

G22 - A Security and Compliance Risk Management Framework for Health Care

Bryan Cline



September 21, 2009 – September 23, 2009



An Information Security and Compliance Risk Management Framework for Healthcare

Bryan S. Cline, PhD, MSIE
CISM, CISA, CISSP-ISSEP, CPP, CAP (PM Lvl II), ASEP
Chief Information Security Officer, The Children's Hospital of Philadelphia



September 21, 2009 – September 23, 2009



Information Security and Compliance Risk Management

- Why do it?
- What is it?
- How does CHOP do it?
 - Then ... InfoSec
 - Now ... InfoSec risk management
 - Future ... unified InfoSec & compliance risk mgmt
- The Health Information Trust (HITRUST) Alliance
 - Introduction / features



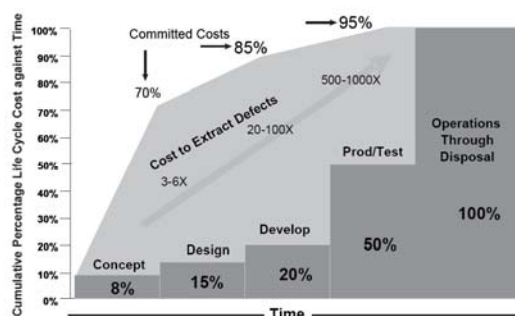
Why Do It?

- Why do information security and compliance risk management at all?
 - To protect information that has value
 - To avoid costs associated with non-compliance
- What are some of the threats?
 - Loss of value
 - Examples: trade secrets, proprietary information
 - Misappropriation of value
 - Examples: identity, intellectual property
 - Regulatory and civil penalties
 - Examples: fines, fees, damages (monetary)

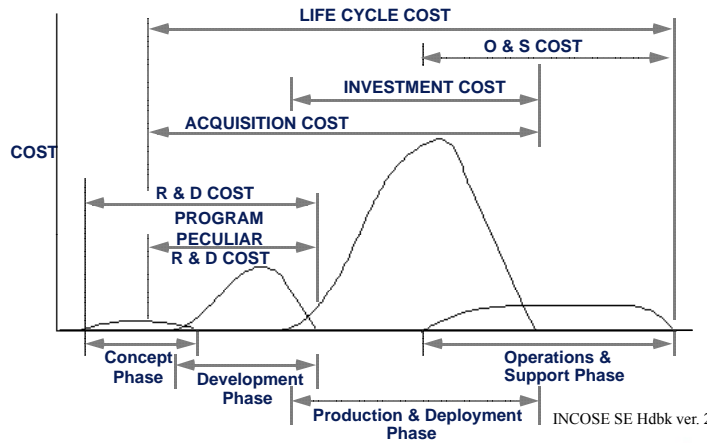


Why Do It?

- Costs increase with the stage in the SDLC the security “defect” is identified and subsequently corrected



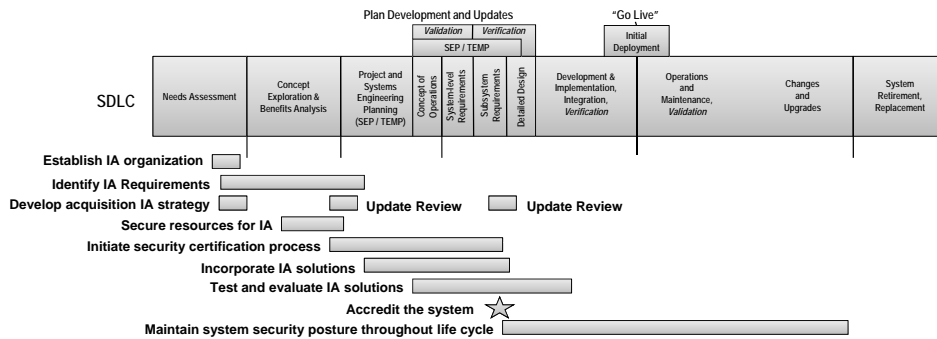
Why Do It?



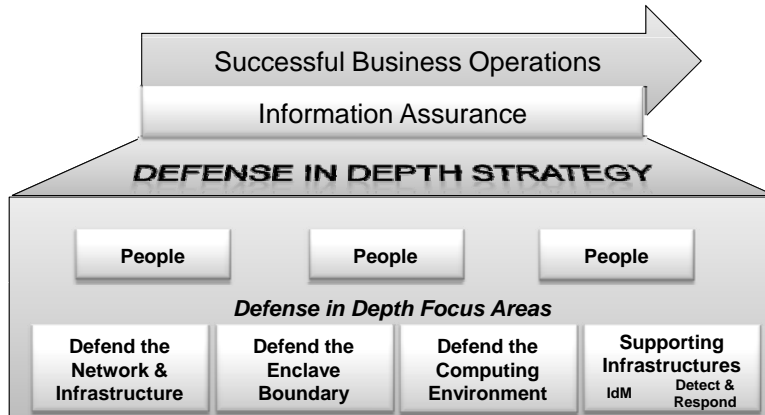
INCOSE SE Hdbk ver. 2a



Why Do It?

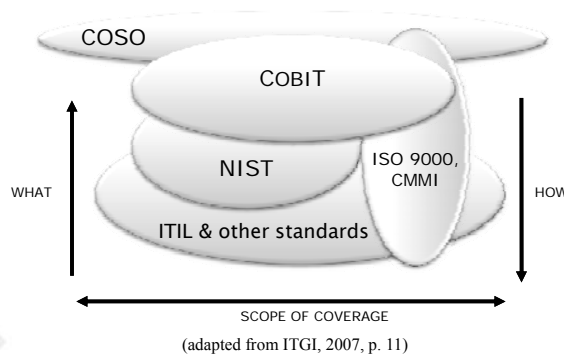


Why Do It?



Why Do It?

- As a part of an overall enterprise governance and risk management program



What Is It?

- Enterprise risk management
 - “... is a process, effected by an entity’s board of directors, management, and other personnel, applied in a strategy setting and across the enterprise, designed to
 - identify potential events that may affect the entity, and
 - manage risk to be within its risk appetite,
 - to provide reasonable assurance regarding the achievement of entity objectives.” (COSO, 2004, p. 2)



What Is It?

- Information security [& compliance] risk mgmt
 - is intended to “balance the benefits gained from the use of ... information systems with the risk of these ... systems being the vehicle through which [threats] cause mission or business failure.” (NIST, 2007, p. 1), and
 - “is made up of *Information security incorporated into the*
 - Enterprise architecture
 - System development life cycle (“birth-to-death”) (NIST, 2007, p. 1)



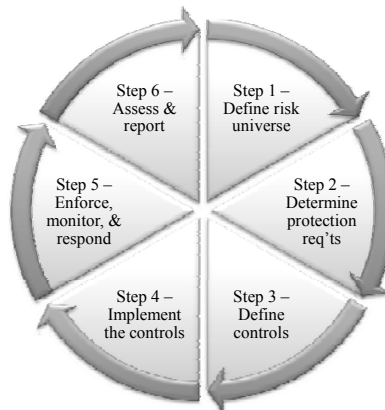
What Is It?

- In general, risk management is
 - “the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and
 - “deciding what [controls or safeguards], if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization”



What Is It?

- Step 1: Understand and define the information risk universe
- Step 2: Determine confidentiality, integrity, and availability requirements
- Step 3: Define required controls
- Step 4: Implement the controls
- Step 5: Develop enforcement, monitoring, and response mechanisms
- Step 6: Assess and report



“Hamster Wheel of Pain”



What Is It?

- ***Step 1: Understand and define the information risk universe***
- Step 2: Determine confidentiality, integrity, and availability requirements
- Step 3: Define required controls
- Step 4: Implement the controls
- Step 5: Develop enforcement, monitoring, and response mechanisms
- Step 6: Assess and report



What Is It?

- Step 1: Understand and define the information risk universe
- ***Step 2: Determine confidentiality, integrity, and availability requirements***
- Step 3: Define required controls
- Step 4: Implement the controls
- Step 5: Develop enforcement, monitoring, and response mechanisms
- Step 6: Assess and report



What Is It?

- Step 1: Understand and define the information risk universe
- Step 2: Determine confidentiality, integrity, and availability requirements
- **Step 3: Define required controls**
- Step 4: Implement the controls
- Step 5: Develop enforcement, monitoring, and response mechanisms
- Step 6: Assess and report



What Is It?

- Step 1: Understand and define the information risk universe
- Step 2: Determine confidentiality, integrity, and availability requirements
- Step 3: Define required controls
- **Step 4: Implement the controls**
- Step 5: Develop enforcement, monitoring, and response mechanisms
- Step 6: Assess and report



What Is It?

- Step 1: Understand and define the information risk universe
- Step 2: Determine confidentiality, integrity, and availability requirements
- Step 3: Define required controls
- Step 4: Implement the controls
- *Step 5: Develop enforcement, monitoring, and response mechanisms*
- Step 6: Assess and report



What Is It?

- Step 1: Understand and define the information risk universe
- Step 2: Determine confidentiality, integrity, and availability requirements
- Step 3: Define required controls
- Step 4: Implement the controls
- Step 5: Develop enforcement, monitoring, and response mechanisms
- *Step 6: Assess and report*



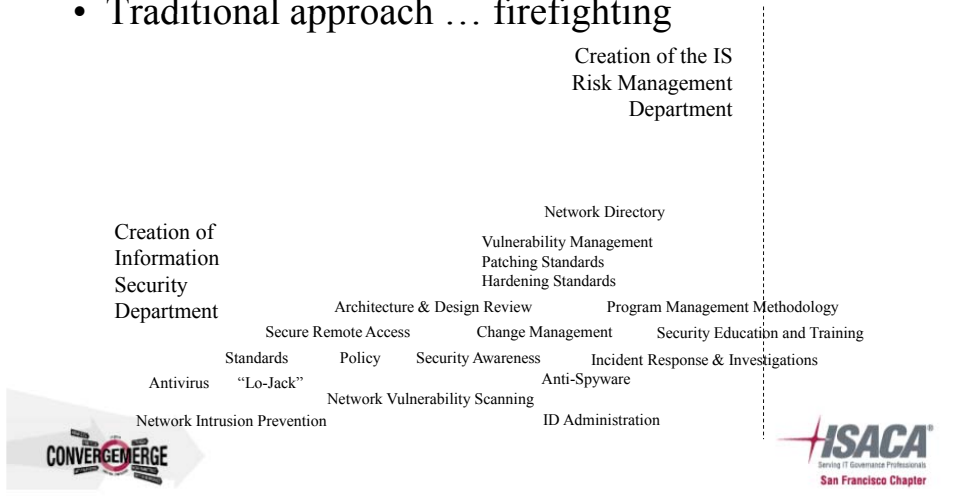
How Does CHOP Do It?

- Then ... information security
 - Traditional
 - Fire-fighting
 - (Pain) Point solutions
 - “Best” (i.e., common) practices
 - Candidates frameworks identified but not adopted
 - COBIT, NIST



How Does CHOP Do It?

- Traditional approach ... firefighting



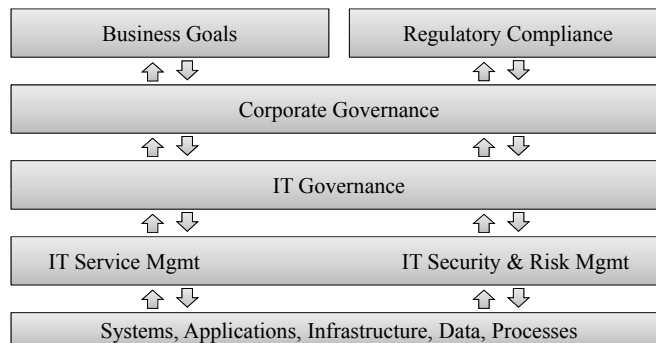
How Does CHOP Do It?

- Now ... information security risk management
 - Progressive
 - Proactive
 - Focused on synergistic solutions
 - Based on formal frameworks and methodologies



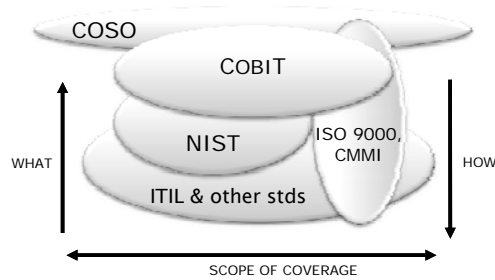
How Does CHOP Do It?

- Frameworks help achieve business objectives by improving governance of IT services, infrastructure, security, and risk



How Does CHOP Do It?

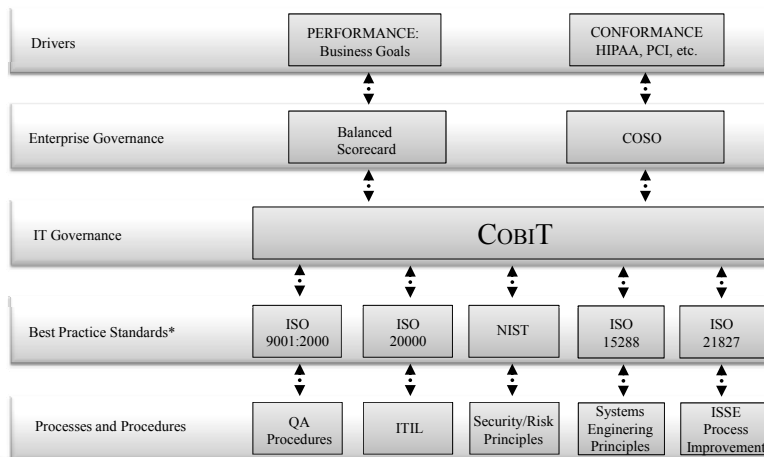
- Now ... information security risk mgmt
 - Enterprise governance
 - COSO (assumed)
 - IT governance
 - COBIT
 - IT risk management
 - NIST



(adapted from ITGI, 2007, p. 11)



How Does CHOP Do It?



(adapted from ITGI, 2007, p. 12)



How Does CHOP Do It?

- Step 2: Determine CIA requirements
 - Information Management Model (IMM)
 - Establishes specific categories of information
 - Includes information owners / custodians
 - Drives protection requirements
 - Information Protection Policy (IPP)
 - Establishes specific CIA requirements IAW IMM
 - Drives system categorization and control req'ts
 - Role-Based Access Control (RBAC) Model
 - System- or implementation-independent model
 - Drives access control requirements for new (project) and existing (production) systems



How Does CHOP Do It?

- Step 3: Define controls
 - Formally define CHOP risk-related controls
 - Business requirements
 - HIPAA, PCI, etc.
 - Governance control objectives (high-level controls)
 - COBIT
 - Risk mgmt controls (detailed controls)
 - NIST, PCI, etc.
 - Accepted control practices
 - Industry standards, best or commonly accepted practices, etc.
 - IS Security and Compliance Review Board (alternative controls)



How Does CHOP Do It?

ISO Compliance Map - HIPAA Security Rule Standards				
Section	Objective	Control	Implementation Guidance	Requirements
05 Security Policy	5.1 Information Security Policy: Provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	5.1.1 An information security policy document is approved by management, and published and communicated to all employees and relevant external parties.	5.1.1.1 Management shall approve the information security policies annually or when the policy has been significantly revised.	
			5.1.1.10 Detailed security policies, procedures, and plans for specific information systems, information technologies, or physical facilities shall be updated within 90 days after an update or modification is noted as required.	
			5.1.1.11 Develop and implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements taking into account the size, complexity, and ...	Requirements Traceability HIPAA <-- 164.306 <-- 164.306b2i HIPAA <-- 164.306 <-- 164.306b2ii HIPAA <-- 164.306 <-- 164.306b2iii HIPAA <-- 164.306 <-- 164.306b2iv HIPAA <-- 164.316 <-- 164.316a



How Does CHOP Do It?

- Step 4: Implement controls
 - Identify control owners
 - Promulgate control framework/practices
 - Develop control self assessment (CSA) methodology
 - Educate/train control owners on CSA



How Does CHOP Do It?

EXHIBIT A
SAMPLE POA&M TEMPLATE

Control Owner: John Smith
POA&M Delegated To: Jill Jones

Control Practices:

A formal documented process for granting and revoking access should be in place to ensure that only authorized users have access to YYYY systems.
Excessive # of users have access to YYYY database.

Control Deficiency:
Implementation Date: 11/30/08

#	Start Date	Actions	Completion Date	Responsible Party
Tactical Solution To Remediate Control Deficiencies				
<i>[Indicate what actions may be required in the future to further improve established processes]</i>				
	8/1/08	Identify appropriate contact at YYYY department and obtain list of active users that support the Hospital and require access to YYYY database.	8/7/08	
	8/1/08	Review user report & identify terminated users that no longer require access to YYYY database	8/15/08	
	8/18/08	Initiate requests to YYYY department to notify YYYY of terminated accounts that must be disabled.	8/18/08	
		[ADD ADDITIONAL ROWS AS NECESSARY]		
IMPLEMENTATION OF ONGOING PROCESSES / MAINTENANCE				
<i>[Indicate what actions may be required in the future to further improve established processes]</i>				
	8/1/08	Document Standard Operating Procedures (SOPs) for establishing, updating, terminating access to the YYYY database for employees, approved affiliates.	8/30/08	
		[ADD ADDITIONAL ROWS AS NECESSARY]		
PROVIDE EVIDENCE/REPORT STATUS TO ISRM AUDIT LIAISON TO DEMONSTRATE DEFICIENCY IS ADDRESSED.				
<i>Note: Internal/external audit entities may request status of corrective action.</i>				
	9/15/08	Provide copy of SOPs and documented procedures for performing periodic review of active YYYY access to validate that only active and authorized users have access to YYYY database.	9/15/08	
	9/15/08	Provide evidence that all terminated user accounts were disabled.	9/15/08	



How Does CHOP Do It?

- Step 5: Develop enforcement, monitoring and response
 - Determine requirements
 - Establish policy and procedures (methods)
 - Assess current capabilities
 - Perform gap analysis
 - Remediate/optimize current capabilities
 - Plan and program (budget) for enhancements and/or new capabilities

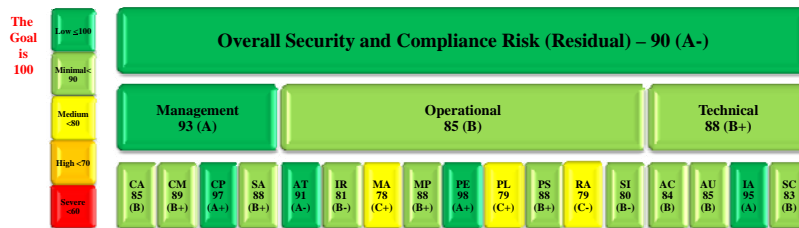


How Does CHOP Do It?

- Step 6: Assess and Report
 - Establish CHOP policy and procedures for reporting
 - Define and report executive- and operational-level metrics/dashboards
 - Develop control assessment, monitoring, and reporting workflow management capability
 - Implement routine, periodic executive-level reporting and follow-up



How Does CHOP Do It?



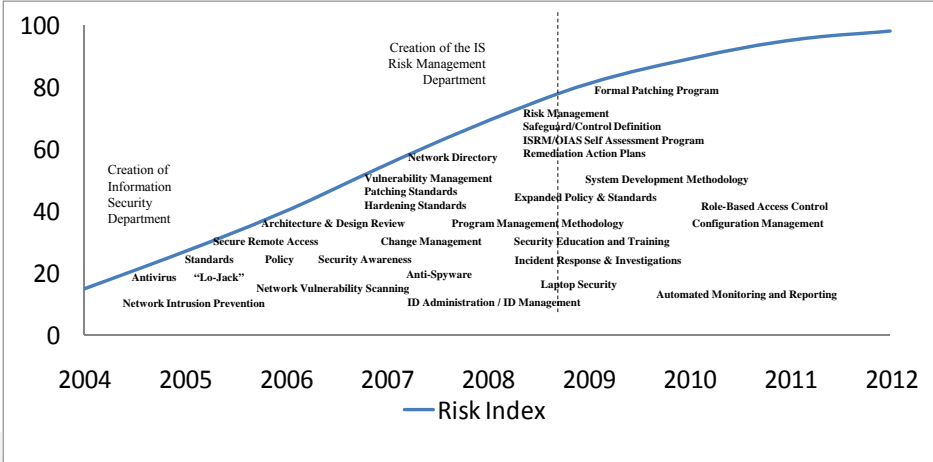
Management Controls
 CA: Certification, Accreditation, & Security Assessments
 CM: Configuration Management
 CP: Contingency Planning (BCP/DR)
 SA: System & Services Acquisition

Operational Controls
 AT: Awareness & Training
 IR: Incident Response
 MA: Maintenance
 MP: Media Protection
 PE: Physical & Environmental Protection
 PL: Planning
 PS: Personnel Security
 RA: Risk Assessment
 SI: System and Information Integrity

Technical Controls
 AC: Access Control
 AU: Audit & Accountability
 IA: Identification & Authentication
 SC: System and Communications Protection

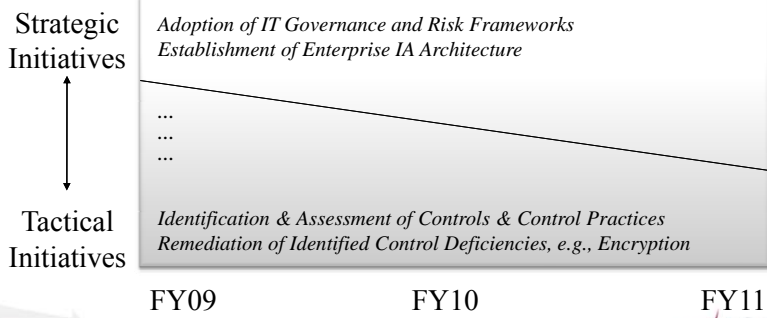


How Does CHOP Do It?



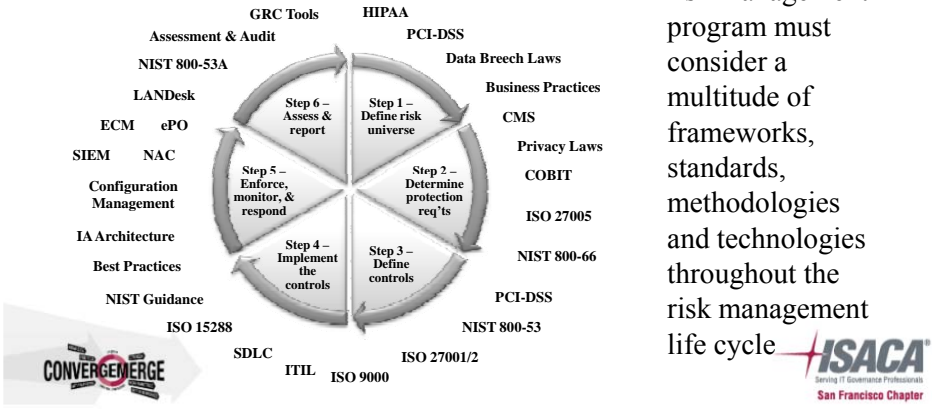
How Does CHOP Do It?

- Apportion strategic and tactical work in accordance with the organizational maturity of the IS department



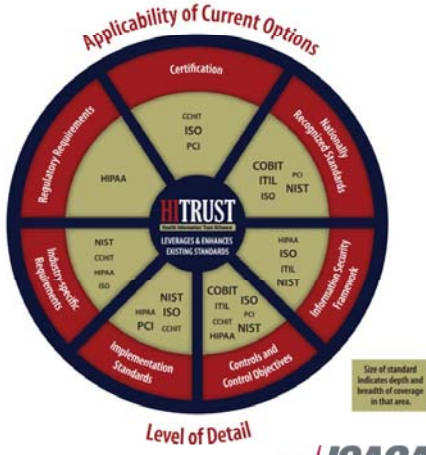
How Does CHOP Do It?

- Future ... unified information security and compliance risk management
- A robust, enterprise-level risk management program must consider a multitude of frameworks, standards, methodologies and technologies throughout the risk management life cycle



How Does CHOP Do It?

- Health Information Trust (HITRUST) Alliance Common Security Framework (CSF)
- Fortunately, integrated security and compliance controls frameworks exist in the commercial space. And while there are several to choose from, only the HITRUST CSF is solely focused on health care and none are as prescriptive.



How Does CHOP Do It?

- Overall benefits of the CSF
 - Outstanding ROI for initial and successive years
 - Unified framework focused on the health care environment
 - Easily tailored to fit CHOP requirements
 - Constantly maintained to fit changing security and compliance risk environment
 - Accelerates implementation of our risk management program by 12 months or more



How Does CHOP Do It?

- Costs/risks of the CSF
 - Yearly maintenance fees
 - Offset by ROI
 - CSF is a new unified compliance framework
 - May still need to “iron out the bugs”
 - Will allow us to influence the direction of the standard
 - May not be widely accepted within the industry
 - HITRUST is actively marketing the government and the health care industry
 - Will require some level of effort to revise current self assessment and subsequent risk indices

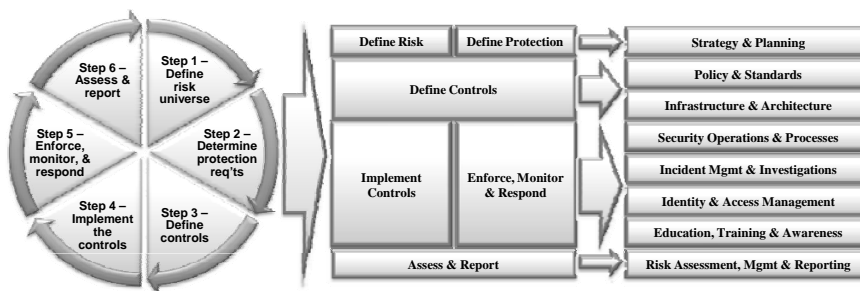


How Does CHOP Do It?

- Future ... unified information security and compliance risk management
 - Formally adopting the CSF
 - Actively participating in the HITRUST Alliance Leadership Forum to influence the direction of the Alliance and the CSF
 - Implementing the HITRUST Compliance Manager to support CSF adoption



Questions?



Additional Slides

The logo for the CONVERGEMERGE 2009 Fall Conference is centered on a large, light gray arrow pointing to the right. The word "CONVERGEMERGE" is written in large, bold, black letters. Above the "E" in "MERGE" is a circular graphic with three arrows forming a loop, labeled "SF ISACA" at the top and "2009 FALL CONFERENCE" at the bottom. Surrounding the central text are several smaller arrows pointing outwards, each containing a word: "KNOWLEDGE", "CONTROLS", "STRONGER", "WITH YOUR PEERS", "MORE MARKETABLE", and "BETTER NETWORKED". Below the main text, the dates "September 21, 2009 – September 23, 2009" are displayed. In the bottom left corner is the HITRUST logo with the tagline "Health Information Trust Alliance". In the bottom right corner is the ISACA logo with the tagline "Serving IT Governance Professionals" and "San Francisco Chapter".



HITRUST Mission

The Health Information Trust Alliance (HITRUST) exists to ensure that information security becomes a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges.

- Information security is critical to the broad adoption, utilization and confidence in health information systems, medical technologies and electronic exchanges of health information
- Collaborating with healthcare, business, technology and information security leaders to standardize on a higher level of security to build greater trust
- Certifiable framework that any and all organizations in the healthcare industry can implement and be certified against

Page 45

What is it that we wanted to accomplish?

- To **increase Trust** in the way health information is safeguarded, while **reducing the complexities** and **managing the costs**
 - Lower costs
 - Reduce risk
 - Increase efficiency
 - Reduce complexity
- Establish a **fundamental** and **holistic change** in the way the healthcare industry manages information security risks:
 - Regulations and standards rationalized into a single overarching framework tailored for the industry
 - Prescriptive, Scalable, Certifiable
 - Address inconsistent approaches to certification, risk acceptance and adoption of compensating controls to eliminate ambiguity in the process
 - Ability to cost effectively monitor compliance of organizational, business partner and government requirements
 - Provide support and enable sharing of ideas, feedback, experiences amongst the industry

Page 46

HITRUST Executive Council



Robert E. Booker
Chief Information Security Officer
United Health Group



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



Jim DeMaoribus
Senior Director, Health Care Strategy
Johnson & Johnson Health Care Systems, Inc.



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



Kimberly S. Gray, Esq., CIPP
Chief Privacy Officer
Highmark Inc.



Patrick Heim
Chief Information Security Officer
Kaiser Permanente



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



Nick Mankovich
Senior Director, Product Security
& Privacy
Philips Healthcare



Jon Moore
Chief Information Security Officer
Humana Inc.



Daniel Nutkis
Chief Executive Officer
Health Information Trust Alliance



Russell Pierce
Chief Information Security Officer
CVS Caremark



Michael Wilson
Vice President and
Chief Information Security Officer
McKesson Corporation

Page 47

What we learned over the last 18 months

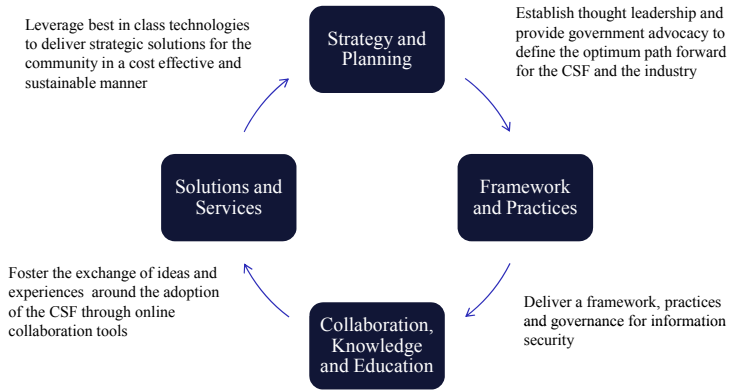
In the process of developing the Common Security Framework (CSF), a number of items were identified and summarized:

1. Organizations need to be able to understand and utilize the CSF
2. Organizations need to be able to obtain accurate and timely information and support relating to the CSF
3. Organizations need to be able to utilize alternative means to obtain certification without introducing any ambiguity or inconsistency into the certification process
4. Organizations have limited access to tools to aid in the managing of their compliance due to cost and resources
5. Organizations are challenged with effectively managing the status of their business partners compliance with their security policies, in addition to complying and reporting to their own business partners
6. Organizations **do not** want to add another compliance or audit requirement

The process and CSF need to be able to evolve as business models, technology, regulations and threats change

Page 48

2009 Strategy and beyond



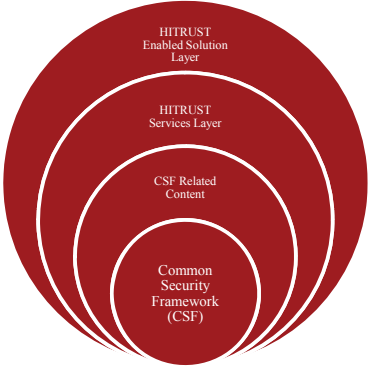
HITRUST has recognized that only by delivering a holistic and integrated approach to this issue will the healthcare industry be able to manage the complex task of cost effectively addressing information security for all organizations

Page 49

HITRUST's Core Content and Services

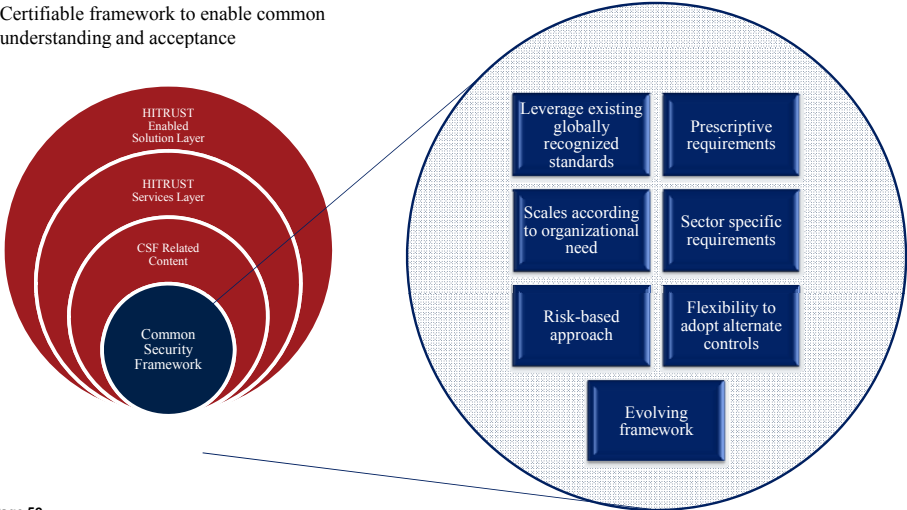
HITRUST's core content and services

- HITRUST delivers an approach for the practical, efficient, and consistent adoption of security by the healthcare industry.
 - Common Security Framework (CSF) developed by the industry for the industry
 - Certification and reporting processes to simplify compliance with regulatory and business partner requirements
 - Online community for collaboration and idea sharing
 - Services Architecture for integrating content and technology
 - Support infrastructure for organizations adopting the CSF

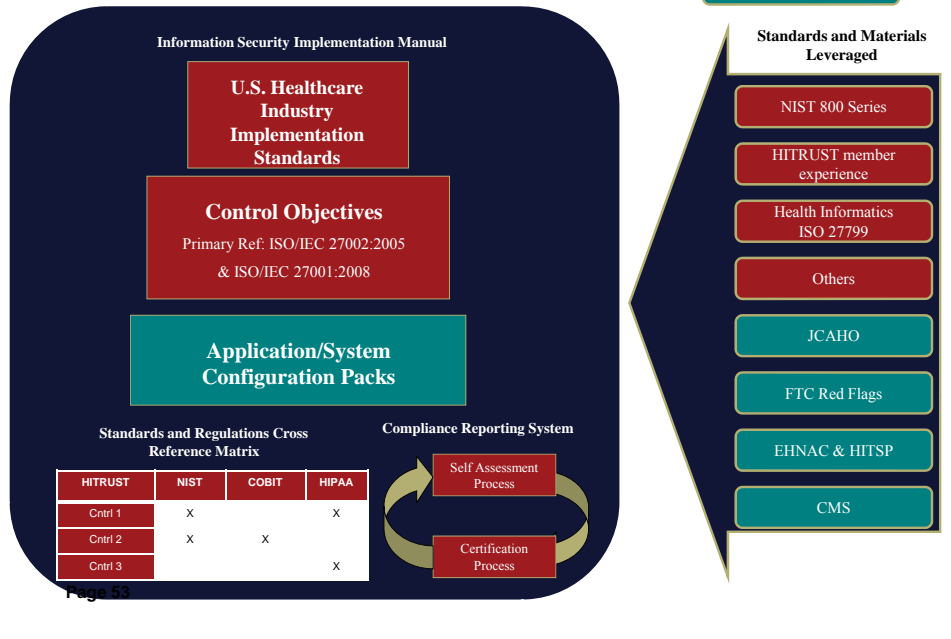


HITRUST CSF

Certifiable framework to enable common understanding and acceptance



HITRUST Common Security Framework



2009 CSF Evolution

Fundamental to HITRUST's mission is the availability of a framework that provides the needed structure, clarity, functionality and cross-references to authoritative sources.

- Authoritative Sources
- In 2009, HITRUST will add the following sources:
 - The Joint Commission IM.1.10 | IM.2.20 | IM.2.30 | LD.4.20 | LD.4.40
 - CMS Information Security (IS)
 - FTC Red Flags Rule
 - Healthcare Information Technology Standards Panel
 - EHNAC's Healthcare Network Accreditation Program (HNAP-EHN)
 - State Requirements
- Alternate Controls
- Application Security Packs
- HITRUST will also continue to evolve the CSF based on feedback regarding adoption from the industry

Synergy and Alignment with other Info. Sec. Efforts

- **CCHIT**
 - Focused on certification of HIT (Applications and Systems)
 - The Certification Commission for Healthcare Information Technology or CCHIT is a recognized certification body (RCB) for electronic health records and their networks, and an independent, voluntary, private-sector initiative. The mission of CCHIT is to **accelerate the adoption of health information technology by creating an efficient, credible and sustainable certification program**
 - Certified systems (criteria based) can significantly reduce effort in CSF compliance process
- **HITSP**
 - Focused on interoperability among healthcare software applications
 - The **Healthcare Information Technology Standards Panel (HITSP)** is a cooperative partnership between the public and private sectors. The Panel was formed for the purpose of harmonizing and integrating standards that will meet clinical and business needs for sharing information among organizations and systems
 - Focused on seven areas
 - Electronic Health Record (EHR) Laboratory Results Reporting, Biosurveillance, Consumer Empowerment, Emergency Responder Electronic Health Record (ER-EHR), Consumer Empowerment and Access to Clinical Information via Media, Quality, Medication Management, Personalized Healthcare, Consultations and Transfers of Care
 - Practices developed can be incorporated or cross referenced in the CSF
- **HITRUST**
 - Focused broadly (entire organization) on a certifiable security framework specific to healthcare organizations (providers, health plans, pharmacies, distributors) that scales according to size and complexity of an organization

Page 55

HITRUST CSF Sample

The screenshot displays the HITRUST CSF Common Security Framework System interface. The main content area shows a table of CSF Controls with the following columns: Control Reference, Control Specification, and Control Objectives.

Control Reference	Control Specification	Control Objectives
01.1 Session Time-out	Inactive sessions shall shut down after a defined period of inactivity.	01.1 - Access Control 01.1B - Operating System Access Control
01.4 Limitation of Connection Time	Restrictions on connection times shall be used to provide additional security for high-risk applications.	01.1 - Access Control 01.1B - Operating System Access Control
01.6 Information Access Restrictions	Logical and physical access to information and application systems and functions by users and support personnel shall be restricted in accordance with the defined access control policy.	01.1 - Access Control 01.1B - Application and Information Access Control
01.6a Sensitive System Isolation	Required for HITRUST Certification 2009 Sensitive systems shall have a restricted and isolated computing environment.	01.1 - Access Control 01.1B - Application and Information Access Control
01.6b Mobile Computing and Communications	Required for HITRUST Certification 2009 A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.	01.1 - Access Control 01.1B - Mobile Computing and Teleworking
01.7 Teleworking	A policy, operational plans and procedures shall be developed and implemented for teleworking activities.	01.1 - Access Control 01.1B - Mobile Computing and Teleworking
01.8 Roles and Responsibilities	Required for HITRUST Certification 2009 Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.	02.0 - Human Resources Security 02.0.1 - Prior to Employment
01.8a Succession	Required for HITRUST Certification 2009 Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the permitted risks.	02.0 - Human Resources Security 02.0.1 - Prior to Employment
01.8b Terms and Conditions of Employment	All part of their contractual obligations, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall include their responsibilities for information security.	02.0 - Human Resources Security 02.0.1 - Prior to Employment
01.8c Management Responsibilities	Management shall require employees, and where applicable contractors and third party users, to apply security in accordance with established policies and procedures of the organization.	02.0 - Human Resources Security 02.0.1 - Prior to Employment
01.8d Information Security Awareness, Education, and Training	Required for HITRUST Certification 2009 All employees of the organization and contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.	02.0 - Human Resources Security 02.0.1 - Prior to Employment
01.8e Disciplinary Process	Required for HITRUST Certification 2009 There shall be a formal disciplinary process for employees who have violated security policies and procedures.	02.0 - Human Resources Security 02.0.1 - Prior to Employment
01.8f Termination Responsibilities	Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.	02.0 - Human Resources Security 02.0.1 - Termination or Change of Employment
01.8g Return of Assets	All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.	02.0 - Human Resources Security 02.0.1 - Termination or Change of Employment
01.8h Removal of Access Rights	The access rights of all employees, contractors and third party users to information and information assets shall be removed upon termination of their employment, contract or agreement, or adjusted upon a change of employment, or upon transfer within the organization.	02.0 - Human Resources Security 02.0.1 - Termination or Change of Employment
01.9 Risk Management Process Development	Organizations shall develop and maintain a risk management program to manage risk to an acceptable level.	03.0 - Risk Management 03.0.1 - Risk Management Process
01.9a Performing Risk Assessments	Risk assessments shall be performed to identify and quantify risks.	03.0 - Risk Management

Page 56

HITRUST CSF Sample (Cont'd)

Scales according to type, size and complexity of the organization and system as determined by a predefined criteria.

<p>► General Information</p>	
<p>► Level 1 Implementation Requirement</p>	
<p>► Level 1 Alternate Controls</p>	
<p>▼ Level 2 Implementation Requirement</p>	
<p>Level 2 Organizational Factors: BioTech Organizations > \$100,000 Spend on Research and Development Per Year Pharmaceutical Companies > 20,000,000 Prescriptions Per Year Third Party Processors > 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</p>	<p>Level 2 System Factors: None</p>
<p>Level 2 Regulatory Factors: Subject to PCI Compliance</p>	
<p>Level 2 Implementation: Level 1 plus:</p>	
<p>The policy shall refer to the specific procedures and programs to address incidents and also refer to a forensic program. Procedures shall be developed to provide for definition of the information security incidents, roles and responsibilities, incident handling, reporting and communication processes. They shall also state the requirements for an incident handling team to address regulatory requirements, third party relationships, and the handling of third party security breaches.</p> <p>All employees, contractors and third party users shall receive mandatory incident response training to ensure they are aware of their responsibilities to report any information security events as quickly as possible, the procedure for reporting information security events and the point(s) of contact.</p> <p>The reporting procedures shall include:</p> <ul style="list-style-type: none"> i. feedback processes to ensure that those reporting information security events are notified of results after the issue has been dealt with and closed; ii. information security event reporting forms to support the reporting action, and to help the person reporting to remember all necessary actions in case of an information security event including: <ul style="list-style-type: none"> 1. the correct behavior to be undertaken in case of an information security event and noting all important details (e.g. type of non-compliance or breach) occurring malfunction, messages on the screen, strange behavior, immediately; and 2. not carrying out any own action, but immediately reporting to the point of contact; iii. reference to an established formal disciplinary process for dealing with employees, contractors or third party users who commit security breaches; iv. communicating incidents to local and federal law enforcement agencies; and v. automated work flow processes for incident management, reporting and resolution. <p>Alerts from the organization's intrusion-detection and intrusion-prevention systems shall be utilized for reporting information security events.</p>	
<p>Level 2 Control Audit Procedure: Example:</p> <ul style="list-style-type: none"> i. The organization's information security policy to ensure 4 refers to the specific procedures and programs to address incidents and also refers to a forensic program. ii. The organization's information security policy to ensure 4 contains a definition of the information security incidents, roles and responsibilities, incident handling, reporting and communication processes. iii. The organization's information security policy to ensure 4 defines the requirements to address regulatory requirements, third party relationships, and the handling of third party security breaches. iv. The organization's information security policy to ensure 4 refers to a formal disciplinary process for dealing with employees, contractors or third party users who commit security breaches. v. The security event reporting forms that support the reporting action, to ensure all necessary actions in case of an information security event are defined. <p>Interview:</p> <ul style="list-style-type: none"> i. Select organization personnel with incident response responsibilities to verify that they are aware of their roles and responsibilities, and the processes for incident handling, reporting and communication in line with what is defined in the policy and procedures. 	
<p>Page 57</p>	

HITRUST CSF Sample (Cont'd)

Prescriptive to ensure clarity and consistency of implementation.

<p>► General Information</p>	
<p>► Level 1 Implementation Requirement</p>	
<p>► Level 1 Alternate Controls</p>	
<p>▼ Level 2 Implementation Requirement</p>	
<p>Level 2 Organizational Factors: BioTech Organizations > \$100,000 Spend on Research and Development Per Year Pharmaceutical Companies > 20,000,000 Prescriptions Per Year Third Party Processors > 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</p>	<p>Level 2 System Factors: None</p>
<p>Level 2 Regulatory Factors: Subject to PCI Compliance</p>	
<p>Level 2 Implementation: Level 1 plus:</p>	
<p>The policy shall refer to the specific procedures and programs to address incidents and also refer to a forensic program. Procedures shall be developed to provide for definition of the information security incidents, roles and responsibilities, incident handling, reporting and communication processes. They shall also state the requirements for an incident handling team to address regulatory requirements, third party relationships, and the handling of third party security breaches.</p> <p>All employees, contractors and third party users shall receive mandatory incident response training to ensure they are aware of their responsibilities to report any information security events as quickly as possible, the procedure for reporting information security events and the point(s) of contact.</p> <p>The reporting procedures shall include:</p> <ul style="list-style-type: none"> i. feedback processes to ensure that those reporting information security events are notified of results after the issue has been dealt with and closed; ii. information security event reporting forms to support the reporting action, and to help the person reporting to remember all necessary actions in case of an information security event including: <ul style="list-style-type: none"> 1. the correct behavior to be undertaken in case of an information security event and noting all important details (e.g. type of non-compliance or breach) occurring malfunction, messages on the screen, strange behavior, immediately; and 2. not carrying out any own action, but immediately reporting to the point of contact; iii. reference to an established formal disciplinary process for dealing with employees, contractors or third party users who commit security breaches; iv. communicating incidents to local and federal law enforcement agencies; and v. automated work flow processes for incident management, reporting and resolution. <p>Alerts from the organization's intrusion-detection and intrusion-prevention systems shall be utilized for reporting information security events.</p>	
<p>Level 2 Control Audit Procedure: Example:</p> <ul style="list-style-type: none"> i. The organization's information security policy to ensure 4 refers to the specific procedures and programs to address incidents and also refers to a forensic program. ii. The organization's information security policy to ensure 4 contains a definition of the information security incidents, roles and responsibilities, incident handling, reporting and communication processes. iii. The organization's information security policy to ensure 4 defines the requirements to address regulatory requirements, third party relationships, and the handling of third party security breaches. iv. The organization's information security policy to ensure 4 refers to a formal disciplinary process for dealing with employees, contractors or third party users who commit security breaches. v. The security event reporting forms that support the reporting action, to ensure all necessary actions in case of an information security event are defined. <p>Interview:</p> <ul style="list-style-type: none"> i. Select organization personnel with incident response responsibilities to verify that they are aware of their roles and responsibilities, and the processes for incident handling, reporting and communication in line with what is defined in the policy and procedures. ii. Select organization personnel with incident response responsibilities to verify their understanding of regulatory requirements, third party relationships, and the handling of third party security breaches. iii. Select organization personnel to verify that incident response training is provided and required. iv. Select organization personnel to ensure they are aware of their responsibilities to report any information security events as quickly as possible, the procedure for reporting information security events and the point(s) of contact. <p>Test:</p> <ul style="list-style-type: none"> i. Any automated work flow processes for incident management, reporting and resolution to validate they are in compliance with the defined policy and procedures. 	
<p>Page 58</p>	

HITRUST CSF Sample (Cont'd)

<p>General Information</p> <p>Control Reference: 11 a Reporting Information Security Events</p> <p>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.</p> <p>Control Objective: 11 d - Information Security Incident Management 11.01 Operating Information Security Programs and Effectiveness</p> <p>*Required for HITRUST Certification 2009</p> <p>Factor Type: Organizational</p>	
<p>▶ Level 1 Implementation Requirement</p> <p>▶ Level 1 Alternate Controls</p> <p>▶ Level 2 Implementation Requirement</p> <p>▶ Level 2 Alternate Controls</p> <p>▶ Level 3 Implementation Requirement</p> <p>▶ Level 3 Alternate Controls</p> <p>▶ Authoritative Sources</p> <p>▶ Providers</p> <p>▶ Health Plans and PBMs</p> <p>▶ Manufacturers (Pharma and Device)</p> <p>▶ Pharmacies and Distributors</p> <p>▶ Information Networks and Clearing Houses</p> <p>▶ Liability Insurance Brokers and Underwriters</p> <p>▶ Information Security Vendors</p> <p>▶ Other Information</p>	<p>Follows a risk-based approach to allow organizations to identify the appropriate level of controls. This includes multiple levels of Implementation Requirements as determined by risk.</p>
<p>Page 59</p>	

HITRUST CSF Sample (Cont'd)

<p>Level 3 Implementation Requirement</p> <p>Level 3 Organizational Factors: BioTech Organizations > \$200,000,000 Spend on Research and Development Per Year Pharmaceutical Companies > 100,000,000 Prescriptions Per Year Third Party Processor > 5,000,000 Records Processed Per Year Physician Practice > 50,000 Visits Per Year Medical Facilities / Hospital > 10,000 Licensed Beds Health Plan / Insurance > 7,500,000 Covered Lives</p> <p>Level 3 System Factors: None</p> <p>Level 3 Regulatory Factors: Subject to Federal Government Compliance</p> <p>Level 3 Implementation: Level 2 plus:</p> <p>A duress alarm shall be provided whereby a person under duress can indicate such problems. The procedures for responding to duress alarms shall reflect the high risk situation such alarms are indicating.</p> <p>An information security assessment shall be made either on all incidents or on a sample, to further validate the effectiveness or otherwise of established controls and of the risk assessment that lead to them. Examples include:</p> <ul style="list-style-type: none"> i. A break-in leading to theft of IT hardware, resulting in a confidentiality breach; or ii. A fire could be set to degrade misuse of IT equipment. <p>Level 3 Control Audit Procedure: Example:</p> <ul style="list-style-type: none"> i. The procedures for responding to duress alarms to ensure they reflect the high risk situation such alarms are indicating. ii. The information security policy to ensure an information security assessment is made either on all incidents or on a sample. iii. The results of the most recent information security assessment for an incident to validate the effectiveness or otherwise of established controls. <p>Interview:</p> <ul style="list-style-type: none"> i. Select organization personnel with incident response responsibilities to verify their understanding of the procedures for responding to a duress alarm. <p>Test:</p> <ul style="list-style-type: none"> i. The duress alarm to validate its working functionality and notification. <p>Level 3 Control Standard Mapping:</p> <ul style="list-style-type: none"> • ISO/IEC 27002:2005 13.1.1 • NIST SP800-53 RD SI-4 	
	<p>Consistency in audit procedures allows standardized comparisons and improves the secure exchange of data throughout the information's lifecycle.</p>
<p>Page 60</p>	

HITRUST CSF Sample (Cont'd)

▼ Authoritative Sources

References:	CobT 4.0 (2005)	Add
	03 Deliver & Support	
	05 Ensure Systems Security	
	05.06 Security Incident Definition	
HPAA (August, 1996)	E. Administrative Safeguard (164.308)	
	Security Incident Procedures	
	(a)(6)(ii) Response and Reporting (Required)	
ISO 27799:2008	07.0 Healthcare implications of ISO/IEC 27002	
	07.10 Information security incident management	
	07.10.1 Reporting information security events and weaknesses	
ISO/IEC 27001:2005(E)	A.13.0 Information Security Incident Management	
	A.13.01 Reporting information security events and weaknesses	
	A.13.01.01 Reporting information security events	
ISO/IEC 27002:2005(E)	13.0 Information Security Incident Management	
	13.01 Reporting information security events and weaknesses	
	13.01.01 Reporting information security events	
NIST SP 800-53 (February, 2005) and SP 800-26 (April, 2005)	Operational	
	Incident Response	
	IR-02 (1) Incident Response Training	
	IR-02 (2) Incident Response Training	
	IR-02 Incident Response Training	
	IR-06 (1) Incident Reporting	
	IR-06 Incident Reporting	
	System and Information Integrity	
	SI-04 (1) Intrusion Detection Tools & Techniques	
	SI-04 (2) Intrusion Detection Tools & Techniques	
	SI-04 (3) Intrusion Detection Tools & Techniques	
	SI-04 (4) Intrusion Detection Tools & Techniques	
	SI-04 Intrusion Detection Tools & Techniques	
	SI-05 (1) Security Alerts & Advisories	
	SI-05 Security Alerts & Advisories	
PCI Data Security v1.2 (October 2008)	06 Maintain an Information Security Policy (v1.2)	
	12 Maintain a policy that addresses information security for employees and contractors. (v1.2)	
	12.05 Assion Information Security Responsibilities (v1.2)	
	12.09 Incident Response (v1.2)	

Leverages existing globally and nationally recognized standards to expand on the implementation requirements of the framework and to **avoid** introducing additional **redundancy** and **ambiguity** into the industry.

Page 61

HITRUST CSF Sample (Cont'd)

▼ Authoritative Sources

References:	CobT 4.0 (2005)	Add
	03 Deliver & Support	
	05 Ensure Systems Security	
	05.06 Security Incident Definition	
HPAA (August, 1996)	E. Administrative Safeguard (164.308)	
	Security Incident Procedures	
	(a)(6)(ii) Response and Reporting (Required)	
ISO 27799:2008	07.0 Healthcare implications of ISO/IEC 27002	
	07.10 Information security incident management	
	07.10.1 Reporting information security events and weaknesses	
ISO/IEC 27001:2005(E)	A.13.0 Information Security Incident Management	
	A.13.01 Reporting information security events and weaknesses	
	A.13.01.01 Reporting information security events	
ISO/IEC 27002:2005(E)	13.0 Information Security Incident Management	
	13.01 Reporting information security events and weaknesses	
	13.01.01 Reporting information security events	

Allows organizations to drill down into the authoritative sources referenced in each control.

Sub Section	Sub Section ID: 00-2005-C114
<p>Sub Section Name: 13.01.01 Reporting information security events</p> <p>Sub Section Description: Control information security events should be reported through appropriate management channels as quickly as possible.</p> <p>Implementation guidance: A formal information security event reporting procedure should 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. A point of contact should be established for the reporting of information security events. It should be ensured that this point of contact is known throughout the organization, is always available and is able to provide adequate and timely responses.</p> <p>All employees, contractors and third party users should be made aware of their responsibility to report any information security events as quickly as possible. They should also be aware of the procedure for reporting information security events and the point of contact. The reporting procedure should include:</p> <ol style="list-style-type: none"> substantive feedback processes to ensure that those reporting information security events are notified of results after the issue has been dealt with and closed; information security event reporting forms to support the reporting action, and to help the person reporting to remember all necessary actions in cases of an information security event; the correct behavior to be undertaken in case of an information security event, i.e. <ol style="list-style-type: none"> noting all important details (e.g. type of non-compliance or breach, security malfunction, messages on the screen, strange behaviour); immediately; not carrying out any non-action, but immediately reporting to the point of contact; reference to an established formal disciplinary process for dealing with employees, contractors or third party users who commit security breaches. <p>In high-risk environments, a dursax alarm may be provided whereby a person under dursax can indicate such problems. The procedures for responding to dursax alarms should reflect the high-risk situation such alarms are indicating.</p>	

Page 62

HITRUST CSF Sample (Cont'd)

Structured in accordance with ISO 27001 / 27002 standard.

General Information

Control Reference: 11 a Reporting Information Security Events

Control Objective: 11 a: Information Security Incident Management
11 a1 Reporting Information Security Incidents and Timeliness

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.

Factor Type: Organizational

Factor: *Required for HITRUST Certification 2009

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 Processed - 1,000,000 Records Processed Per Year
Physician Practices - 22,000 Visits Per Year
Medical Facilities / Hospitals - 1,000 Licensed Beds
Health Plan / Insurance - 1,000,000 Covered Lives

Level 1 System Factors: None

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.

Level 1 Control Audit Procedure:

Example:

- The organization's information security policy to ensure information security event reporting procedures that support the corporate direction have been established.
- The organization's information security policy to ensure an incident response and escalation procedure is defined, setting out the action to be taken on receipt of a report of an information security event, and the timeliness of reporting and response.
- The organization's information security policy to ensure it defines the direction of management.
- The organization's information security policy and/or organization itself to a point of contact has been established for the reporting of information security events.

Interview:

- Management to verify the direction of the organization relating to information security and incident reporting, response and escalation is aligned with the policy.
- Select organization personnel to verify that the point of contact is known throughout the organization.
- The point of contact for incident reporting to verify their awareness of their responsibilities as defined in the policy and procedures.

Test:

- None

Level 1 Control Standard Mapping:

- HIPAA §164.312 (a)(5)(ii)

Level 1 Alternate Controls

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

Page 63

Accreditation

Defines the requirements for organizations performing the certification assessments and attesting organizations' compliance with the requirements of the CSF.

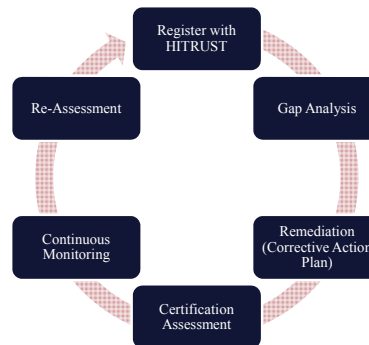
- Must perform in accordance with requirements defined and based on ISO 27006

The requirements imposed on HITRUST CSF Certifiers include:

- Formal agreement and support with qualified resources
- Policies and procedures to ensure the integrity and ethics of its employees
- Strict competency requirements as related to both healthcare and information security
 - Healthcare technical competency must match that of the client
 - Maintains a minimum of 120 CPEs over 3 years
- A minimum of one subject-matter expert (SME) with at least 5 years of practical experience and a professional security certification (e.g. CISSP, HISP) for each engagement
- Minimum of 5 HITRUST trained professionals per organization
- Oversight and continual review of Accredited Organizations performing HITRUST CSF Certifications through annual trainings

Certification

- Based on ISO 27006
- Incorporates the expertise and best practices of certifying organizations
- Defines a standardized testing methodology to ensure consistent and comparable results across all organizations of the industry
- 2-year certification cycle to ensure continual improvement



Page 65

HITRUST Central

Page 66

Access to the CSF online

A professional network for:

- sharing knowledge
- understanding industry issues & events
- exchanging ideas and best practices
- discovering new ways to solve business problems
- downloading documentation and training materials

Providing support:

- What does this control mean?
- How do I implement these requirements?
- What do I do if I cannot meet a requirement?

Industry perspective

“The development of a common security framework is critical, not just for protecting electronic health information, but in minimizing the costs and complexities associated with securing electronic health information.” – Dr. Ross Martin, Director of Health Information Convergence, **BearingPoint**

“The HITRUST CSF program is creating what has been lacking in the healthcare industry relating to information security guidance and clarity. It removes the confusion, inconsistencies and variability that have existed to date in how organizations have implemented security measures.” – G. Christopher Hall, Partner, Security, **Accenture**

“Through the shared experiences of HITRUST’s framework participants, we can develop a comprehensive and agile security framework that can grown with new health information technologies.” – Jon Moore, Chief Information Security Officer, **Humana**

“As an information security professional in the healthcare industry, I have struggled to identify a practical strategy and approach that appropriately addresses risk, and which can be implemented and accepted by management, finance, internal and external auditors, and trading partners. The HITRUST CSF provides a consistent framework by which a healthcare organization can address security challenges,” said Michael Frederick, Director - Office of Information Security and Chief Information Security Officer, **Baylor Health Care System**.

“As an organization that recognizes the importance of EHR, PHR, and information exchanges to improving quality and better management of medical expenses, we also recognize that a critical component to achieving their potential is confidence by business partners, regulators and consumers that safeguards are in place to protect sensitive health information. The HITRUST CSF allows organizations to better understand the appropriate safeguarding measures and communicate their efforts in a uniform manner to their partners.” – Robert Mandel, MD, MBA, Senior Vice President, Health Care Services, **Blue Cross Blue Shield of Tennessee**

Page 67

BACKUP SLIDES

KNOWLEDGE
CONTROLS
WITH YOUR PEERS
CONVERGEMERGE
2009 FALL CONFERENCE
STRONGER
MORE MARKETABLE
BETTER NETWORKED

September 21, 2009 – September 23, 2009

ISACA
Setting IT Governance Professionals
San Francisco Chapter

Risk

- Risk is defined as the likelihood that something will happen that causes harm to an informational asset (or the loss of the asset)
- A vulnerability is a weakness that could be used (exploited) to endanger or cause harm to an informational asset
- A threat is anything (man made or act of nature) that has the potential to cause harm
- Therefore when a threat exploits a vulnerability, there is a probable impact to the informational asset
 - In the context of information security, the impact is a loss of informational availability, integrity and confidentiality, and possibly other losses (e.g., lost income, loss of life, loss of real property)
- Risk may be therefore be written as a function of two likelihood estimators, where
 - Risk = F[P(Exploit), P(Impact)] = F[P(Threat, Vulnerability), P(asset, loss)]

69

Risk Management

- In general, risk management is defined as “the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what [controls or safeguards], if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization”
- For any given risk, executive management can
 - Choose to accept the risk based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the business,
 - Leadership may choose to mitigate the risk by selecting and implementing appropriate controls to reduce the risk,
 - In some cases, the risk can be transferred to another business by buying insurance or outsourcing to another business, and
 - In cases where the reality of some risks may be disputed, they can choose to deny the risk, which is in and of itself a potential risk

70

Controls

- A control is defined as a safeguard or countermeasure used to avoid, counteract or minimize security risks and may be of three general types:
 - Management controls focus on the management of risk and the management of information system security
 - Technical controls are mechanisms implemented in the hardware, software, or firmware that provide automated protection to systems or applications
 - Operational controls address security methods primarily implemented and executed by people (as opposed to systems)
- Controls are designed to minimize the probability a threat can exploit a vulnerability; thus, the level of control compliance, e.g., meets, partially meets, or does not meet, provides a measure of the (threat, vulnerability) likelihood function.
 - $P(\text{Threat, Vulnerability}) \doteq \text{Level of Control Compliance}$
- Similarly, the impact to an informational asset previously defined as an (asset, loss) pair may also be estimated from a control failure
 - $P(\text{Asset, Loss}) \doteq \text{Impact of Control Failure}$

71

Residual Risk

- Residual risk is defined as the risk that remains in the operation of an information system or systems after all possible, cost-effective threat mitigation controls (safeguards or countermeasures) have been applied
 - $\text{Residual Risk} = \text{Inherent Risk} - \text{Controlled Risk}$
- Residual risk is made up of two components: acceptable and unacceptable
 - $(\text{Residual Risk}_A + \text{Residual Risk}_U) = \text{Inherent Risk} - \text{Controlled Risk}$
- Acceptable residual risk consists of control risk, i.e., the risk for which the control is intended to mitigate but does not, and the risk for which no controls are defined
 - $(\text{Control Risk} + \text{Uncontrolled Risk}) + \text{Residual Risk}_U = \text{Inherent Risk} - \text{Controlled Risk}$
- Thus unacceptable residual risk is generally the amount of risk that occurs when approved controls and control practices are partially implemented or not implemented at all
 - $\text{Residual Risk}_U = \text{Inherent Risk} - \text{Controlled Risk} - \text{Control Risk} - \text{Uncontrolled Risk}$

72

Residual Risk

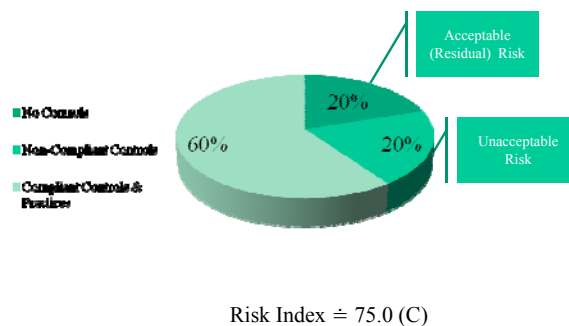
- In order to minimize unacceptable residual risk, one must either mitigate more risk through the application of additional controls (or more rigorous control practices) OR accept more residual risk through the application of fewer controls (or less rigorous control practices)
 - Residual Risk $U = \text{Inherent Risk} - \text{Controlled Risk} - (\text{Control Risk} + \text{Uncontrolled Risk})$
- When considering unacceptable residual risk as a function of (threat, vulnerability) and (asset, loss) pairs, overall unacceptable residual risk to the enterprise may be estimated as a function of control compliance
 - Residual Risk $U \cong F(\text{Level of Control Compliance, Impact of Control Failure})$
 - $\cong [\sum^n \text{Compliance} \cdot \text{Impact}] / n$, where $n = \text{number of controls and compliance and impacts are quasi-quantitative}$

73

Controls-based Risk Management

- In a controls-based risk management program, the defined controls and supporting control practices establish the level of residual risk acceptable to the enterprise

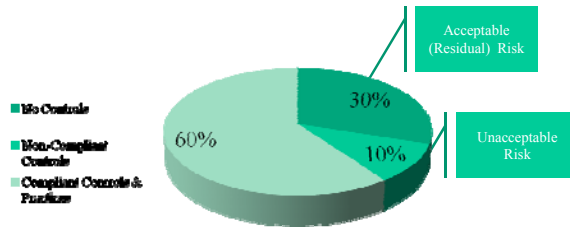
- ▶ Thus the goal of any metric related to control-based risk will always target 100% of control compliance since the amount of acceptable residual risk is the risk not addressed AFTER ALL accepted controls & supporting control practices are implemented



74

Controls-based Risk Management

- The number, type, and rigor of controls will vary from one enterprise to another, i.e., enterprises accept different levels of risk based on their individual business requirements



Risk Index \approx 85.7 (B) with the same number of compliant controls, i.e., we've "lowered the bar"

- Less "control" implies more acceptable risk
- Regardless, the goal is still the same—100% compliance with ALL approved controls and supporting control practices within the enterprise

75

IT Governance

Strategic alignment

Focuses on ensuring the linkage of business and IT plans; on defining, maintaining and validating the IT value proposition; and on aligning IT operations with enterprise operations

Value delivery

Is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT

Resource management

Is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure.

Risk management

Requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise, and embedding of risk management responsibilities in the organisation

Performance measurement

Tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting

(ITGI, 2007, p. 69)

IT Governance Framework

COBIT helps bridge the gaps between business risks, control needs and technical issues.
 It provides good practices across a domain and process framework and presents activities in a manageable and logical structure.

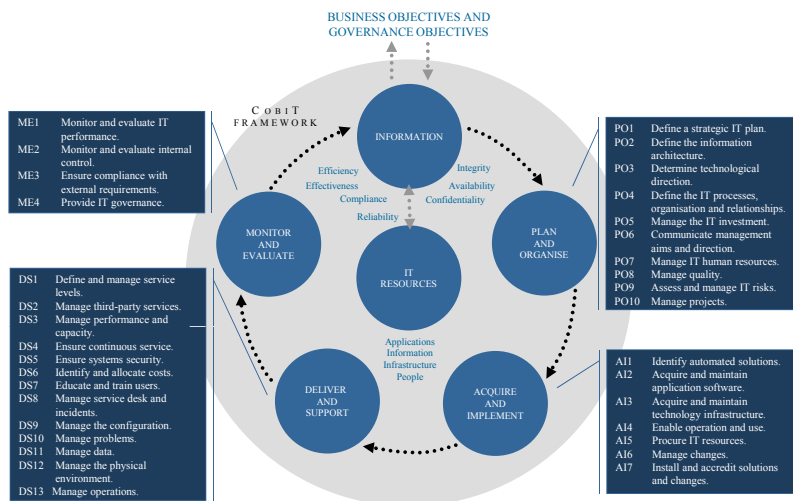
COBIT:

- Starts from business requirements
- Is process-oriented, organizing IT activities into a generally accepted process model
- Identifies the major IT resources to be leveraged
- Defines the management control objectives to be considered
- Incorporates major international standards
- Has become the *de facto* standard for overall control of IT

IT resources need to be managed by a set of naturally grouped processes. COBIT provides a framework that achieves this objective.

(ITGI, 2007, p. 9) 77

COBIT Framework



(ITGI, 2007, p. 40) 78

IS Risk Management Framework

- “... provides ... a disciplined, structured, flexible, extensible, and repeatable *process for achieving risk-based protection* related to the operation and use of information systems
- “... facilitates *continuous monitoring and ... improvement* in the security state of the information systems within an organization
- “... incorporates a *well-defined set of information security standards and guidelines*” (NIST, 2007, p. 20)

79