HITRUST

HITRUST THIRD PARTY ASSURANCE SUMMIT 2018

HITRUST THIRD PARTY ASSURANCE SUMMIT 2018

WHAT TO EXPECT WHEN UNDERGOING A HITRUST CSF ASSESSMENT

Abe Dress, Senior Director, Healthcare and Life Sciences, Coalfire
Chad Phillips, Managing Director, Deloitte & Touche LLP
Ken Vander Wal, Chief Compliance Officer, HITRUST

HITRUST THIRD PARTY ASSURANCE SUMMIT 2018

Abe Dress, Senior Director, Healthcare and Life Sciences

HOW TO PLAN FOR YOUR HITRUST JOURNEY

About Coalfire - Full Lifecycle Cybersecurity Service Provider

Cyber Risk Advisory

- Strategic planning
- Maturity assessments
- Enterprise risk management
- Policy development
- Incident response planning
- M&A due diligence
- Virtual CISO
- Business continuity
- Governance programs

Compliance & Risk Assessments

- PCI DSS
- FedRAMP
- FISMA
- ISO
- SOC
- HITRUST
- HIPAA
- GDPR
- CSA STAR

COALFIRE

Labs/Technical Security Services

- Vulnerability assessments
- Application security
- Hunt operations
- Training
- Penetration testing
- Red teaming
- Digital/Data forensics

Cyber Engineering

- Security architecture
- Technology evaluations
- Security monitoring and analytics
- Environment optimization and health checks
- Secure cloud solutions Virtualization solutions
- Vulnerability management programs

Tale of 2 Personas

Company A – Certification Driven

- Looking for a competitive differentiator or to satisfy a customer requirement
- Price driven
- Doesn't understand the value
- Wants a check-in-the-box assessment
- Thinks HITRUST is a commodity
- Doesn't plan accordingly; views certification as an audit

Company B – Value Driven

- Embraces the CSF to mature their infosec program
- Understands the required investment
- Staffs their organization with HITRUST SMEs
- Has support from the Board and executive leadership
- Understands the value of the framework, with or without certification

Things You Should Do to Prepare

- ✓Identify the following:
  - a) What's wrong with your current state
  - b) What does your future state look like (PBOs)
  - c) What are the required capabilities to satisfy your PBOs
- ✓Are you Company A or Company B? If Org B, build adoption, implementation, and assessment strategy.
- ✓Work with your Customer
- ✓Go to HITRUST Training

Things You Should Do to Prepare

- ✓Select an Assessor firm to work with
- ✓Perform a HITRUST workshop
  - ✓ Identify scope
  - ✓ Define system and regulatory factors
  - ✓ Identify opportunities for “leveragability”
  - ✓ Define # of MyCSF Objects and in-scope requirements
- ✓Prepare for the challenges
- ✓Develop your Roadmap for Certification

Scoping Assessments

- The MyCSF GRC tool allows organizations to define the scope of their environment
  - Focus on your need (Internal requirement, external need, support the business)
- Define assessment objects (within scope) to be included
- Assessments can be **Single** (efficient) or **Multiple** (increased data accuracy)
- For certification a report is needed for each assessment object
  - Multiple Assessments = Multiple Reports

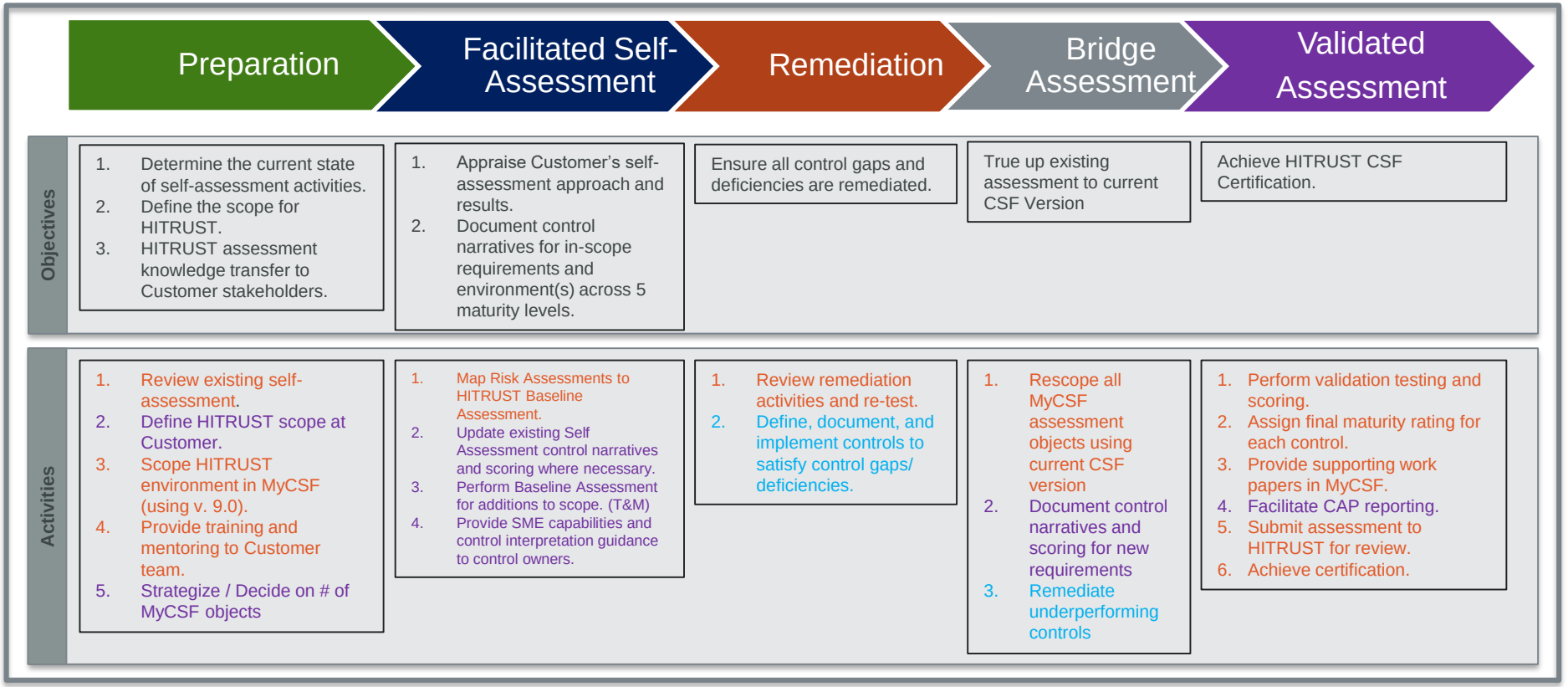
Scoping Assessments

What and Why Am I Doing This?

- What is the purpose of this assessment / compliance work
  - Internal (Audit) requirements
  - External requirements (Meaningful Use Attestation)
  - Support BA requirements
  - Demonstrate compliance internally
  - Improve security posture / stance
  - Other……

Without this information, scoping is infinitely harder and more complex

Sample Assessment Journey



Chad Phillips, Managing Director, Deloitte & Touche LLP

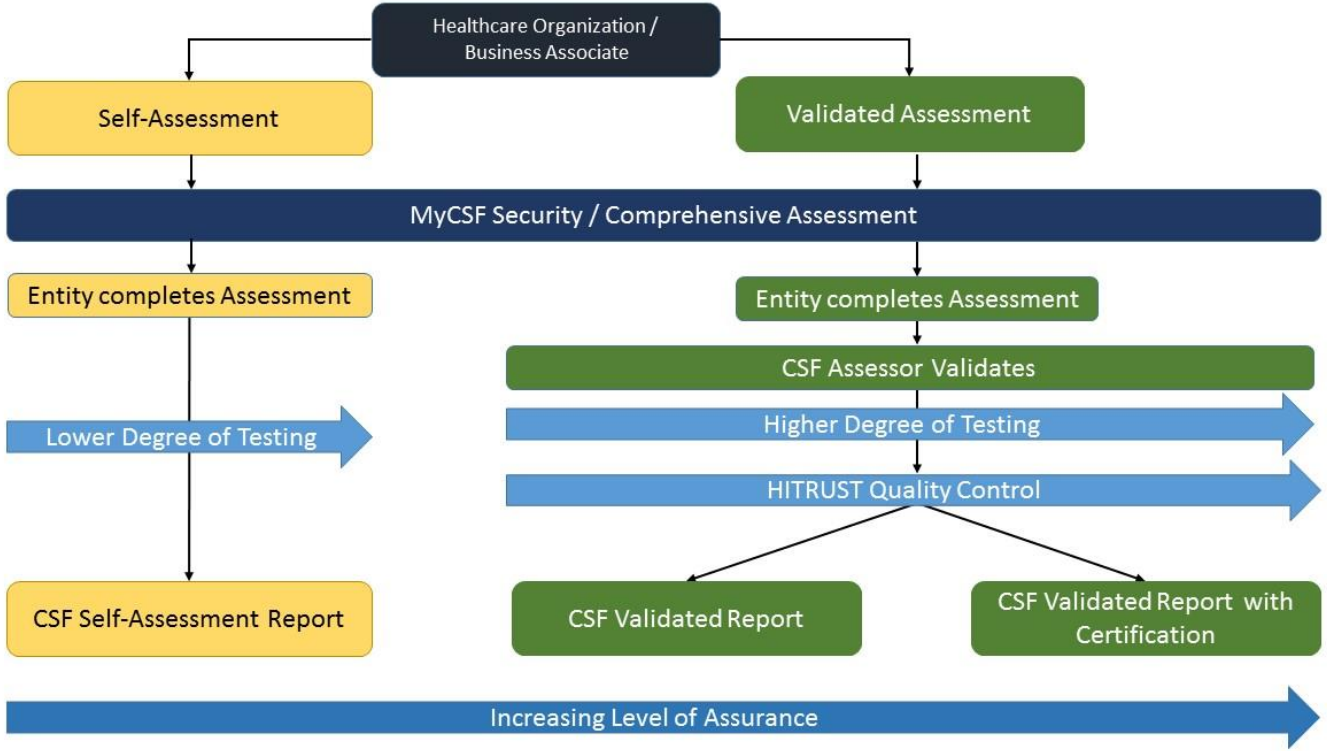
PERFORMING A HITRUST ASSESSMENT

Deloitte Risk and Financial Advisory

Lead. Accelerate. Disrupt.

Deloitte Risk and Financial Advisory helps organizations effectively navigate business risks and opportunities—from strategic, reputation, and financial risks to operational, cyber, and regulatory risks—to gain competitive advantage. We apply our experience in ongoing business operations and corporate lifecycle events to help clients become stronger and more resilient. Our market-leading teams help clients embrace complexity to accelerate performance, disrupt through innovation, and lead in their industries.

Overview of HITRUST CSF Assurance Program



What can HITRUST Certify?

HITRUST only certifies implemented systems.

- HITRUST does **not** certify *facilities, people, services or product*. It must be an implemented environment for a certification to be awarded.

Within a scope, an assessment may include:

- Business Units
- Facilities
- Departments
- Applications
- Servers and Databases
- Network Infrastructure
- Information Security Control Systems
- Business Associate / Vendor

HITRUST CSF Design

Implementation Levels

- The Implementation levels are built upon three risk factors:
  - Organizational factors (e.g. type, size, locations)
  - System factors (e.g. connection to the internet, use of mobile devices)
  - Regulatory factors (e.g. PCI / CMS / State requirements)
- Identifying these factors may drive higher implementation levels
- Level 1 is a baseline control agreed by the industry
  - Objective of Level 1 is to meet the HIPAA Security Rule requirements (required & addressable)
  - Each additional level encompasses the lower levels and includes additional requirements commensurate with risk
  - **Example:** A control identified to be Level 3 would need to have requirements in Levels 1 & 2 also implemented

Assessment Process

Responding to Assessment Requirement Statements

- When answering requirement statements, you must consider **ALL** objects within your scope
  - e.g., Scope is your Meaningful Use environment
    - 3 Applications
    - 2 Databases
    - 2 File Servers
    - 1 Firewall, 2 Routers
    - Wireless Infrastructure
- When you answer a security statement, you consider the answers for all objects

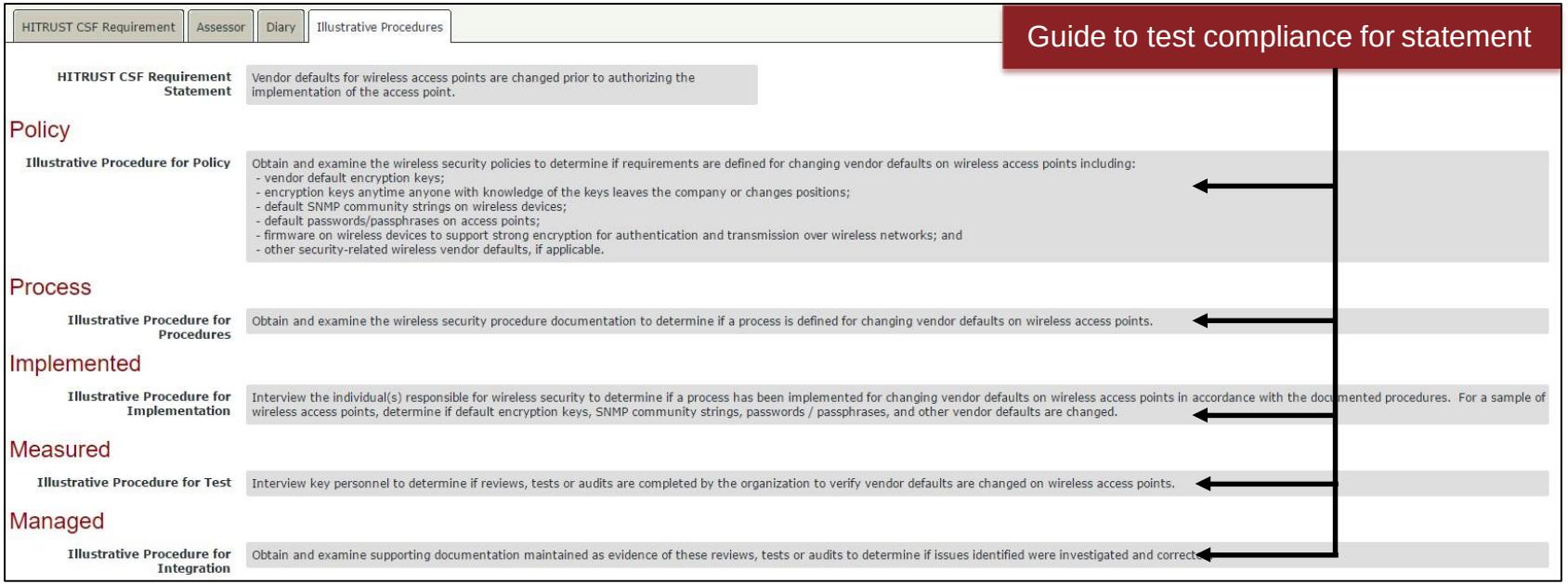
Assessment Process

Responding to Assessment Requirement Statements

- Completing a risk-based questionnaire (Factors tab) drives control requirement selection
- The organization will enter responses for each requirement statement that will assess the level of compliance for each of five (5) PRISMA-based maturity levels. Those five maturity levels are:
  - Is a **policy** or standard in place?
  - Is there a **process** or procedure to support the policy?
  - Has it been **implemented**?
  - Is it being **measured** and tested by management to ensure it is operating?
  - Are the measured results being **managed** to ensure corrective actions are taken as needed?
- For each maturity level, the organization indicates its level of compliance. The five options are:
  - Non-Compliant (0%)
  - Somewhat Compliant (25%)
  - Partially Compliant (50%)
  - Mostly Compliant (75%)
  - Fully Compliant (100%)

Assessment Process

Understanding the Illustrative Procedures



Scoring an Assessment

Scoring Breakdown by Maturity Domain

- Policy 25%
- Process 25%
- Implementation 25%
- Measured 15%
- Managed 10%

Sample Score

Policy	= 100 * .25
Process	= 75 * .25
Implementation	= 100 * .25
Measure	= 25 * .15
Managed	= 0 * .10
Overall Score:	= 72.5

Certification Requirements

- Each domain MUST score at least a 3 (61.99%) to achieve certification requirements
  - Any control requirement that scores less than a 3+ will raise a CAP
  - You can be Certified with CAPs as long as the overall score of all domains is 3
- If any domain scores less than a 3, a Validated report **only** will be issued

Submission of Assessment to Assessor

- Assessor will review all supporting documentation to meet the implementation requirement statements
  - Are there documented and approved **policies, procedures?**
  - Perform testing and review documentation that confirms the correct **Implementation**
  - Supporting evidence for all **Measure and Managed** efforts
    - Names and dates of documents
    - Frequency of tests/audits
    - Any process documents for Managed
- Assessor will interview personnel and **test** to ensure:
  - **Policies** and **procedures** and **implementation** is completed at the relevant levels and are being followed.
- The results of this work will be documented within the tool

Assessor Technical Testing

- Technical testing is designed to help reveal security flaws and weaknesses in information systems
  - This testing can include configuration settings, vulnerability assessments and penetration testing
- Validation of configuration settings for select system controls provides evidence regarding the implemented security policies and procedures
  - Audit settings
  - Patch levels
  - Password settings
  - Account privileges
  - Encryption deployment
  - User listings

Assessor Documentation

- For each requirement statement, the assessor will either agree or disagree with the client's response
- Will enter relevant comments to support the finding
- Will identify the documents reviewed
- Will identify the interviews performed
- The Additional Comments/Observations/Recommendations box can used to highlight these findings in general for a particular statement
- Revision requests from client can be performed per statement

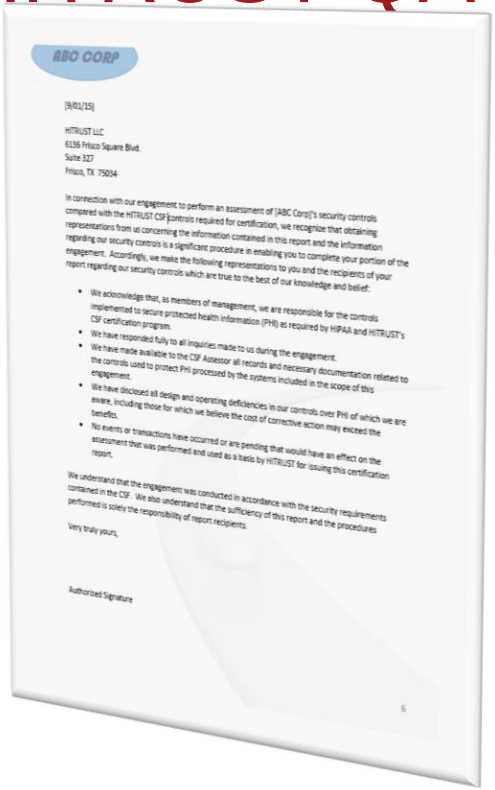
HITRUST THIRD PARTY ASSURANCE SUMMIT 2018

Ken Vander Wal, Chief Compliance Officer, HITRUST

WHAT IS HITRUST'S QA PROCESS

Key Submission Items for HITRUST QA

- Assessment Questionnaire/Object
- Third-Party Participation Agreement
- Management Representation Letter
- Organizational Overview and Scoping
- Assessor Timesheet
  - Documents the hours the assessor spent
  - At least 33% of the total testing hours performed by a CCSFP


ABC CORP

[9/01/15]

HITRUST LLC
6136 Frisco Square Blvd.
Suite 327
Frisco, TX 75034

In connection with our engagement to perform an assessment of [ABC Corp]'s security controls compared with the HITRUST CSF controls required for certification, we recognize that obtaining representations from us concerning the information contained in this report and the information regarding our security controls is a significant procedure in enabling you to complete your portion of the engagement. Accordingly, we make the following representations to you and the recipients of your report regarding our security controls which are true to the best of our knowledge and belief:

- We acknowledge that, as members of management, we are responsible for the controls implemented to secure protected health information (PHI) as required by HIPAA and HITRUST's CSF certification program.
- We have responded fully to all inquiries made to us during the engagement.
- We have made available to the CSF Assessor all records and necessary documentation related to the controls used to protect PHI processed by the systems included in the scope of this engagement.
- We have disclosed all design and operating deficiencies in our controls over PHI of which we are aware, including those for which we believe the cost of corrective action may exceed the benefits.
- No events or transactions have occurred or are pending that would have an effect on the assessment that was performed and used as a basis by HITRUST for issuing this certification report.

We understand that the engagement was conducted in accordance with the security requirements contained in the CSF. We also understand that the sufficiency of this report and the procedures performed is solely the responsibility of report recipients.

Very truly yours,

Authorized Signature

Quality Assurance Process

Within 24-48 hours of submission of a Validated assessment, HITRUST sends out an email to assessor organization requesting the following QA evidence:

- Testing documentation for policy, process and implementation for a HITRUST selected sample of implementation requirements – one from each domain
- Names and frequency of the operational and/or independent measurements and metrics used, as well who reviews them
- Clarification of any implementation requirements marked as N/A

Assessor has 14 days to respond with requested evidence

Report Delivery

Reports are delivered via the MyCSF tool.
The POC on the assessment will be notified via email that a report is ready.

MyCSF Notification: FINAL HITRUST CSF Report Now Available for XYZ Self Assessment
Click here to access this Report

Your Final HITRUST CSF Report is now available for download in MyCSF. You will find it behind the "HITRUST CSF Reports" link of your Assessment Homepage. If you do not have a MyCSF subscription and have only purchased an assessment, your MyCSF access will be removed 30 days from the date the final report is posted.

If you would like to purchase a subscription, please contact sales@hitrustalliance.net. If you need assistance or are having technical problems, please contact support@hitrustalliance.net.

Breakdown of Validated Assessment Report

- Title Page
- Table of Contents
- HITRUST Background
- Letter of Validation … or … Letter of Certification
- Representation Letter from Management
- Assessment Context
- Scope of Systems in the Assessment
- Security Program Analysis
- Assessment Results – Controls required for certification
- Overall Security Program Summary – Benchmarking and breakdown by Domain
- Appendix A – Testing Summary
- Appendix B – Corrective Action Plans (Certification CAPs)
- Appendix C – Corrective Action Plans (Additional GAPs)
- Appendix D – NIST Scorecard
- Appendix E – Questionnaire Results
- Appendix F – System Profile

Report Timeframes

Event	Timeline for Completion
Completing Assessment and Assessor Validation (Report Only vs. Subscription)	90 Days
Days Allowed for Reviewing Draft Report	30 Days
Days Allowed for Submitting CAPs	30 Days
Days Allowed for Assessor to Submit QA Evidence	14 Days
HITRUST Window for Issuance of Draft Report	4-6 Weeks
Date When Interim Assessment Due	1 Year from Date of Certification
Certification Window	2 Years

Interim Review

(Only Applies to Certified Assessment Reports)

- Performed at the 1-year anniversary
- Interim assessment MUST be submitted by the 1-year anniversary date
- Assessor Re-Assessment Process:
  - Request assessed entity to update the scoping questions
  - Review the updated questionnaire for changes to original questionnaire
  - Test at least **1** control/statement in each domain
  - Review the status of any required CAPs from the original assessment and ensure satisfactory progress/milestones are being met
  - Submit results to HITRUST for review

Thank You

Open Discussion and Questions

HITRUST®

Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Content Spotlight