUST 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

Questionnaire



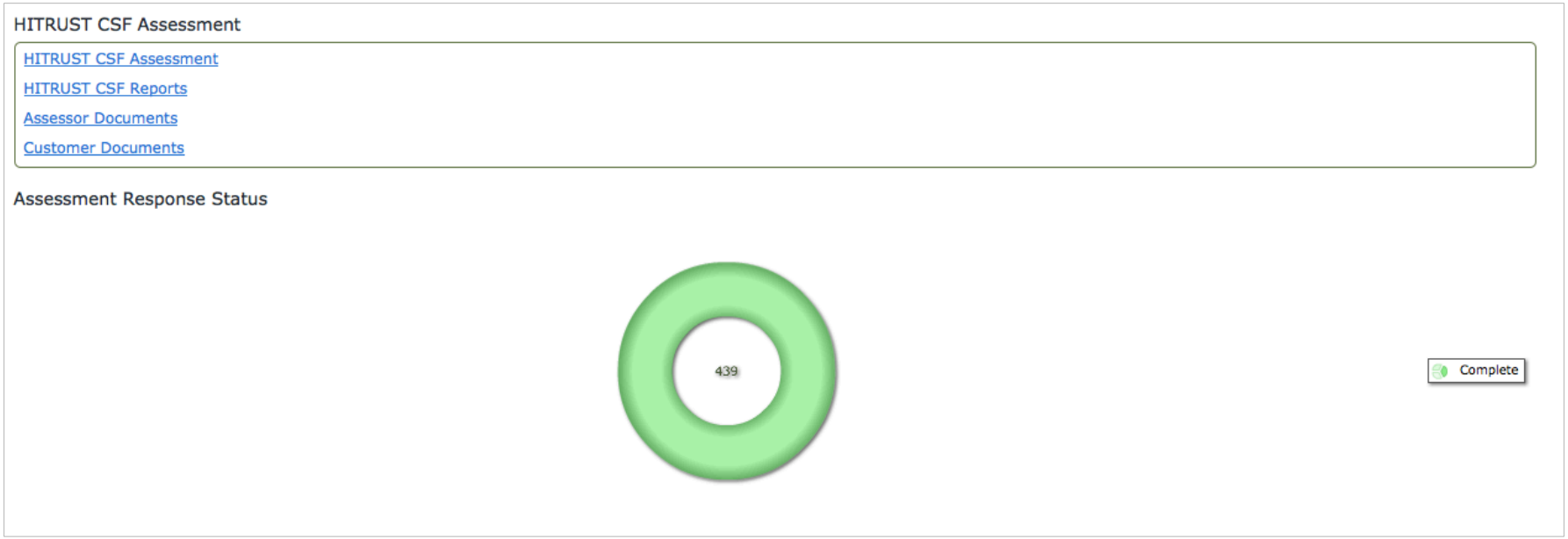
HITRUST
Health Information Trust Alliance

Examples of HITRUST CSF Requirements

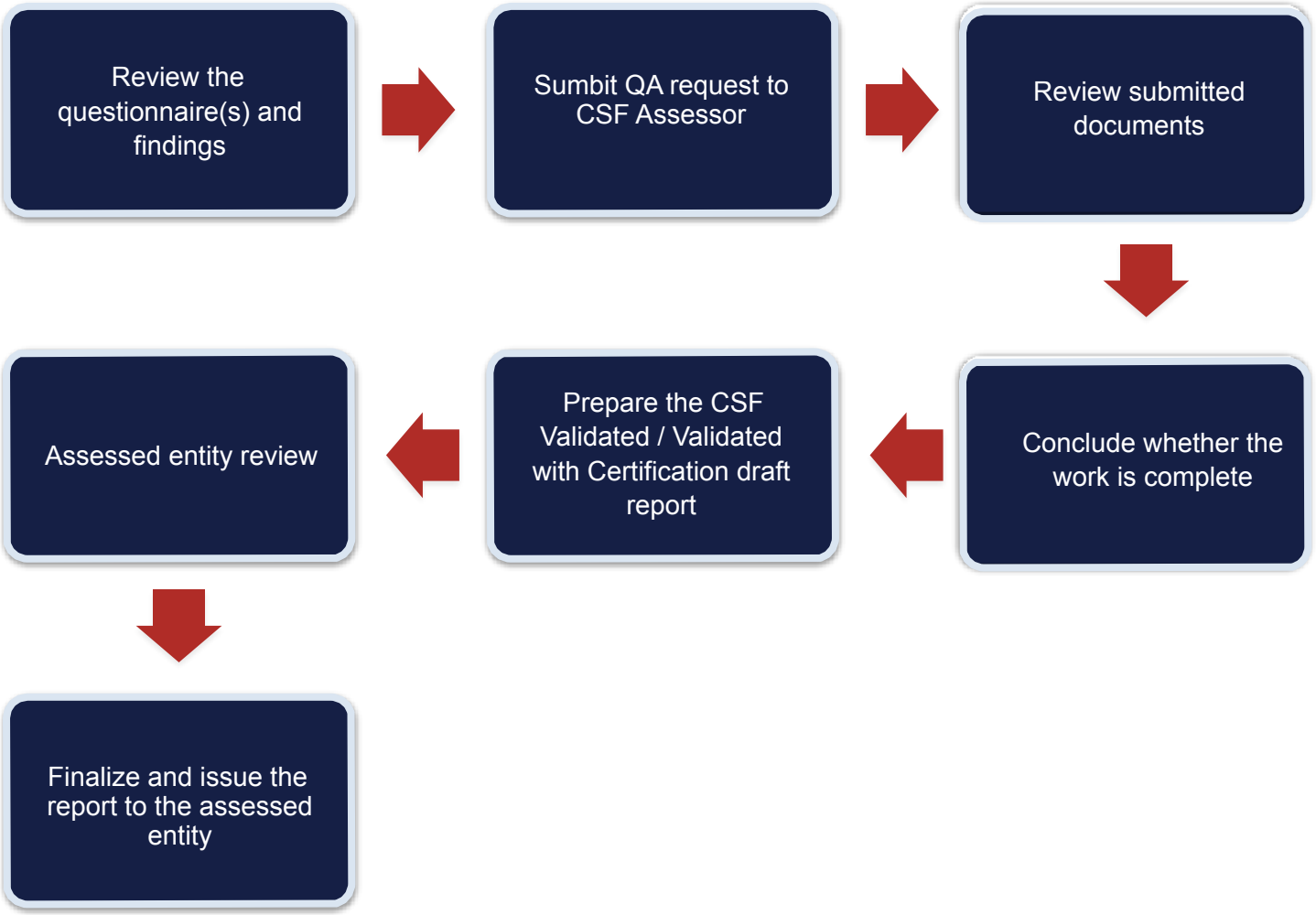
- The organization has a formal information protection program based on an accepted industry framework that is reviewed and updated as needed.
- The security policies are regularly reviewed, updated and communicated throughout the organization.
- Firewalls are configured to deny or control any traffic 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.

Assessment Process – Submit to HITRUST

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



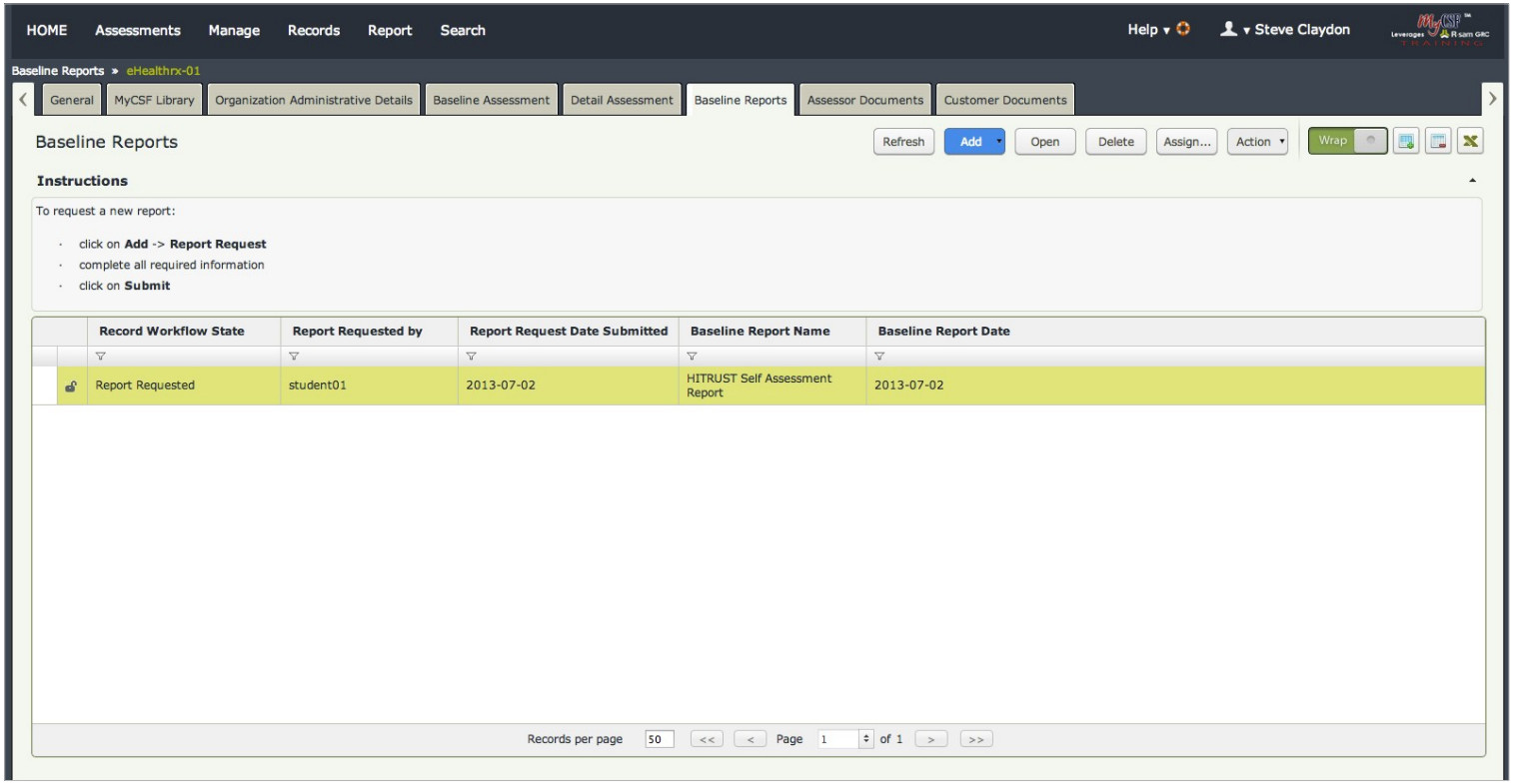
Assessment Process – HITRUST Quality Review



HITRUST
Health Information Trust Alliance

Assessment Process – Review Report

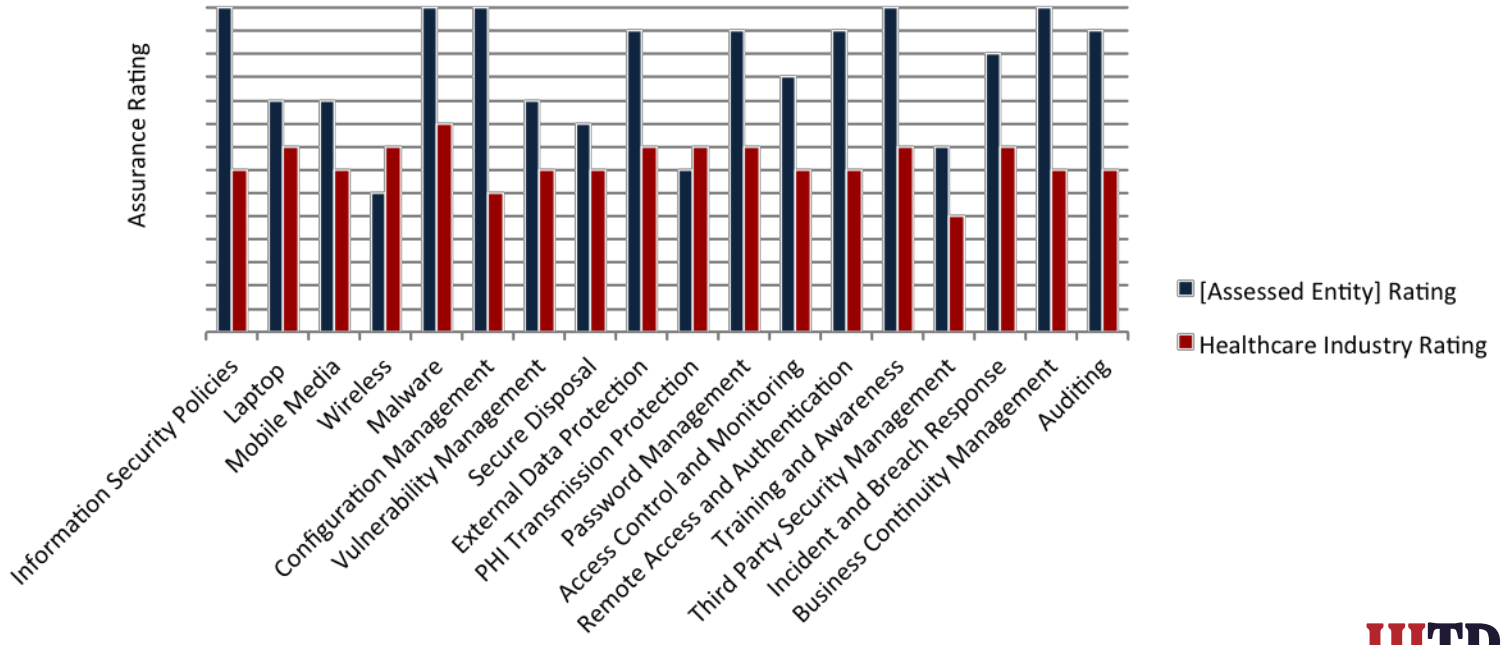
- You will be notified when your draft and final reports are ready and you can download them from MyCSF when they are available



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.



HITRUST Health Information Trust Alliance

CSF Assurance Report

HITRUST
Health Information Trust Alliance

CSF Control Areas	Rating	Comments
Information Security Policies	5+	None
Laptop Security	4	Higher ratings can be achieved by: • Defining metrics for laptop security including encryption and firewall to monitor and track deployment and operating effectiveness. The HITRUST CHIP Questionnaire outlines a number of metrics that should be considered.
Mobile Media Security	4	Higher ratings can be achieved by: • Periodically evaluating the laptop security measures including encryption and firewall to ensure they are installed and operating correctly on all devices. Many tools have centralized management consoles which can monitor and alert security personnel if the tool is not working correctly. • Defining metrics for laptop security including encryption and firewall to monitor and track deployment and operating effectiveness. The HITRUST CHIP-Questionnaire outlines a number of metrics that should be considered.
Wireless Security	3-	Higher ratings can be achieved by: • Regularly scanning for rogue wireless access points in the organization's environment and disabling any devices found. • Defining metrics for wireless security including implementation of security protocols, vulnerabilities found, and rogue access points found, and monitor and track deployment and operating effectiveness. The HITRUST CHIP-Questionnaire outlines a number of metrics that should be considered.
Malware Protection	5+	None
Configuration Management	5+	None
Vulnerability Management	4	Higher ratings can be achieved by: • Developing formal procedures and timelines for remediating any critical or high

10

HITRUST
Health Information Trust Alliance