



HITRUST – Silver bullet of healthcare compliance?

MN HIMSS Spring Conference



Agenda

- Introduction to HITRUST CSF
- Getting Started With CSF
- CSF is not...
- CSF is...
- What does it all mean?

The Acronym Game

- HIPAA – Health Insurance Portability and Accountability Act
- PHI – Protected Health Information
- HITECH – Health Information Technology for Economic and Clinical Health

The Acronym Game

- CMS – Centers for Medicare & Medicaid Services
- NHIN – Nationwide Health Information Network
- HITSP – Healthcare for Information Technology Standards Panel

The Acronym Game

- OCR – Office of Civil Rights
- ARRA - American Recovery and Reinvestment Act of 2009
- PCI – Payment Card Industry
- NIST – National Institute of Standards and Technology

The Acronym Game

What do all these acronyms have in common?

The Acronym Game

They all impact the healthcare
industry...
and make your life a lot more
complicated

Had enough yet?

- Additional Healthcare organizations, standards and regulations include:
 - ONC - Office of the National Coordinator for Health Information Technology
 - EHNAC - Electronic Healthcare Network Accreditation Commission
 - NHIN—Nationwide Health Information Network
 - AHIMA—American Health Information Management Association
 - URAC—formerly known as the “Utilization Review Accreditation Commission”
 - NAHIT—The National Alliance for Health Information Technology
 - AMA—American Medical Association
 - IOM—Institute of Medicine
 - GINA—Genetic Information Non-discrimination Act

Had enough yet?

- What about non-healthcare related?
 - SAS 70
 - SysTrust
 - NIST
 - FISMA
 - PCI
 - ISO
 - COBIT
 - ITIL

HITRUST

- Health Information Trust Alliance (HITRUST), a for-profit company that created the Common Security Framework (CSF)
- The framework was created collaboratively with over 140 healthcare providers, payers, and service providers
- HITRUST has positioned itself as a certification body that will allow companies to demonstrate their acceptance of the CSF framework
- Certification does not mean that the organization has implemented 100% of the controls described within the framework
- HITRUST Alliance leverages the power of the healthcare community in defining a minimum set of requirements, intended to move security and compliance posture in the right direction.

HITRUST Executive Council



Jim Ansell
Chief Information Security Officer
Highmark Inc.



Robert E. Booker
Chief Information Security Officer
UnitedHealth Group



Roy R. Mellinger, CISSP-ISSAP, ISSMP, CIM
Vice President, IT Security & Chief Information
Security Officer
WellPoint, Inc.



Jon Moore
Chief Information Security Officer
Humana Inc.



Paul Connelly
Vice President and
Chief Information Security Officer
Hospital Corporation of America



Frank Grant
Senior Director - US Healthcare
Cisco Systems, Inc.



Daniel Nutkis
Chief Executive Officer
HITRUST



Russell Pierce
Chief Information Security Officer
CVS Caremark



Kimberly Gray, Esq., CIPP
Chief Privacy Officer, Americas Region
IMS Health



Patrick Heim
Chief Information Security Officer
Kaiser Permanente



Michael Wilson
Vice President and
Chief Information Security Officer
McKesson Corporation

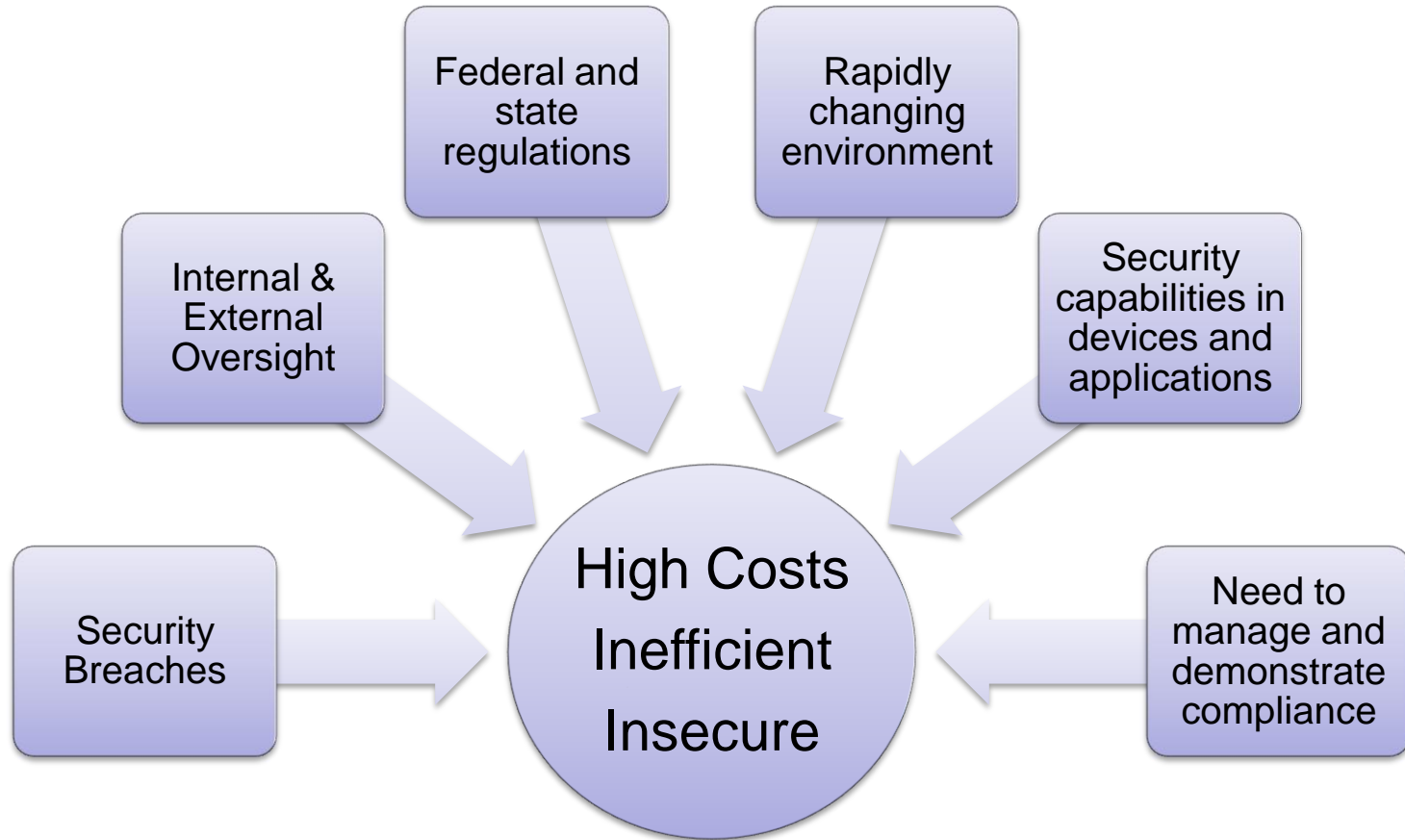


Mark Kinnunen
Chief Information Security Officer
Express Scripts, Inc.



Robert Mandel, MD
Senior Vice President, Health Care Services
BlueCross BlueShield of Tennessee

Why Do You Need a CSF?



HITRUST - CSF

- The CSF is designed based on the ISO/IEC 27001:2005 and ISO/IEC 27002:2005 standards. Additionally, the framework includes:
 - Healthcare:
 - HIPAA (August, 1996)
 - HITECH Act, Subpart D
 - CMS Information Security ARS Appendix A-CMSR (HIGH)
 - JCAHO Information Management(IM)
 - Frameworks:
 - ISO 27799:2008
 - NIST SP 800-53 (February, 2005) and SP 800-26 (April, 2005)
 - CobiT 4.0 (2005)
 - Other Regulations / Requirements
 - PCI Data Security v1.2 (October 2008)
 - 16 CFR Part 681 - Identity Theft Red Flags
 - 201 CMR 17.00 (State of Massachusetts Data Protection Act)
 - NRS 603A (State of Nevada - Security of Personal Information)
 - CSA Cloud Controls Matrix v1

HITRUST - CSF

- Each control described within the framework includes basic information such as control objectives, descriptions, and a few different categories that it may be associated with, consistent with other frameworks
- CSF also includes:
 - Control Implementation
 - Control Audit Procedures
 - Control Standards Mapping
 - Alternative Controls
 - Required for Certification
 - Organizational or System

HITRUST - CSF

- HITRUST incorporated different levels ranging from Level 1 to Level 3
- The appropriate implementation level is established by an evaluation of organizational and system factors, combination of which help determine the specific control required for implementation
- HITRUST has created spreadsheets where an organization simply needs to fill out some basic information in order to see required levels of implementation for each organization / division / system

CSF Sample

Structured in accordance with ISO 27001 / 27002 standard

▼ General Information

Control Reference: 11.a Reporting Information Security Events	Control Objective: 11.0 - Information Security Incident Management 11.01 Reporting Information Security Incidents and Weaknesses
Control Specification: Information security events shall be reported through appropriate communications channels as quickly as possible. All employees, contractors and third party users shall be made aware of their responsibility to report any information security events as quickly as possible. *Required for HITRUST Certification 2009	
Factor Type: Organizational	

▼ Level 1 Implementation Requirement

Level 1 Organizational Factors: BioTech Organizations: < \$100,000 Spend on Research and Development Per Year Pharmaceutical Companies: < 20,000,000 Prescriptions Per Year Third Party Processor: < 1,000,000 Records Processed Per Year Physician Practice: < 22,500 Visits Per Year Medical Facilities / Hospital: < 1,000 Licensed Beds Health Plan / Insurance: < 1,000,000 Covered Lives	Risk factors tailored for healthcare organizations
Level 1 Regulatory Factors: None	
Level 1 Implementation: Formal information security event reporting procedures to support the corporate direction (policy) shall be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event, and the timeliness of reporting and response. With the importance of Information Security Incident Handling, a policy shall be established to set the direction of management. A point of contact shall be established for the reporting of information security events. It shall be ensured that this point of contact is known throughout the organization, is always available and is able to provide adequate and timely response.	
Level 1 Control Audit Procedure: Examine: i. The organization's information security policy to ensure information security event reporting procedures that support the corporate direction have been established. ii. The organization's information security policy to ensure an incident response. iii. The organization's information security policy to ensure it defines the point of contact for reporting of information security events. iv. The organization's information security policy and/or organizational structure to ensure the point of contact is known throughout the organization. Interview: i. Management to verify the direction of the organization relating to information security and incident reporting, response and escalation is aligned with the policy. ii. Select organization personnel to verify that the point of contact is known throughout the organization. iii. The point of contact for incident reporting to verify his/her awareness of his/her responsibilities as defined in the policy and procedures. Test i. None	Multiple levels of implementation requirements
Level 1 Control Standard Mapping: • HIPAA §164.312 (a)(6)(ii)	Cross-references to industry standards and regulations

▼ Level 1 Alternate Controls

Control Name ↕	Control ID	Control Type	Control Description
No records specified.			

Cross-references to industry standards and regulations

Organizational Risk Factors

- Biotech Organizations: \$ Spent on Research and Development Per Year
- Third Party Processor: Records Processed Per Year
- Physician Practice: Visits Per Year
- Medical Facilities / Hospital: Licensed Beds
- Health Plan / Insurance / PBM: Covered Lives
- IT Service Providers (Vendors): Employees
- Pharmacy Companies: Prescriptions Per Year

System Risk Factors

- Processing PHI: Yes / No
- Accessible from the Internet: Yes / No
- Exchanges Data with a Business Partner: Yes / No
- Third Party Support (Vendor Access or Maintenance): Yes / No
- Publicly Accessible: Yes / No
- Used Directly by Mobile Devices: Yes / No
- Number of Interfaces to Other Systems
- Number of Users of the System
- Number of Transactions per Day

Common Risk Factors

- Regulatory:
 - Subject to PCI
 - Subject to FISMA
 - Subject to FTC Red Flags rules
 - Subject to HITECH Breach Notification
- Geographical Factors:
 - State
 - Multi-state
 - Off-shore

Sample Profiles

5	HITRUST CSF System Controls				
6	HITRUST CSF System Controls				
7	Control Category	Ref.	Implementation Requirements		
8	1 - Access Control	1.b	Level 1	Level 2	Level 3
9		1.c	Level 1	Level 2	
10		1.d	Level 1	Level 2	
11		1.e	Level 1		
12		1.k	Level 1		
13		1.p	Level 1		
14		1.q	Level 1		
15		1.r	Level 1	Level 2	
16		1.s	Level 1	Level 2	
17		1.t	Level 1		
18		1.u	Level 1		
19		1.v	Level 1	Level 2	Level 3
20		1.w	Level 1		
21		1.x	Level 1		
22	9 - Communication and Operations	9.a	Level 1	Level 2	
23		9.b	Level 1	Level 2	
24		9.d	Level 1	Level 2	
25		9.e	Level 1	Level 2	
26		9.f	Level 1	Level 2	Level 3
27		9.g	Level 1	Level 2	
28		9.h	Level 1	Level 2	
29		9.i	Level 1	Level 2	
30		9.aa	Level 1	Level 2	
31		9.ab	Level 1	Level 2	Level 3
32		9.ac	Level 1	Level 2	Level 3
33	9.ad	Level 1	Level 2		

5	HITRUST CSF Organizational Controls					
6	HITRUST CSF Organizational Controls					
7	Control Category	Ref.	Implementation Requirements			
8	0 - Information Security	0.a	Level 1	Level 2		
9		1 - Access Control	1.a	Level 1	Level 2	
10			1.f	Level 1		
11			1.g	Level 1		
12			1.h	Level 1		
13			1.i	Level 1		
14			1.j	Level 1		
15			1.l	Level 1		
16			1.m	Level 1	Level 2	
17			1.n	Level 1		
18			1.o	Level 1		
19			1.y	Level 1	Level 2	Level 3
20			2 - Human Resources Security	2.a	Level 1	
21				2.b	Level 1	
22				2.c	Level 1	
23		2.d		Level 1	Level 2	
24		2.e		Level 1	Level 2	
25		2.f		Level 1		
26		2.g		Level 1		
27	2.h	Level 1				
28	2.i	Level 1				
29	3 - Risk Management	3.a	Level 1			
30		3.b	Level 1			
31		3.c	Level 1			
32		3.d	Level 1			

Alternative Controls

- HITRUST allows organizations to submit alternative controls for consideration
- HITRUST will maintain an authoritative list of approved alternative controls, and publish them in the CSF
- The HITRUST Alternative Controls Committee (ACC) was formed to facilitate discussions among service providers, healthcare providers, medical device manufacturers, and other key parties with regards to alternative controls for addressing control failures when certifying to the HITRUST CSF

Primary Drivers

- Strengthening an organization's compliance posture
 - Created, maintained and vetted by experts in consultation with industry
 - Most widely adopted
- Incorporates third party, industry-accepted, validation of your security program
 - Efficiency of internal security program
 - Leverages globally recognized standards, including HIPAA, HITECH, NIST, ISO, PCI, FTC and Cobit
- Lowers costs associated with monitoring and keeping pace with the evolving regulatory environment
 - Management of business associates
 - Establishes a commercially reasonable approach to measuring business associates
 - Provides common security baseline and method for communicating security controls between parties

CSF is Not...

- A new framework
- Required
- Proof of HIPAA (or any other) regulatory compliance
- Replacement for authoritative sources
- Requiring organization to achieve or even pursue certification

CSF is...

- Healthcare Industry approved risk-based approach to determining appropriate controls.
- Easy to leverage and scale
- Great for third-party risk management
- Capable of reducing the cost of managing compliance

HITRUST CSF Potential

- The CSF can be used as a baseline for an internal Information Security Program.
- Once implemented, compliance with any of the standards included in the framework can be quickly established and demonstrated.
- The CSF can provide system implementation guidelines / requirements for all existing and new technology acquisitions.
- The implementation roadmap can be used to not only recognize gaps, but also celebrate and document accomplishments.
- The CSF can be used to strengthen the third-party risk management efforts by holding vendors to the same standards.

Summary

- The HITRUST CSF continues to gain popularity and broader acceptance, and organizations can begin benefitting from the framework right away
- Based on ISO, early adopters risk little by integrating CSF into security frameworks
- Proactively offering an assessment under the CSF Assurance Program is an acceptable alternative to third-party risk assessments that will help simplify vendor risk management

About NetSPI

- Our HITRUST certified CSF Practitioners can help you take advantage of the CSF by using it to streamline current security program management efforts
- NetSPI offers a full range of Information Security and Compliance services

HITRUST SIG - MN

Meets last Tuesday of every month

Next meeting: May 31st, 2:30pm – 4:30pm

Fairview Health Services

400 Stinson Blvd

Minneapolis, MN 55413

More information: <http://hitrustsigmn.web.officelive.com/>

RSVP: <http://hitrustsigmn.eventbrite.com/>

Questions & Answers

Thank You

NetSPI

800 Washington Avenue North
Minneapolis, MN 55401
612-465-8880





netsp*i*
RISK COMPLIANCE SECURITY