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
• 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
HITRUST Common Security Framework

Certifiable framework to enable common understanding and acceptance

- Leverage existing, globally recognized standards
- Prescriptive requirements
- Scales according to organizational need
- Sector-specific requirements
- Risk-based approach
- Flexibility to adopt alternate controls
- Evolving framework

© 2013 HITRUST, Frisco, TX. All Rights Reserved.
Standards and Regulations Overlap

COBIT

ISO 27001/2

PCI

HIPAA Security

HITECH Act

Meaningful Use

NIST 800-53

States

© 2013 HITRUST, Frisco, TX. All Rights Reserved.
CSF Standards and Regulations Coverage

- ISO 27001/2
- PCI
- NIST 800-53
- HIPAA Security
- HITECH Act
- HITRUST CSF
- Meaningful Use
- States

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

• The CSF has 135 controls
• Each control has 3 levels of implementation
• Implementation levels build on each other as the complexity risk of your organization grows
• Organizations can require different levels of implementation for different controls. Organizations would not be “Level 1” or “Level 2” across the board
• Implementation levels are determined by organizational, system and regulatory factors
CSF Controls Required for Certification

- ISO 27001/2
- PCI
- COBIT
- NIST 800-53
- HIPAA Security
- HITECH Act

- Chosen based upon risk to help organizations assess and remediate efficiently

- Divided into 19 Domains to group questions and maximize the utilization of subject matter experts

© 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.
## CSF Assurance Program – Degrees of Assurance

### Current State

**Proprietary Assessment**
- Wide range of inconsistent controls and requirements from org. to org.
- Wide range of inconsistent questionnaires, tools, and processes from org. to org.
- Wide range of formats for reporting and tracking corrective action plans (CAPs)
- No oversight
- No third party validation of assessment results

### HITRUST CSF Assurance Program

#### Self Assessment
- Common set of controls based on existing standards/regulations
- Standard set of questionnaires, tools, and processes for assessing
- Standard report, compliance scorecard, Corrective Action Plan
- Risk factors encompass all sizes and risks of organizations
- Oversight and governance by HITRUST

#### CSF Validated
- Self assessment plus:
  - Performed by a HITRUST CSF Assessor
  - Prioritized requirements based on industry output and breach analysis
  - HITRUST validates the results and CAP
- Risk factors encompass all sizes and risks of organizations
- Oversight and governance by HITRUST

#### CSF Certified
- CSF Validated plus:
  - No gaps with the prioritized requirements based on CSF controls
  - Established, industry accepted baseline of security requirements
  - Reduced risk and compliance exposure
  - Increased assurance of data protection with third parties
  - HITRUST certifies the results and CAP

- CSF Self Assessments can be conducted by business associate
- CSF Validated or Certified requires third party engagement
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 Assessor
Assessment Options: 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
• 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
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