HITRUST Risk Management Framework and the Texas Certification Program – A Model for the Healthcare Industry

Dr. Bryan Cline, CISSP-ISSEP, CISM, CISA, CCSFP, HCISPP CISO & VP, CSF Development & Implementation
Bryan.Cline@HITRUSTAlliance.net
Introduction

• Multitude of challenges
  – Significant Oversight
  – Evolving requirements
  – Complex business relationships
  – Uncertain standard of care
    • Reasonable & appropriate?
    • Adequate protection?

• HITRUST Risk Management Framework
  – Standard of due care and diligence

• Texas Covered Entity Privacy and Security Certification
  – A model for the healthcare industry
Outline

• Current Environment
• Improving Critical Infrastructure Cybersecurity
• NIST Cybersecurity Framework
• HITRUST Risk Management Framework
• The Cybersecurity Framework and HITRUST
• Texas Certification Program
• Summary/Conclusion
Current Environment

- HIPAA
  - Established initial requirements
    - Vague, non-prescriptive
    - Limited enforcement

- HITECH
  - Expanded scope
  - Incentives and penalties
    - Meaningful Use
    - Data breach notification
    - Increased penalties & enforcement

- Omnibus Rule
  - Integrated HIPAA/HITECH
  - Expanded scope

- Other drivers
  - PCI, FTC Red Flag, FDA, etc.
Current Environment

Inconsistency
Inefficiency
Increasing Costs
Greater Risk

Numerous and ambiguous federal and state regulations

Rapidly changing business, technology and regulatory environment

Inability or failure to implement security in devices and applications

Ineffective and inefficient compliance management

Limited guidance and inconsistent expectations for security across the industry

Increasing breaches in the industry

Greater oversight, scrutiny both internally and externally

Provider
Pharmacies
Bio-tech firms
Device Manufacturers
Information Networks
Health Plans
PBM
Third-Party Processors

© 2014 HITRUST, Frisco, TX. All Rights Reserved.
But what is cybersecurity?

Cybersecurity is as the ability to protect or defend the use of cyberspace—a global domain within the information environment consisting of the interdependent network of information systems infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers]—from cyber attacks, which are attack[s], via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

[from CNSSI 4009, 2010]
Critical Infrastructure Cybersecurity

Information Assurance
- Strategy Focused
- Broader Spectrum of Info Management & Protection
- Concerned with Overall Organization’s Risk & Mitigations
- Examples: Certification, Privacy, Compliance, Audits, BC, DR, Physical (Protect, Detect, React)

Cybersecurity
(Information security & assurance focused on external human threat actors in cyber space)

Information Security
- Tools & Tactics Focused
- Stresses Tech & Operations
- Concerned with Security Applications & Infrastructure
- Examples: A/V, Firewalls, IDSs, VPNs, Pen Testing, Vulnerability Analysis
Critical Infrastructure Cybersecurity

- Dec 2011 - GAO Report
- Aug 2013 - Discussion Draft, Preliminary Cybersecurity Framework
- Feb 2013 - President’s E.O. 13636
- Oct 2013 - Preliminary Cybersecurity Framework
- Feb 2014 - Cybersecurity Framework (Formal Release)
NIST Cybersecurity Framework
NIST Cybersecurity Framework

- SANS 20 Critical Controls for Cyber Security
- NIST SP 800-53
- COBIT, ISO 27001, etc.

Cybersecurity Framework for Critical Infrastructure
NIST Cybersecurity Framework for Critical Infrastructure

- Dams
- Defense Industrial Base
- Transportation Systems
- Chemical
- Communications
- Nuclear
- Energy
- Emergency Services
- Critical Manufacturing
- Commercial Facilities
- Information Technology
- Gov’t Facilities
- Healthcare and Public Health
- Financial Services
- Food and Agriculture
- Water

© 2014 HITRUST, Frisco, TX. All Rights Reserved.
NIST Cybersecurity Framework

Cybersecurity Framework for Critical Infrastructure

- Dams?
- Transportation Systems?
- Chemical?
- Communications?
- NISPO
- HITRUST RMF
- SOX, GLBA
- PCI-DSS
- Food and Agriculture?
- Water?
- Emergency Services?
- Critical Manufacturing?
- Commercial Facilities?
- Information Technology?
- NIST
- CEDS
## NIST Cybersecurity Framework

<table>
<thead>
<tr>
<th>Function</th>
<th>Categories</th>
<th>Subcategories</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROTECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DETECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RESPOND</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECOVER</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# NIST Cybersecurity Framework

<table>
<thead>
<tr>
<th>Unique Identifier</th>
<th>Function</th>
<th>Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RM</td>
<td>Risk Management</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AT</td>
<td>Awareness &amp; Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP</td>
<td>Info Protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>AE</td>
<td>Anomalies &amp; Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>PL</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>
# NIST Cybersecurity Framework

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td>(ID)</td>
<td>IDAM-1: Identify and track physical devices and systems within the organization</td>
<td>- ISA 99.02.01 4.2.3.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IDAM-3: Identify organizational network</td>
<td>- C081T BA103.04, BA109.m, BA109, BA109.0:5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IDAM-5: Identify classification / criticality / business value of hardware, devices, and software</td>
<td>- ISO/IEC 27001 A-1-1.1, A-7.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- NIST SP 800-53 Rev ‘4 CM-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- CCSCS1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- ISA 99201 4.2.3.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- C081T DS05.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- ISO/IEC 27001 A-7, 1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- NIST SP 800-53 Rev. 4 CA-3, CM-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- CCSCS 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- NIST SP 500-2913, 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- NIST SP 800-53 Rev ‘4 AC-20, SA-9</td>
</tr>
</tbody>
</table>

Asset Management (AM): Identify and manage assets that enable the organization to perform its business objectives, in support of effective risk decision-making.

IDAM-1: Identify and track physical devices and systems within the organization.

IDAM-3: Identify organizational network.

IDAM-5: Identify classification / criticality / business value of hardware, devices, and software.
## Threat Mitigation Profile: Cybersecurity Intrusion

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategories</th>
<th>IR</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Risk Assessment</td>
<td>• Identify threats to organizational assets (both internal and external)</td>
<td>NIST SP 800-53 Rev. 4 PM-16</td>
<td>Allows the organization to identify current known IP addresses for adversary servers and block inbound and outbound connections to this source.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Identify providers of threat information</td>
<td>ISO/IEC 27001 A.13.1.2</td>
<td></td>
</tr>
</tbody>
</table>
## NIST Cybersecurity Framework

<table>
<thead>
<tr>
<th>Cybersecurity Implementation Tiers</th>
<th>Cybersecurity Implementation Tier Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tier 0: Partial</strong></td>
<td>Organization has not yet implemented a formal, threat-aware risk management process and may implement some portions of the framework on an irregular, case-by-case basis; may not have capability to share cybersecurity information internally and might not have processes in place to participate, coordinate or collaborate with other entities.</td>
</tr>
<tr>
<td><strong>Tier 1: Risk-Informed</strong></td>
<td>Organization uses a formal, threat-aware risk management process to develop [target] profile [control requirements]; formal, approved processes and procedures are defined and implemented; adequate training &amp; resources exist for cybersecurity; organization aware of role in “ecosystem” but has not formalized capabilities to interact/share info externally.</td>
</tr>
<tr>
<td><strong>Tier 2: Repeatable</strong></td>
<td>Organization regularly updates [target] profile [control requirements] due to changing threats; risk-informed policies, processes and procedures are defined, implemented as intended, and validated; consistent methods are in place to provide updates when a risk change occurs; personnel have adequate skills &amp; knowledge to perform tasks; organization understands dependencies/partners and can consume information from these partners.</td>
</tr>
<tr>
<td><strong>Tier 3: Adaptive</strong></td>
<td>Organization proactively updates [target] profile [control requirements] based on predictive indicators; actively adapts to changing/evolving cyber threats; risk-informed decisions are part of organizational culture; manages and actively shares information with partners to ensure accurate, current information is distributed and consumed to improve cybersecurity before an event occurs.</td>
</tr>
</tbody>
</table>
NIST Cybersecurity Framework

Cybersecurity Framework for Critical Infrastructure
• Healthcare-centric RMF
  – Rationalizes healthcare-specific requirements
  – Leverages international & U.S. RMFs
  – Single industry approach
    • Current, prescriptive & relevant
    • Free to qualified healthcare organizations
    • Risk-based vs. compliance-oriented
      – Baselines tailored based on multiple risk factors
      – Managed alternate control process
    • Consumable by organizations with limited resources
  – Provides industry standard of due diligence and due care
    • Specifies “reasonable and appropriate” controls
    • Defines “adequate” protection
• Selecting reasonable & appropriate safeguards
  – Two general approaches
    • Conduct comprehensive risk analysis
      – Threat & vulnerability assessment
      – Information asset valuation
      – Information protection control selection
    • Modify general baseline control standard
      – Threat modeling and control selection performed for general threats, vulnerabilities
      – Baseline controls based on confidentiality and criticality requirements
      – Limited risk analysis performed for organization-specific requirements
  – Comprehensive risk analysis too difficult for most
    • Lack of skilled resources, funding, time; limited information
  – Baseline control approach most widely used
    • ISO/IEC 27001/27002, part of the ISO/IEC 27000-series RMF
    • NIST SP 800-53, part of the NIST SP 800-series RMF
    • HITRUST CSF, part of the HITRUST RMF
      – Based on ISO/IEC 27001 and integrates a significant portion of NIST SP800-53 requirements
HITRUST RMF

- Step 1 – Identify risks & define protection requirements
  - 7-step sub-process
- Step 2 – Specify controls
- Step 3 – Implement & manage controls
- Step 4 – Assess & report

© 2014 HITRUST, Frisco, TX. All Rights Reserved.
(1) Identify & Define
- CSF rationalizes industry-relevant regulations & standards into a single overarching framework
  - ISO provides the foundation
  - NIST provides additional prescription
(2) Specify

- Three risk-based control baselines
  - Organizational type and size
  - System requirements
  - Regulatory requirements

- Additional tailoring encouraged
  - Alternate controls: one-time or general use
  - Currently developing additional guidance for risk analysis
• (3) Implement & Manage
  – Trained & certified third-party consulting & assessment firms
    • Readiness assessments
    • Remediation/implementation support
  – Ongoing initiatives
    • Draft integration guidance
      – Ties the control framework with defined security services & available resources
      – Supports development of operational and capital project plans
    • Draft Corrective Action Plan guidance
      – Uses new non-contextual risk ratings from CSF assessments
      – Incorporates contextual factors to support residual risk analysis
      – Supports risk treatment selection and remediation prioritization
(4) Assess & Report

- CSF Assurance Program
  - Cost-effective risk assessment
    - High-risk controls (data breach analysis)
    - HIPAA implementation requirements
  - Certified assessor organizations
  - Standardized reporting
    - Supports third-party assurance for covered entities, business associates and regulators

- Defined assessment methodology
  - PRISMA-based control maturity model supports “repeatable” likelihood estimates
  - Addition of non-contextual impact ratings provides initial risk estimates for analysis
  - Maturity and risk calculations support:
    - Internal baselines
    - External benchmarking
(4) Assess & Report (continued)
   – More on the scoring model
     • For any CSF requirement statement, response is 5 x 5 matrix

<table>
<thead>
<tr>
<th>Level</th>
<th>NC</th>
<th>SC</th>
<th>PC</th>
<th>MC</th>
<th>FC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Implemented</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Measured</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Managed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>NC</td>
<td>Non Compliant (0%)</td>
</tr>
<tr>
<td>SC</td>
<td>Somewhat Compliant (25%)</td>
</tr>
<tr>
<td>PC</td>
<td>Partially Compliant (50%)</td>
</tr>
<tr>
<td>MC</td>
<td>Mostly Compliant (75%)</td>
</tr>
<tr>
<td>FC</td>
<td>Fully Compliant (100%)</td>
</tr>
</tbody>
</table>

• Example yields maturity score of 66, which provides a maturity rating of ‘3’
• Model supports reporting of scores across controls, objectives, domains, etc.
• Addition of non-contextual impact ratings supports risk calculations
  – Derived from work performed by the Defense Department
• Risk ratings support HIPAA risk analysis requirement & remediation planning
  – Rollup of risk ratings can be performed in the same manner as the maturity scores
• High impact yields a risk of .272, a score of 73, or a grade of “C” for this example
• (4) Assess & Report (continued)
  – Tool Support
  • MyCSF
    – GRC-based platform
    – CSF controls
    – Illustrative procedures
    – Assessment scoping
    – Workflow management for assessments and remediation
    – Documentation repository for test plans, CAPs, and supporting documentation
    – Dashboards and reporting
    – Automated submission of assessments for HITRUST validation & certification
HITRUST RMF

- Legislative & regulatory requirements for risk analysis
  - Ill-defined and non-prescriptive

  “Organizations can use targeted risk assessments, in which the scope is narrowly defined, to produce answers to specific questions … or to inform specific decisions[,] … have maximum flexibility on how risk assessments are conducted; … [and] are encouraged to use [NIST] guidance in a manner that most effectively and cost-effectively provides the information necessary to senior leaders/executives to facilitate informed decisions.”
  (NIST SP 800-30 r1, p. 22)

- HITRUST RMF provides an industry standard of due care & due diligence for the management of information-related risk
  - CSF provides harmonized set of information protection safeguards
    - Baselines determined from organizational, system & regulatory risk factors
    - Additional RA used at multiple points in the risk management process
      - Initial / baseline control selection (baseline tailoring)
      - Alternate control analysis
      - Remediation planning
    - CSF Assurance provides standardized approach to organizational risk assessment and reporting
The Cybersecurity Framework & HITRUST

Cybersecurity Framework for Critical Infrastructure

© 2014 HITRUST, Frisco, TX. All Rights Reserved.
### The Cybersecurity Framework & HITRUST

#### NIST Cybersecurity Subcategories mapped to CSF Cybersecurity Controls

<table>
<thead>
<tr>
<th>Cyber</th>
<th>CSF</th>
<th>Cyber</th>
<th>CSF</th>
<th>Cyber</th>
<th>CSF</th>
<th>Cyber</th>
<th>CSF</th>
<th>Cyber</th>
<th>CSF</th>
<th>Cyber</th>
<th>CSF</th>
<th>Cyber</th>
<th>CSF</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID.AM-1</td>
<td>07.a</td>
<td>ID.RM-3</td>
<td>11.c, 11.d</td>
<td>PR.DS-8</td>
<td>09.k, 10.h, 10.k</td>
<td>DE.AE-2</td>
<td>03.a, 03.d, 09.m, 09.ab, 11.c</td>
<td>RS.CO-3</td>
<td>09.b, 09.j–09.n, 09.q, 09.s, 09.v, 09.x, 09.y, 09.za–09.af, 11.b</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.AM-2</td>
<td>07.a</td>
<td>PR.AC-1</td>
<td>01.a–01.f, 01.i, 01.j, 01.l–01.o, 01.q–01.s, 01.v–01.y</td>
<td>PR.DS-9</td>
<td>06.d</td>
<td>DE.AE-3</td>
<td>06.g</td>
<td>RS.CO-4</td>
<td>11.c</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.AM-3</td>
<td>07.a, 09.m</td>
<td>PR.AC-2</td>
<td>01.i, 01.j, 01.l–01.o, 01.v, 01.w</td>
<td>PR.IP-1</td>
<td>10.h, 10.k</td>
<td>DE.AE-4</td>
<td>11.d</td>
<td>RS.CO-5</td>
<td>11.c</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.AM-4</td>
<td>09.e, 09.f</td>
<td>PR.AC-3</td>
<td>01.i, 01.j, 01.l–01.o, 01.v, 01.x, 01.y, 10.f, 10.g</td>
<td>PR.IP-2</td>
<td>10.a</td>
<td>DE.CM-1</td>
<td>06.g, 06.h, 09.ab, 09.ad, 09.ae, 10.h</td>
<td>RS.AN-1</td>
<td>11.c</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.AM-5</td>
<td>03.a, 07.a, 10.a</td>
<td>PR.AC-4</td>
<td>01.a</td>
<td>PR.IP-3</td>
<td>09.b</td>
<td>DE.CM-2</td>
<td>06.g, 10.h</td>
<td>RS.AN-2</td>
<td>11.c, 11.d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.AM-6</td>
<td>03.a</td>
<td>PR.AC-5</td>
<td>01.m</td>
<td>PR.IP-4</td>
<td>09.l</td>
<td>DE.CM-3</td>
<td>06.g, 10.h</td>
<td>RS.AN-3</td>
<td>11.d, 11.e</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.BE-1</td>
<td>12.c</td>
<td>PR.AT-1</td>
<td>02.e</td>
<td>PR.IP-5</td>
<td>12.c</td>
<td>DE.AE-5</td>
<td>09.j</td>
<td>RS.AN-4</td>
<td>11.a–11.d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.BE-1</td>
<td>12.c</td>
<td>PR.AT-2</td>
<td>02.e</td>
<td>PR.IP-6</td>
<td>07.a</td>
<td>DE.CM-5</td>
<td>09.k</td>
<td>RS.MI-1</td>
<td>11.c, 11.d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.BE-2</td>
<td>03.a</td>
<td>PR.AT-3</td>
<td>02.e</td>
<td>PR.IP-7</td>
<td>03.c, 11.d</td>
<td>DE.CM-6</td>
<td>06.g, 06.h</td>
<td>RS.MI-2</td>
<td>11.c, 11.d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.GV-1</td>
<td>01.a, 01.i, 03.a, 10.a, 10.k, 11.c, 12.c</td>
<td>PR.AT-4</td>
<td>02.e</td>
<td>PR.IP-8</td>
<td>12.c</td>
<td>DE.CM-7</td>
<td>01.j, 09.m, 09.ab, 10.m</td>
<td>RS.IM-1</td>
<td>11.d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.GV-2</td>
<td>05.e, 07.a, 09.n, 10.a, 10.f, 10.k, 10.m, 11.a, 11.c, 11.d, 12.c</td>
<td>PR.AT-5</td>
<td>02.e</td>
<td>PR.IP-9</td>
<td>09.m, 12.c</td>
<td>DE.CM-8</td>
<td>09.m, 10.k, 10.m</td>
<td>RS.IM-2</td>
<td>11.d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.GV-3</td>
<td>03.a</td>
<td>PR.DS-1</td>
<td>06.d, 10.f, 10.g</td>
<td>PR.IP-10</td>
<td>02.e, 02.i</td>
<td>DE.DP-1</td>
<td>11.a, 11.c, 11.d</td>
<td>RC.RP-1</td>
<td>12.c</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.RA-1</td>
<td>03.b</td>
<td>PR.DS-2</td>
<td>01.n, 01.x, 09.m, 10.f, 10.g</td>
<td>PR.PT-1</td>
<td>09.q, 09.ac–09.ae</td>
<td>DE.DP-2</td>
<td>06.g, 06.h</td>
<td>RC.IM-1</td>
<td>11.d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.RA-2</td>
<td>11.b</td>
<td>PR.DS-3</td>
<td>07.a</td>
<td>PR.PT-2</td>
<td>09.q</td>
<td>DE.DP-3</td>
<td>11.c, 11.d</td>
<td>RC.IM-2</td>
<td>11.d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.RA-3</td>
<td>03.b, 11.a</td>
<td>PR.DS-4</td>
<td>09.a, 12.c</td>
<td>PR.PT-3</td>
<td>01.n, 09.m, 10.k</td>
<td>DE.DP-4</td>
<td>06.g, 06.h</td>
<td>RC.IM-1</td>
<td>11.d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.RA-4</td>
<td>03.b</td>
<td>PR.DS-5</td>
<td>10.f, 10.g, 10.k</td>
<td>PR.PT-4</td>
<td>01.j, 01.m, 01.n, 01.y, 09.m, 09.s, 09.ab, 09.ac, 10.f, 10.g</td>
<td>RS.PL-1</td>
<td>11.d, 12.c</td>
<td>RC.CO-2</td>
<td>11.c</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.RM-1</td>
<td>03.a–03.d</td>
<td>PR.DS-6</td>
<td>03.a–03.d</td>
<td>PR.PT-5</td>
<td>03.a–03.d</td>
<td>RS.CO-1</td>
<td>11.c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.RM-2</td>
<td>03.a</td>
<td>PR.DS-7</td>
<td>07.a, 09.aa</td>
<td>DE.AE-1</td>
<td>01.n, 09.m</td>
<td>RS.CO-2</td>
<td>11.a, 11.b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2014 HITRUST, Frisco, TX. All Rights Reserved.
### NIST Cybersecurity Subcategories mapped to CSF Controls

<table>
<thead>
<tr>
<th>Cyber</th>
<th>CSF</th>
<th>Cyber</th>
<th>CSF</th>
<th>Cyber</th>
<th>CSF</th>
<th>Cyber</th>
<th>CSF</th>
<th>Cyber</th>
<th>CSF</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID.AM-1</td>
<td>07.a, 07.b</td>
<td>ID.RM-3</td>
<td>11.c, 11.d</td>
<td>PR.DS-8</td>
<td>09.d, 09.k, 10.h, 10.k</td>
<td>DE.AE-2</td>
<td>03.a, 03.d, 09.m, 09.ab, 10.c, 11.c</td>
<td>RS.CO-3</td>
<td>09.a–09.af, 11.b</td>
</tr>
<tr>
<td>ID.AM-2</td>
<td>07.a, 07.b</td>
<td>PR.AC-1</td>
<td>01.a–01.y</td>
<td>PR.DS-9</td>
<td>06.c, 06.d</td>
<td>DE.AE-3</td>
<td>06.g</td>
<td>RS.CO-4</td>
<td>02.a, 05.b, 05.f, 09.f, 11.c</td>
</tr>
<tr>
<td>ID.AM-3</td>
<td>07.a, 09.m</td>
<td>PR.AC-2</td>
<td>01.i–01.o, 01.v, 01.w, 08.a–08.m</td>
<td>PR.IP-1</td>
<td>10.h, 10.k</td>
<td>DE.AE-4</td>
<td>11.d, 11.e</td>
<td>RS.CO-5</td>
<td>05.b, 11.c</td>
</tr>
<tr>
<td>ID.AM-4</td>
<td>01.j, 09.e, 09.f, 09.n, 09.s</td>
<td>PR.AC-3</td>
<td>01.i–01.o, 01.v, 01.x, 01.y, 06.f, 10.f, 10.g</td>
<td>PR.IP-2</td>
<td>10.a, 10.b, 10.l</td>
<td>DE.CM-1</td>
<td>06.g, 06.h, 09.ab, 09.ad, 09 ae, 10.h</td>
<td>RS.AN-1</td>
<td>05.i, 11.c</td>
</tr>
<tr>
<td>ID.AM-5</td>
<td>03.a, 07.a, 07.d, 10.a, 12.a</td>
<td>PR.AC-4</td>
<td>01.a</td>
<td>PR.IP-3</td>
<td>09.b</td>
<td>DE.CM-2</td>
<td>06.g, 08.b, 08.c, 08.e, 10.h</td>
<td>RS.AN-2</td>
<td>05.i, 11.c, 11.d</td>
</tr>
<tr>
<td>ID.AM-6</td>
<td>02.a, 03.a, 10.a, 12.a</td>
<td>PR.AC-5</td>
<td>01.m, 09.d</td>
<td>PR.IP-4</td>
<td>09.j</td>
<td>DE.CM-3</td>
<td>06.g, 10.h</td>
<td>RS.AN-3</td>
<td>11.d, 11.e</td>
</tr>
<tr>
<td>ID.BE-1</td>
<td>09.e, 09.f, 09.g, 12.a, 12.c</td>
<td>PR.AT-1</td>
<td>02.e</td>
<td>PR.IP-5</td>
<td>08.d</td>
<td>DE.CM-4</td>
<td>09.j</td>
<td>RS.AN-4</td>
<td>11.a–11.e</td>
</tr>
<tr>
<td>ID.BE-2</td>
<td>06.a, 12.b</td>
<td>PR.AT-2</td>
<td>02.e</td>
<td>PR.IP-6</td>
<td>07.a, 08.l</td>
<td>DE.CM-5</td>
<td>09.k</td>
<td>RS.MI-1</td>
<td>11.c, 11.d</td>
</tr>
<tr>
<td>ID.BE-3</td>
<td>03.a</td>
<td>PR.AT-3</td>
<td>02.e</td>
<td>PR.IP-7</td>
<td>0.a, 03.c, 04.b, 11.d</td>
<td>DE.CM-6</td>
<td>06.g, 06.h, 09.f</td>
<td>RS.MI-2</td>
<td>11.c, 11.d</td>
</tr>
<tr>
<td>ID.GV-1</td>
<td>01.a, 01.i, 03.a, 04.a, 05.a, 06.i, 08.d, 08.j, 09.o, 10.a, 10.h, 11.c, 12.c</td>
<td>PR.AT-4</td>
<td>02.e</td>
<td>PR.IP-8</td>
<td>12.a–12.e</td>
<td>DE.CM-7</td>
<td>01.i, 08.i, 09.m, 09.ab, 10.m</td>
<td>RS.IM-1</td>
<td>11.d</td>
</tr>
<tr>
<td>ID.GV-2</td>
<td>0.a, 04.a, 05.e, 06.l, 07.a, 08.d, 09.e, 09.n, 09.t, 10.a, 10.f, 10.k, 10.m, 11.a, 11.c, 11.d, 12.c</td>
<td>PR.AT-5</td>
<td>02.e</td>
<td>PR.IP-9</td>
<td>08.h, 09.m, 12.c</td>
<td>DE.CM-8</td>
<td>09.m, 10.k, 10.m</td>
<td>RS.IM-2</td>
<td>11.d</td>
</tr>
<tr>
<td>ID.GV-3</td>
<td>03.a, 06.a</td>
<td>PR.DS-1</td>
<td>06.c, 06.d, 06.f, 07.e, 10.f, 10.g</td>
<td>PR.IP-10</td>
<td>02.e, 02.i, 02.g</td>
<td>DE.DP-1</td>
<td>11.a, 11.c, 11.d</td>
<td>RC.RP-1</td>
<td>12.c, 12.d, 12.e</td>
</tr>
<tr>
<td>ID.RA-1</td>
<td>03.b, 05.i, 05.j, 05.k</td>
<td>PR.DS-2</td>
<td>01.n, 01.x, 05.i, 06.f, 09.m, 09.u, 10.f, 10.g</td>
<td>PR.PT-1</td>
<td>06.i, 09.a, 09.ac–09.ae</td>
<td>DE.DP-2</td>
<td>04.b, 06.g, 06.h</td>
<td>RC.IM-1</td>
<td>11.d</td>
</tr>
<tr>
<td>ID.RA-2</td>
<td>11.b</td>
<td>PR.DS-3</td>
<td>07.a, 08.m, 09.p</td>
<td>PR.PT-2</td>
<td>09.O–09.r</td>
<td>DE.DP-3</td>
<td>05.f, 11.c, 11.d</td>
<td>RC.IM-2</td>
<td>11.d</td>
</tr>
<tr>
<td>ID.RA-3</td>
<td>03.b, 05.g, 11.a</td>
<td>PR.DS-4</td>
<td>08.h, 09.h, 09.z, 09.aa, 12.c</td>
<td>PR.PT-3</td>
<td>01.n, 09.m, 10.k</td>
<td>DE.DP-4</td>
<td>05.f, 11.c</td>
<td>RC.CO-1</td>
<td>11.c, 11.c</td>
</tr>
<tr>
<td>ID.RA-4</td>
<td>03.b</td>
<td>PR.DS-5</td>
<td>06.f, 10.f, 10.g, 10.k</td>
<td>PR.PT-4</td>
<td>01.j, 01.m, 01.n, 01.y, 06.f, 08.g, 09.m, 09.s, 09.ab, 09.ac, 10.f, 10.g</td>
<td>RS.PL-1</td>
<td>11.d, 11.e, 12.c</td>
<td>RC.CO-2</td>
<td>11.c</td>
</tr>
<tr>
<td>ID.RM-1</td>
<td>03.a–03.d</td>
<td>PR.DS-6</td>
<td>05.e, 05.k, 06.b, 06.i, 10.l</td>
<td>PR.PT-5</td>
<td>03.a–03.d</td>
<td>RS.CO-1</td>
<td>05.f11.c</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.RM-2</td>
<td>03.a</td>
<td>PR.DS-7</td>
<td>07.a, 09.aa</td>
<td>DE.AE-1</td>
<td>01.n, 09.j, 09.m</td>
<td>RS.CO-2</td>
<td>11.a, 11.b</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# The Cybersecurity Framework & HITRUST

<table>
<thead>
<tr>
<th>Cybersecurity Framework</th>
<th>HITRUST Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Make Organization-wide Decisions</td>
<td>Adopt the HITRUST CSF</td>
</tr>
<tr>
<td>Step 2: Establish a Target Profile</td>
<td>Determine CSF control baseline using multiple risk-factors; identify alternate controls as needed</td>
</tr>
<tr>
<td>Step 3: Establish a Current Profile</td>
<td>Undergo a CSF assessment</td>
</tr>
<tr>
<td>Step 4: Compare Target and Current Profiles</td>
<td>Request CSF validated or certified report</td>
</tr>
<tr>
<td>Step 5: Implement Target Profile</td>
<td>Prioritize and implement corrective actions identified in the report</td>
</tr>
</tbody>
</table>
## The Cybersecurity Framework7k & HITRI:JST

<table>
<thead>
<tr>
<th>Cybersecurity Implementation Tiers</th>
<th>Cybersecurity Implementation Tier Description</th>
<th>Approximate HITRUST Maturity Levels</th>
<th>Approximate HITRUST Maturity Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 0: Partial</td>
<td>Organization has not yet implemented a formal threat-aware risk management process and may implement some portions of the framework on an irregular, case-by-case basis; may not have capability to share cybersecurity information internally and might not have processes in place to participate, coordinate or collaborate with other entities.</td>
<td>Level 1 - Partial Level 2 - Partial Level 3 - Partial Level 4 - Non-compliant Level 5 - Non-compliant</td>
<td>1 to 3-</td>
</tr>
<tr>
<td>Tier 1: Risk-Informed</td>
<td>Organization uses a formal, threat-aware risk management process to develop [target] profile [control requirements]; formal, approved processes and procedures are defined and implemented; adequate training &amp; resources exist for cybersecurity; organization aware of role in &quot;ecosystem&quot; but has not formalized capabilities to interact/share info externally.</td>
<td>Level 1 - Partial Level 2 - Compliant Level 3 - Compliant Level 4 - Non-compliant Level 5 - Non-compliant</td>
<td>3- to 3+</td>
</tr>
<tr>
<td>Tier 2: Repeatable</td>
<td>Organization regularly updates [target] profile [control requirements] due to changing threats; risk-informed policies, processes and procedures are defined, implemented as intended, and validated; consistent methods are in place to provide updates when a risk change occurs; personnel have adequate skills &amp; knowledge to perform tasks; organization understands dependencies/partners and can consume information from these partners.</td>
<td>Level 1 - Compliant Level 2 - Compliant Level 3 - Compliant Level 4 - Partial Level 5 - Partial</td>
<td>4- to 5-</td>
</tr>
<tr>
<td>Tier 3: Adaptive</td>
<td>Organization proactively updates [target] profile [control requirements] based on predictive indicators; actively adapts to changing/evolving cyber threats; risk-informed decisions are part of organizational culture; manages and actively shares information with partners to ensure accurate, current information is distributed and consumed to improve cybersecurity before an event occurs.</td>
<td>Level 1 - Compliant Level 2 - Compliant Level 3 - Compliant Level 4 - Compliant Level 5 - Compliant</td>
<td>5 to 5+</td>
</tr>
</tbody>
</table>
The Cybersecurity Framework & HITRUST

<table>
<thead>
<tr>
<th>Function</th>
<th>Identify (ID)</th>
<th>Protect (PR)</th>
<th>Detect (DE)</th>
<th>Respond (RS)</th>
<th>Recover (RC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subcategory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Informative References</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COBIT DS05.07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO/IEC 27001 A.10.10.2, A.10.10.4, A.10.10.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIST SP 800-53 R4 CM-3, CA-7, AC-2, IR-S, SC-5, SI-4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CCS ESC 14, 16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HITRUST CSF Ol.b, Ol.c, 01.3, 02i, 06.g, 06.h, 09.b, 09.h, 09.ab, 09.ad, 09.ac, IO.k, ll.d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Cybersecurity Framework & HITRUST

NIST Cybersecurity

NISTSP 800-53

NIST HSR Toolkit

Informative References

Category

Subcategory

Function
The Cybersecurity Framework & HITRUST

Information Security and Privacy Threats / Risk

Cyber-specific Security Risk

NIST RMF

NIST Cybersecurity Framework

NIST SP 800-53

NIST HSR Toolkit

Breadth of Threats / Risks Addressed

Low (Strategic)

High (Tactical)
## The Cybersecurity Framework & HITRUST

<table>
<thead>
<tr>
<th>Function</th>
<th>Identify &amp; Define (ID)</th>
<th>Specify (SP)</th>
<th>Implement &amp; Manage (IM)</th>
<th>Assess &amp; Report (AR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub-function</td>
<td>Security Ops. (SO)</td>
<td>Incident Mgmt. (IN)</td>
<td>...</td>
<td>Educ. &amp; Awareness (EA)</td>
</tr>
<tr>
<td>Category</td>
<td>05.0 Org. of InfoSec</td>
<td>08.0 Phys. &amp; Env. Security</td>
<td>09.0 Comm. &amp; Ops. Mgmt.</td>
<td></td>
</tr>
<tr>
<td>Objective</td>
<td>09.01 Doc. Ops. Procedures</td>
<td>09.02 Control 3rd Party Delivery</td>
<td>09.03 Sys. Planning &amp; Acceptance</td>
<td>...</td>
</tr>
<tr>
<td>Control</td>
<td>09.h Capacity Mgmt.</td>
<td>09.1 System Acceptance</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Informative References (Standard Mappings)
- CSA O9-03
- ISO/IEC 27001 A.10.3.1
- NIST SP 800-53 R4 AU-4, SC-5
- CSS/CSC/14
- NIST Cybersecurity Framework PR OS-4

© 2014 HITRUST, Frisco, TX. All Rights Reserved.
The Cybersecurity Framework & HITRUST

Information Security and Privacy Threats / Risk

Cyber-specific Security Risk

HITRUST RMF

HITRUSTCSF

CSF Assurance

HITRUSTC3

Breadth of Threats / Risks Addressed
The Cybersecurity Framework & HITRUST

Information Security and Privacy Risks

Cyber-specific Security Risk

Breadth of Threats / Risks Addressed

Low (Strategic)

High (Tactical)

NIST/ HITRUST RMF

NIST Cybersecurity Framework

NIST SP 800-53

HITRUST CSF

HITRUSTC3

CSF Assurance

© 2014 HITRUST, Frisco, TX. All Rights Reserved.
Texas Certification Program
Texas Certification Program

- Texas legislators concerned about health information protection
  - Increased use of electronic health records
  - Federal HIPAA guidance lacking
  - Significant increase in data breaches

- Texas House Bill (HB) 300
  - Passed May 30, 2011
  - Signed June 17, 2011
  - Effective Sept. 1, 2012

- Amended the following statutes:
  - Texas Health and Safety Code Chapters 181 & 182;
  - Texas Business and Commerce Code, Chapters 521 and 522;
  - Texas Government Code, Chapter 531; and
  - Texas Insurance Code, Chapter 602
Texas Certification Program

- Maintains the broader, Texas definition of Covered Entity
  - Covers any business or individual coming into contact with PHI
- Supports patient rights re: Electronic Health Records (EHRs)
  - Provides for the collection/reporting of consumer complaints
- Increases penalties for non-compliance/breach
  - $5K to $1.5M per year based on 5 factors, not just intent and risk of harm
  - Capped at $250M per year based on specific circumstances
  - A pattern of non-compliance could result in license revocation
- Establishes Texas standards for healthcare information privacy and security
  - Standards ratified by Texas Health and Human Services Commission and codified at 1 TAC § 390
- Provides for certification of compliance with the Texas standards
  - Potential for mitigation of regulatory and legal penalties

© 2014 HITRUST, Frisco, TX. All Rights Reserved.
Texas Certification Program

- THSA selects HITRUST for Texas certification program
- HITRUST Risk Management Framework (RMF) provides robust support for Texas certification
  - Comprehensive coverage, relevant to healthcare, that is scalable, prescriptive and tailorable to meet entity requirements
  - Certification supports assertions of compliance
  - Common framework & reporting provide significant efficiency & cost savings
  - Most widely adopted information protection framework in U.S. healthcare industry simplifies adoption

“For this program to be successful, it must provide the appropriate level of assurance and verification while still being practical and implementable; therefore, it was important we select the best possible partner for developing and implementing the Texas Covered Entity Privacy and Security Certification Program. We are confident in our choice given HITRUST’s leading role in the assessment and certification of compliance with multiple health information protection regulations and best practices through the HITRUST Common Security Framework (CSF).” - Tony Gilman, CEO, THSA
Texas Certification Program

• In addition to the those provided by leveraging the HITRUST RMF, covered entities receive specific benefits from obtaining Texas Covered Entity Privacy and Security Certification
  – Mitigation of civil and administrative penalties
  – Evidence of good faith efforts to comply with federal and state requirements
## Texas Certification Program

- **Examples of Texas requirements mapped to the CSF**

<table>
<thead>
<tr>
<th>CSF Control</th>
<th>TX Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>All HIPAA xRefs</td>
<td>Texas Health and Safety Code (THSC) § 181.004a – A covered entity, as that term is defined by 45 C.F.R. Section 160.103, shall comply with the Health Insurance Portability and Accountability Act and Privacy Standards.</td>
</tr>
<tr>
<td>02.e, Level 1</td>
<td>THSC § 181.101(a) – Each covered entity shall provide a training program to employees of the covered entity regarding the state and federal law concerning protected health information as it relates to the covered entity's particular course of business and each employee's scope of employment.</td>
</tr>
<tr>
<td>07.e, Level 1</td>
<td>THSC § 81.103, referenced by 1 Texas Administrative Code (TAC) § 390.2(a)(4)(A)(ii) – Specifies that care shall be given to ensure sensitive information subject to special handling, e.g., HIV test results, mental health and substance abuse-related records, is identified and appropriate labeling and handling requirements are expressly defined and implemented consistent with applicable federal and state legislative and regulatory requirements and industry guidelines.</td>
</tr>
<tr>
<td>11.a, TX Covered Entities</td>
<td>THSC § 577, referenced by 1 TAC § 390.2(a)(4)(A)(ii) – To comply with the requirements specified in THSC § 577, private psychiatric (mental) hospitals, crisis stabilization units and other mental health facilities shall incorporate procedures in their security and privacy incident response programs to assist with state investigations, including the release of otherwise confidential information related to the investigation, as required under THSSC 157.</td>
</tr>
</tbody>
</table>

*Refer to the 2013 CSF, 2013 interim Summary of Changes, and the 2014 Summary of Changes for all the Texas certification requirements*
Texas Certification Program

- Texas Covered Entity Privacy and Security Certification
  - Completely flexible implementation, as organizations may:
    - Request Texas certification with CSF (HIPAA) assessment
    - Increment to Texas Certification after CSF (HIPAA) assessment is done
  - Varying levels and 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 privacy and security controls that is required to appropriately understand and mitigate risk.
Texas Certification Program

- Covered entity engages independent assessor organization*
- CSF Assessor conducts assessment against certification requirements
- CSF assessor submits assessment results to HITRUST for review
- HITRUST conducts QA review; resolves outstanding issues
- HITRUST prepares report with Texas Certification “Scorecard”
- If covered entity achieves appropriate scores, HITRUST will provide a certification recommendation to be submitted to THSA
- THSA reviews recommendation and issues certification letter
- Covered entity is added to website listing certified covered entities

*Small organizations may elect for a remote-assessment
Texas Certification Program

• The Texas Covered Entity Privacy and Security Certification
  – Is competitively priced and sufficiently robust to support wide adoption;
  – Demonstrates compliance with the Texas Medical Records Privacy Act and associated standards;
  – Specifically addresses high-risk threats associated with reported data breaches;
  – Supports overall compliance with HIPAA (Final Omnibus Rule) implementation specifications;
  – Leverages HITRUST’s online GRC-based tool, MyCSF, to provide automated workflow for certification assessment, quality assurance and reporting;
  – Provides a standardized method of reporting compliance and risk, including the recommendation for Texas certification;
  – Facilitates the communication of assurances with other business partners, patients and their families, and other key stakeholders, such as federal and state regulators; and
  – Provides for potential mitigation of regulatory and legal penalties
Texas Certification Program

Cybersecurity Framework for Critical Infrastructure

HITRUST RMF
About HITRUST

• Born out of the belief that information protection should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges
• Led by a seasoned management team; governed by a Board of Directors made up of leaders from across the healthcare industry and its supporters

• More than seven years experience as the only industry-wide information protection standards and certification body in healthcare
• Driving adoption and widespread confidence in sound risk management practices through education, advocacy and other activities
About THSA

• In 2007, the Texas Legislature created THSA to help improve the Texas healthcare system
  – Promote and coordinate HIE and HIT throughout the state
  – Ensure right information available to right provider at the right time
• In 2011, the Texas Legislature authorized THSA to:
  – Identify relevant privacy and security standards
  – Develop a privacy and security certification for Texas covered entities
• In 2013, THSA partnered with HITRUST to create the Texas Covered Entity Privacy and Security Certification Program
Questions?

Dr. Bryan Cline, CISSP-ISSEP, CISM, CISA, ASEP, CCSFP
(469) 269-1118 | Bryan.Cline@HITRUSTalliance.net
ADDITIONAL MATERIAL
Availability & Pricing

• Projected Timeline

- Feb 2013 – HB 300 req’ts incorporated in the CSF
- Oct 2013 – TX standards incorporated in the CSF
- Jan 2014 – HIPAA Privacy Rule Requirements based on OCR Audit Protocol incorporated into MyCSF (not yet a formal part of the CSF)
- Begin formal assessment & certification
- Prepare for formal assessment & certification
Availability and Pricing

• Covered entity assessment and report generation fee
  – Certification Remote Assessment (if applicable)
    • $3500 to perform remote assessment and generate recommendation for Texas Certification
    • $1000 if adding Texas certification to an existing HITRUST certification
  – Certification Third Party Assessment
    • $3750 - $7500 to review third party assessment and generate recommendation for Texas Certification
    • $1500 if adding Texas certification to existing HITRUST certification
  – Fees paid to HITRUST

• Covered entity certification fee
  – Certification Remote Assessment: $1500
  – Certification Assessment: $2500 - $7500 (depending on revenue)
  – Fees paid to THSA
# Availability and Pricing

<table>
<thead>
<tr>
<th>Fee Schedule TX Only</th>
<th>Remote &lt; $5M</th>
<th>Third Party &lt; $50M</th>
<th>Third Party &lt; $500M</th>
<th>Third Party &lt; $1B/yr</th>
<th>Third Party &lt; $10B</th>
<th>Third Party &gt;$10B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessor Fees</td>
<td>N/A</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>HITRUST Fees</td>
<td>$3500</td>
<td>$3750</td>
<td>$4500</td>
<td>$5250</td>
<td>$6000</td>
<td>$7500</td>
</tr>
<tr>
<td>THSA Fees</td>
<td>$1500</td>
<td>$2500</td>
<td>$3250</td>
<td>$5000</td>
<td>$6250</td>
<td>$7500</td>
</tr>
<tr>
<td>Total</td>
<td>$5000</td>
<td>$6250</td>
<td>$7750</td>
<td>$10,250</td>
<td>$12,250</td>
<td>$15,000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fee Schedule TX Added to CSF</th>
<th>Remote &lt; $5M</th>
<th>Third Party &lt; $50M</th>
<th>Third Party &lt; $500M</th>
<th>Third Party &lt; $1B/yr</th>
<th>Third Party &lt; $10B</th>
<th>Third Party &gt;$10B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessor Fees</td>
<td>N/A</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>HITRUST Fees</td>
<td>$1000</td>
<td>$1500</td>
<td>$1500</td>
<td>$1500</td>
<td>$1500</td>
<td>$1500</td>
</tr>
<tr>
<td>THSA Fees</td>
<td>$1500</td>
<td>$2500</td>
<td>$3250</td>
<td>$5000</td>
<td>$6250</td>
<td>$7500</td>
</tr>
<tr>
<td>Total</td>
<td>$2500</td>
<td>$4000</td>
<td>$4750</td>
<td>$6500</td>
<td>$7750</td>
<td>$9000</td>
</tr>
</tbody>
</table>