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

Bryan Cline

September 21, 2009 – September 23, 2009

ISACA
Serving IT Governance Professionals
San Francisco Chapter

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

ISACA Serving IT Governance Professionals
San Francisco Chapter

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

CONVERGEMERGE

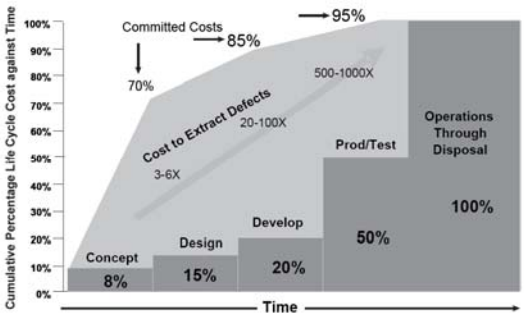
ISACA Serving IT Governance Professionals
San Francisco Chapter

Why Do It?

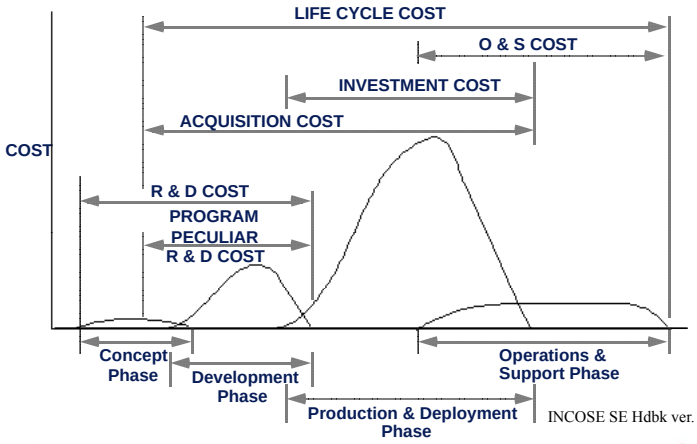
- Why do information security and compliance risk management at all?
  - To protect information that has value
  - To avoid costs associated with non-compliance
- What are some of the threats?
  - Loss of value
    - Examples: trade secrets, proprietary information
  - Misappropriation of value
    - 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

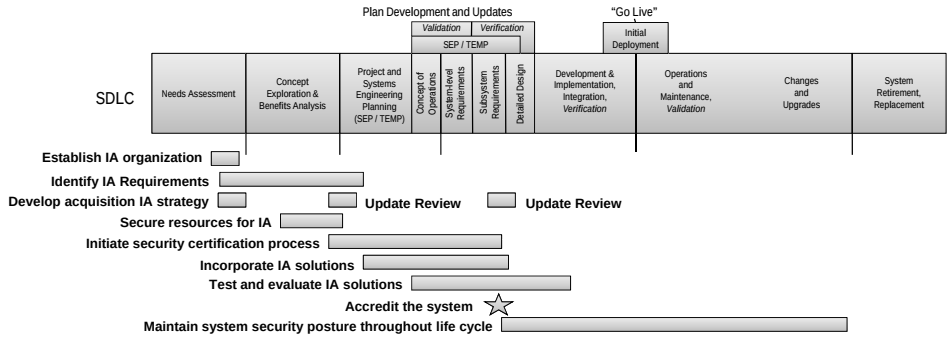


Why Do It?

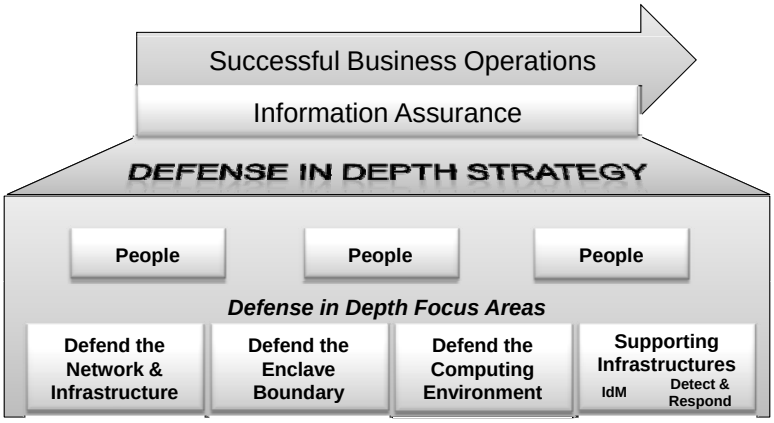


INCOSE SE Hdbk ver. 2a

Why Do It?

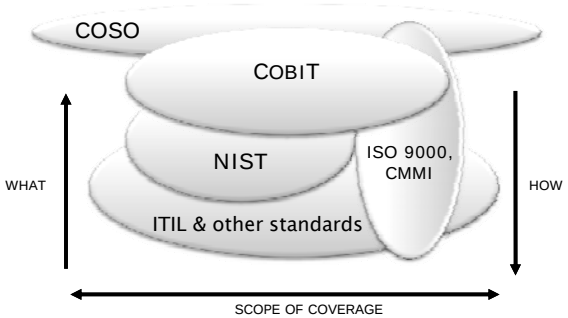


Why Do It?



Why Do It?

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



(adapted from ITGI, 2007, p. 11)

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?

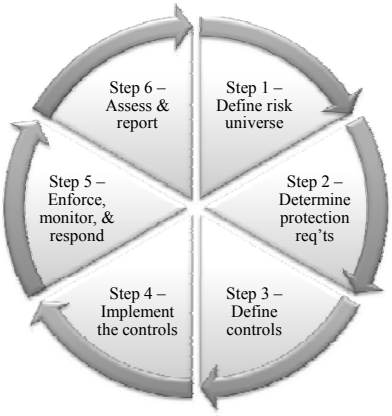
- Information security [& compliance] risk mgmt
  - is intended to "balance the benefits gained from the use of … information systems with the risk of these … systems being the vehicle through which [threats] cause mission or business failure." (NIST, 2007, p. 1), and
  - "is made up of *Information 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

ISACA
Serving IT Governance Professionals
San Francisco Chapter

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

ISACA
Serving IT Governance Professionals
San Francisco Chapter

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

ISACA
Serving IT Governance Professionals
San Francisco Chapter

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

ISACA
Serving IT Governance Professionals
San Francisco Chapter

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

ISACA
Serving IT Governance Professionals
San Francisco Chapter

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***

ISACA
Serving IT Governance Professionals
San Francisco Chapter

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

Creation of the IS Risk Management Department

Creation of Information Security Department

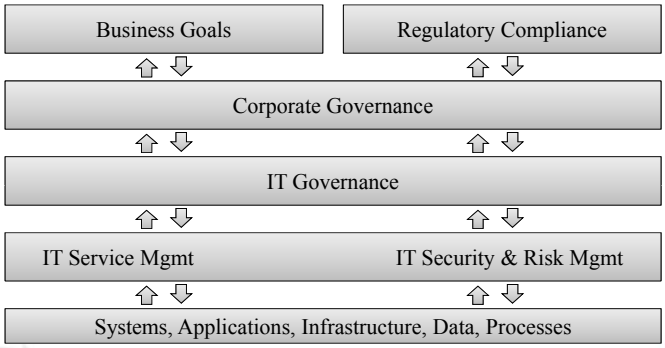
Network Directory
Vulnerability Management
Patching Standards
Hardening Standards
Architecture & Design Review
Program Management Methodology
Secure Remote Access
Change Management
Security Education and Training
Standards
Policy
Security Awareness
Incident Response & Investigations
Antivirus
"Lo-Jack"
Anti-Spyware
Network Vulnerability Scanning
Network Intrusion Prevention
ID Administration

How Does CHOP Do It?

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

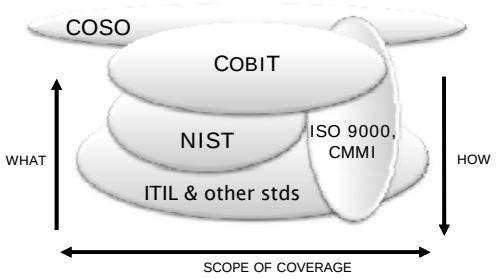
How Does CHOP Do It?

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



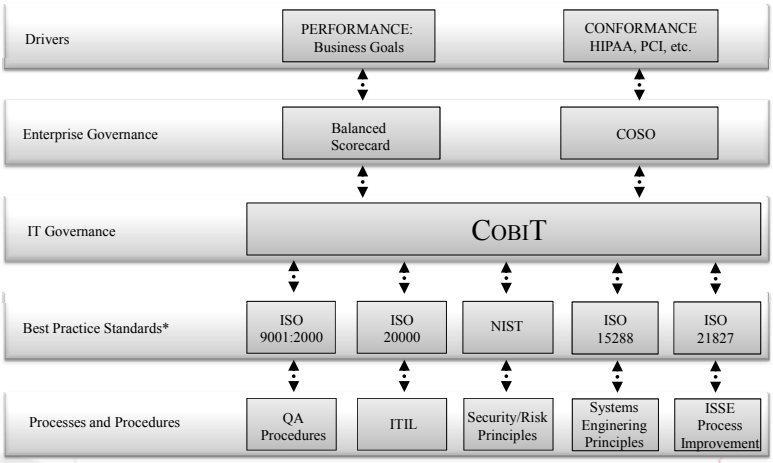
How Does CHOP Do It?

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



(adapted from ITGI, 2007, p. 11)

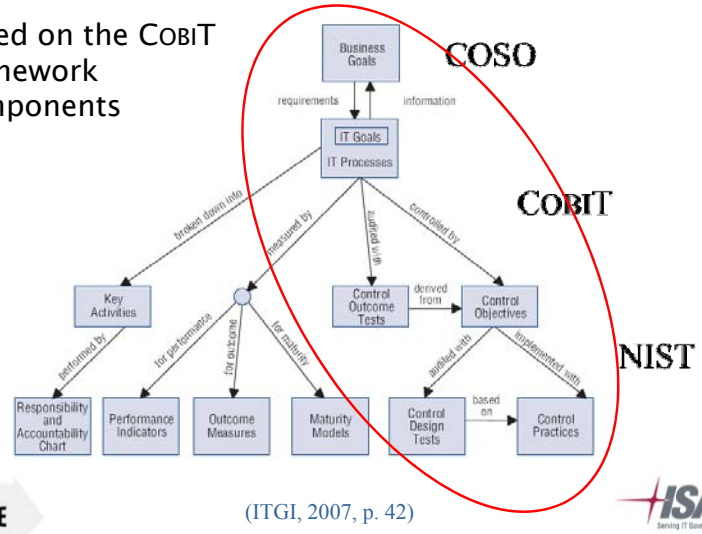
How Does CHOP Do It?



(adapted from ITGI, 2007, p. 12)

How Does CHOP Do It?

Based on the COBIT framework components



(ITGI, 2007, p. 42)

How Does CHOP Do It?

- Step 1: Understand and define the CHOP information risk universe
  - Determine risk mgmt stakeholders
  - Define IS vision/mission in relation to other risk mgmt stakeholders
  - Establish specific governance/risk frameworks
  - Establish IS-led risk mgmt processes

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.
Control Deficiency:	Excessive # of users have access to YYYY database.
Implementation Date:	11/30/08

#	Start Date	Actions	Completion Date	Responsible Party
Tactical Solution To Remediate Control Deficiencies [Indicate what actions may be required in the future to further improve established processes]				
	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 [Indicate what actions may be required in the future to further improve established processes]				
	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. **Note: Internal/external audit entities may request status of corrective action.**				
	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	

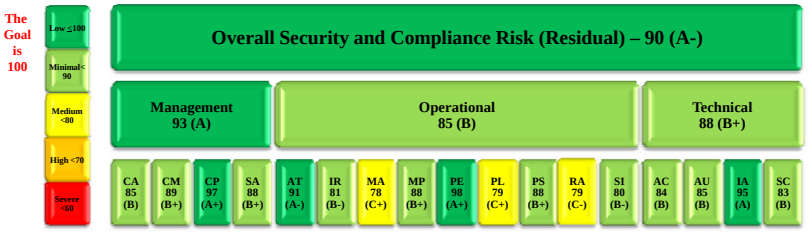
How Does CHOP Do It?

- 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

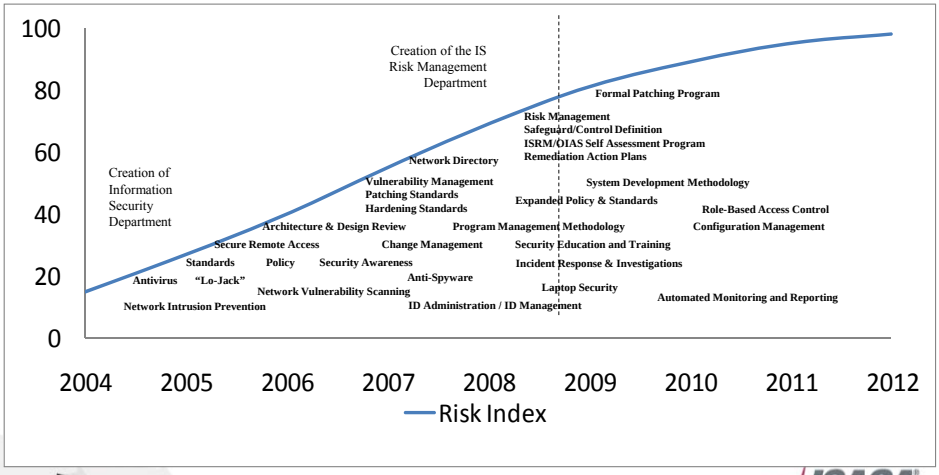
Operational Controls

- 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

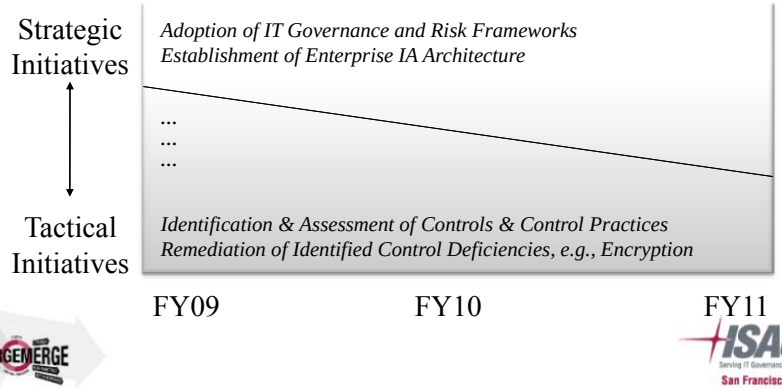
- AC: Access Control
- AU: Audit & Accountability
- IA: Identification & Authentication
- SC: System and Communications Protection

How Does CHOP Do It?



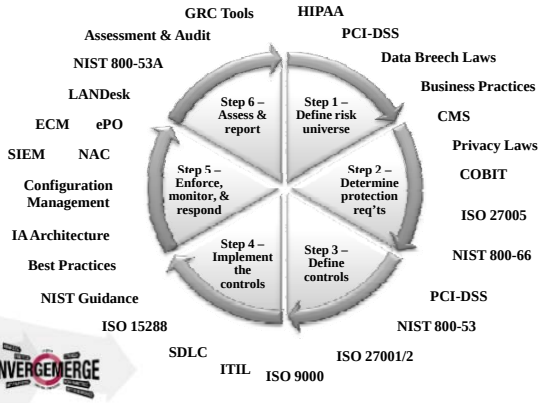
How Does CHOP Do It?

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



How Does CHOP Do It?

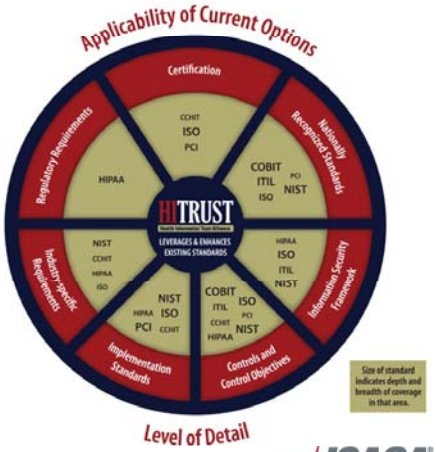
- Future … unified information security and compliance risk management



- 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 chose 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

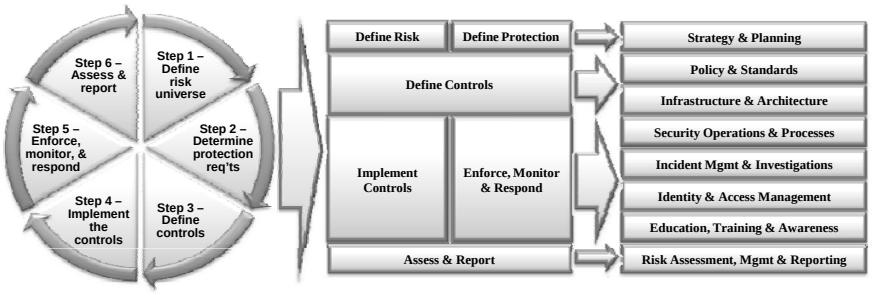
How Does CHOP Do It?

- 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

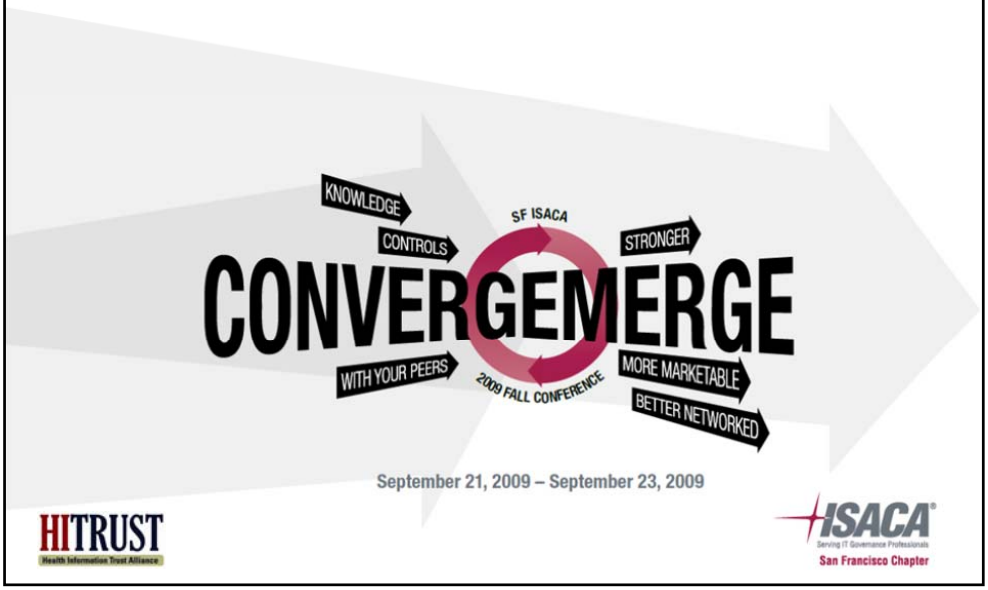
How Does CHOP Do It?

- 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

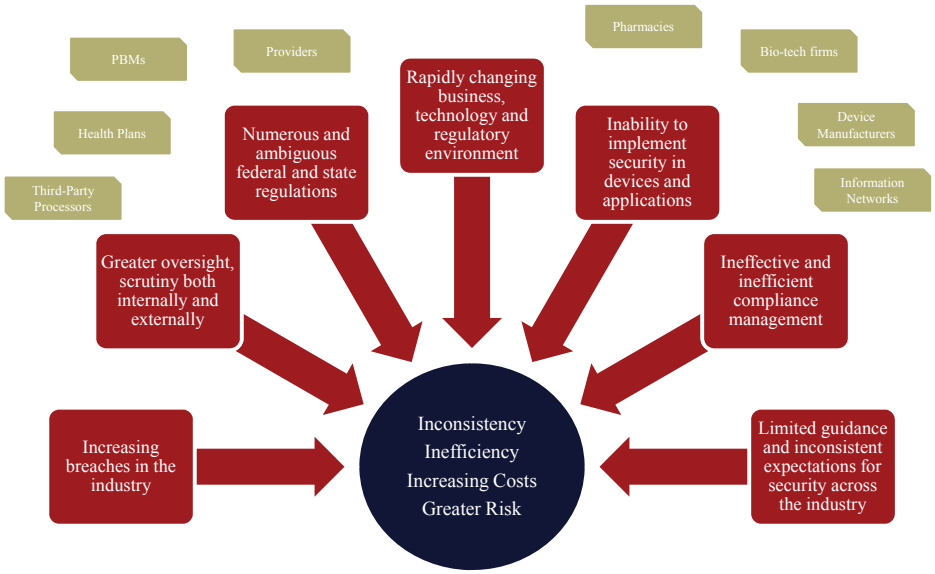
Questions?



Additional Slides



Industry Challenges and Realities



Page 44

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

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

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 DeMaioribus
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

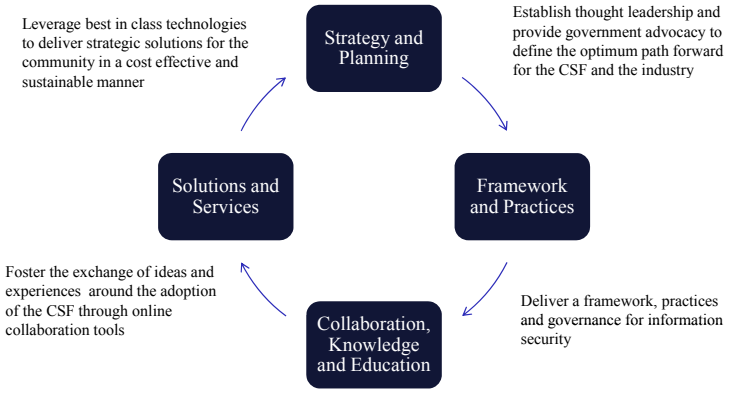
In the process of developing the Common Security Framework (CSF), a number of items were identified and summarized:

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



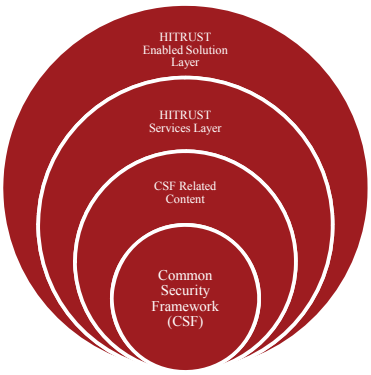
HITRUST has recognized that only by delivering a holistic and integrated approach to this issue will the healthcare industry be able to manage the complex task of cost effectively addressing information security for all organizations

Page 49

HITRUST's Core Content and Services

HITRUST's core content and services

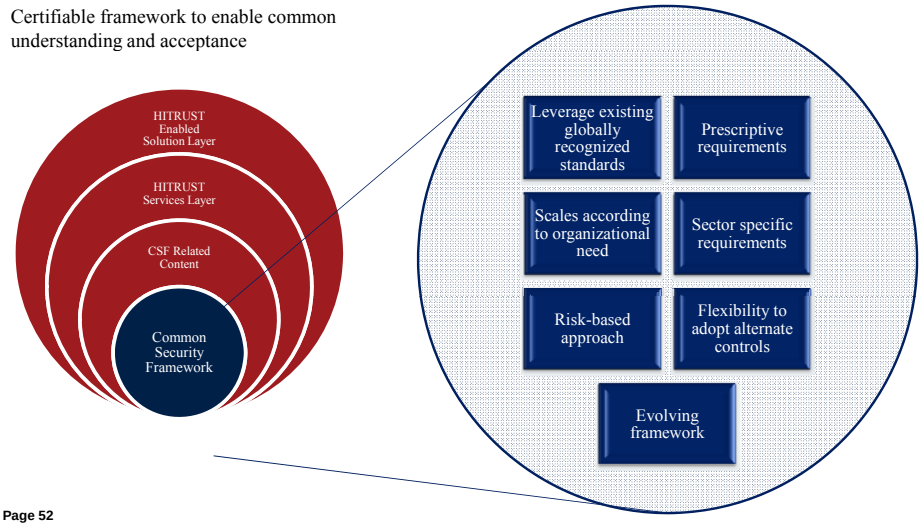
- HITRUST delivers an approach for the practical, efficient, and consistent adoption of security by the healthcare industry.
  - Common Security Framework (CSF) developed by the industry for the industry
  - Certification and reporting processes to simplify compliance with regulatory and business partner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



Page 51

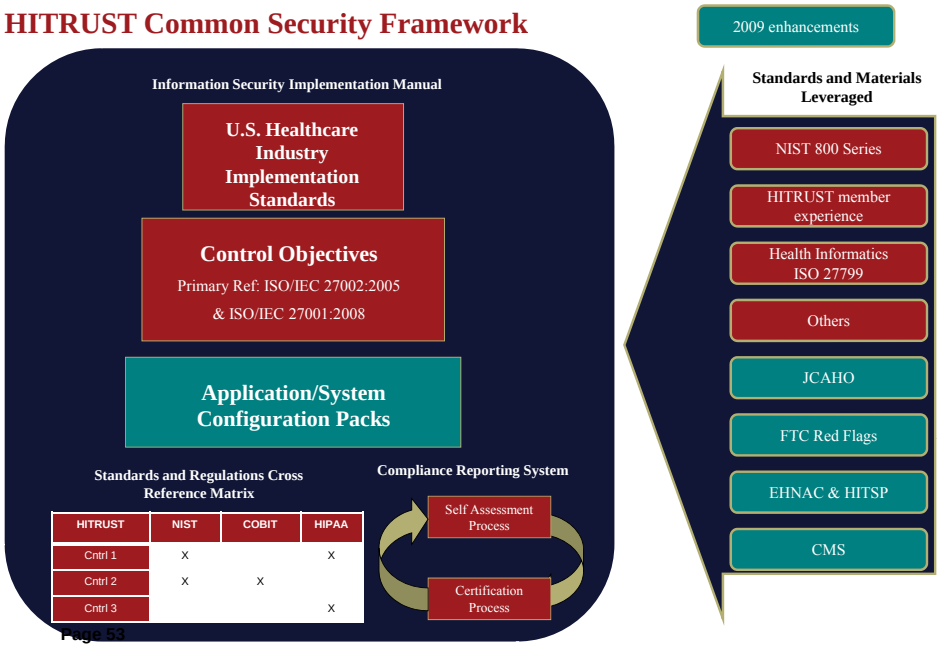
HITRUST CSF

Certifiable framework to enable common understanding and acceptance



Page 52

HITRUST Common Security Framework



Page 53

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

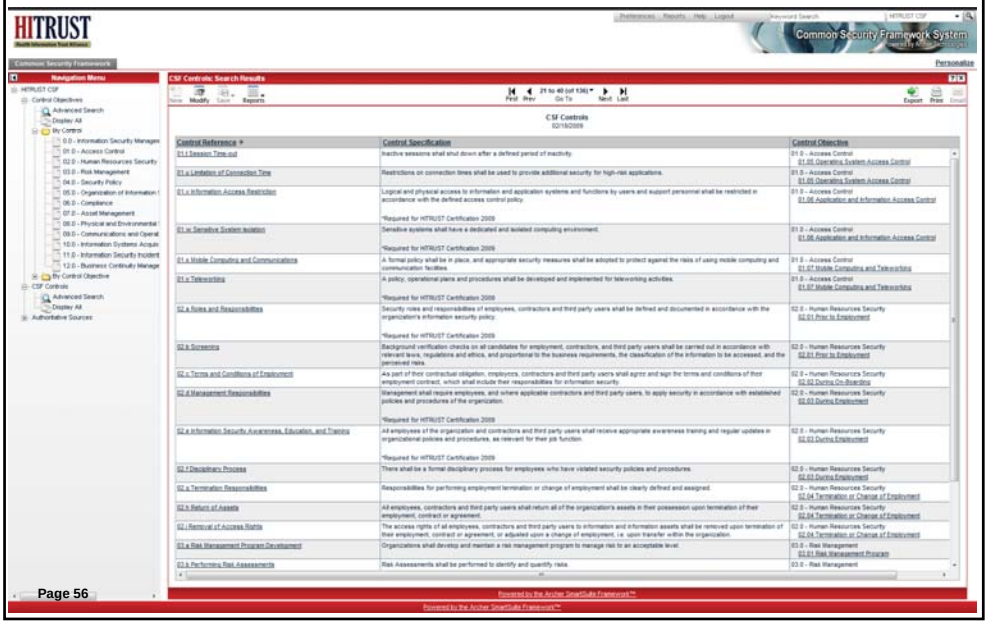
Page 54

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



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.

▸ General Information

▸ Level 1 Implementation Requirement

▸ Level 1 Alternate Controls

▾ Level 2 Implementation Requirement

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 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

Level 2 System Factors: None

Level 2 Regulatory Factors: Subject to PCI Compliance

Level 2 Implementation: Level 1 plus:

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.

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.

The reporting procedures shall include:

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:
    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.

Alerts from the organization's intrusion-detection and intrusion-prevention systems shall be utilized for reporting information security events.

Level 2 Control Audit Procedure: Examine:

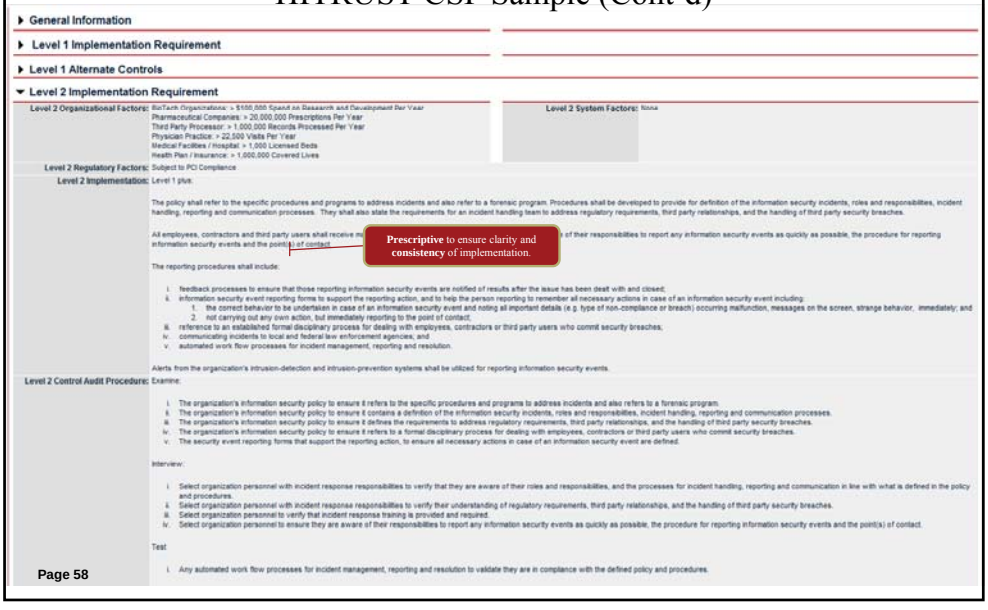
i. The organization's information security policy to ensure it refers to the specific procedures and programs to address incidents and also refers to a forensic program.
ii. The organization's information security policy to ensure it contains a definition of the information security incidents, roles and responsibilities, incident handling, reporting and communication processes.
iii. The organization's information security policy to ensure it 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 it 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.

Interview:

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.

Page 57

HITRUST CSF Sample (Cont'd)



▸ General Information

▸ Level 1 Implementation Requirement

▸ Level 1 Alternate Controls

▾ Level 2 Implementation Requirement

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 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

Level 2 System Factors: None

Level 2 Regulatory Factors: Subject to PCI Compliance

Level 2 Implementation: Level 1 plus:

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.

All employees, contractors and third party users shall receive m… 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.

Prescriptive to ensure clarity and **consistency** of implementation.

The reporting procedures shall include:

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:
    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.

Alerts from the organization's intrusion-detection and intrusion-prevention systems shall be utilized for reporting information security events.

Level 2 Control Audit Procedure: Examine:

i. The organization's information security policy to ensure it 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 it 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 it 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 it 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.

Interview:

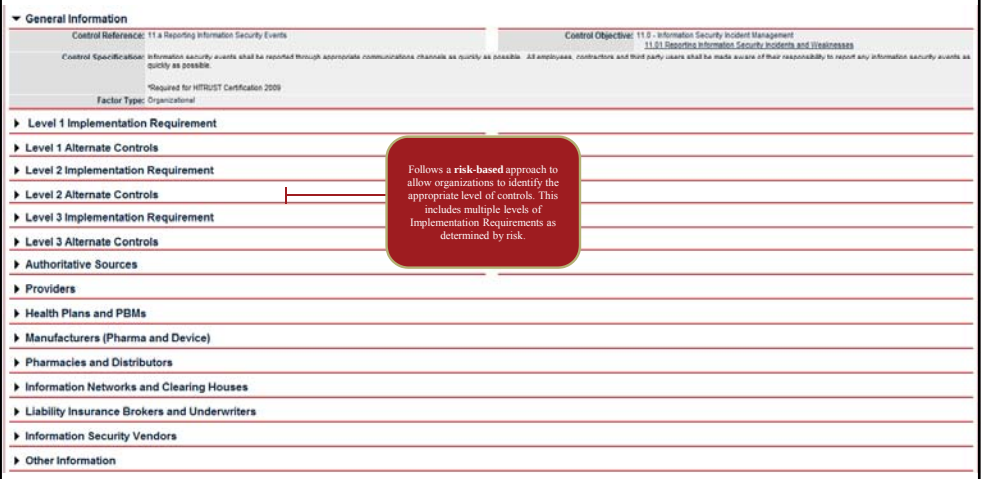
i. Select organization personnel with incident response responsibilities to verify that they are aware of their roles and responsibilities, and the processes for incident handling, reporting and communication in line with what is defined in the policy and procedures.
ii. Select organization personnel 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.

Test

i. Any automated work flow processes for incident management, reporting and resolution to validate they are in compliance with the defined policy and procedures.

Page 58

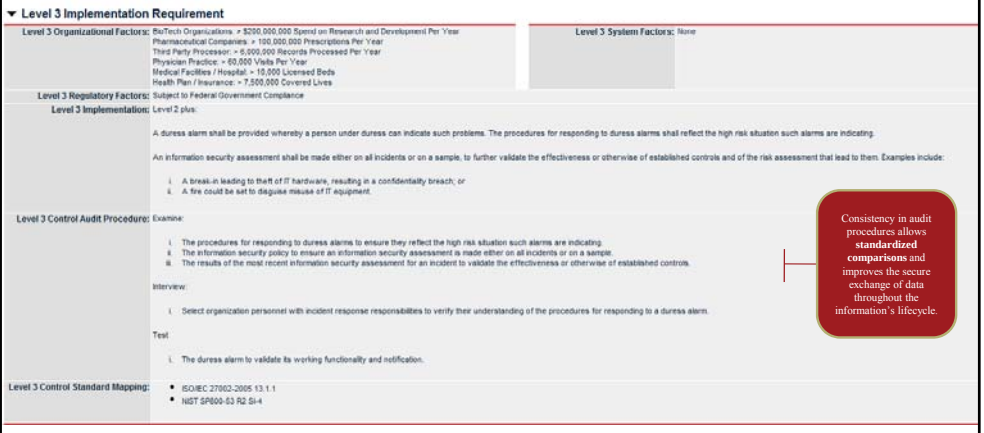
HITRUST CSF Sample (Cont'd)



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.

Page 59

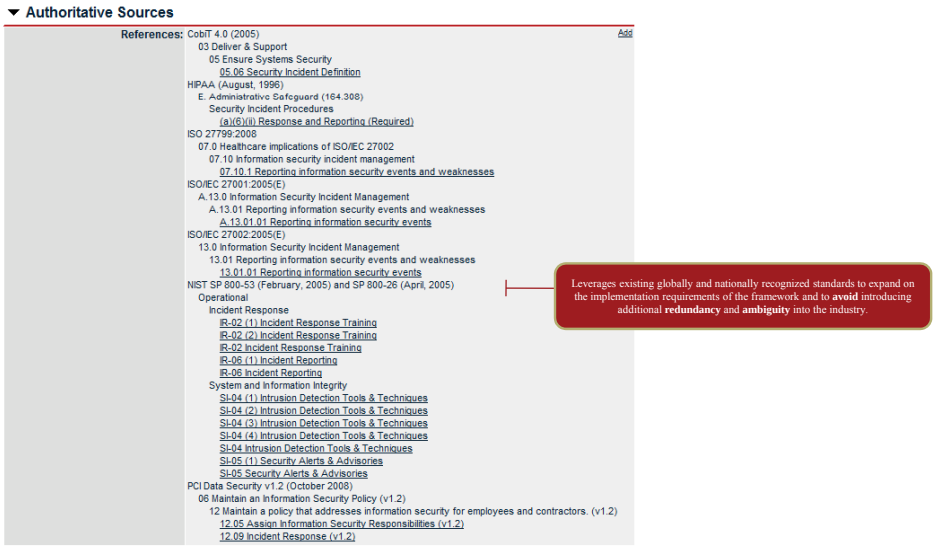
HITRUST CSF Sample (Cont'd)



Consistency in audit procedures allows **standardized comparisons** and improves the secure exchange of data throughout the information's lifecycle.

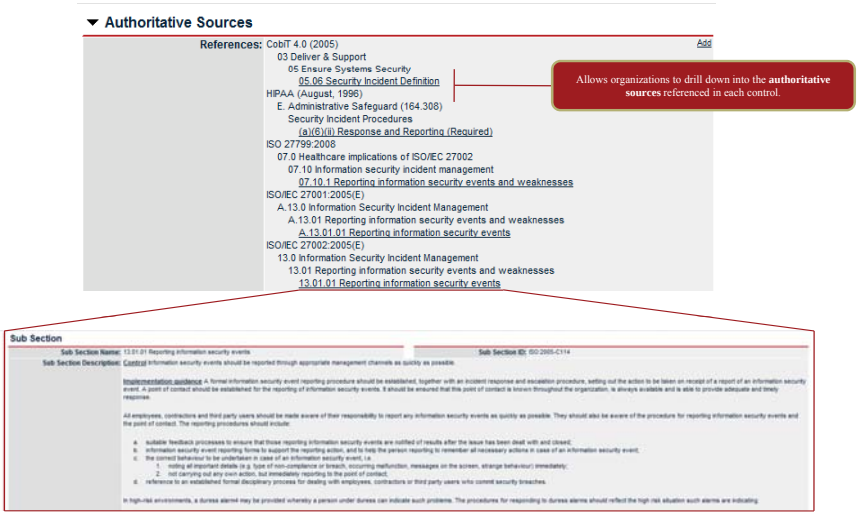
Page 60

HITRUST CSF Sample (Cont'd)



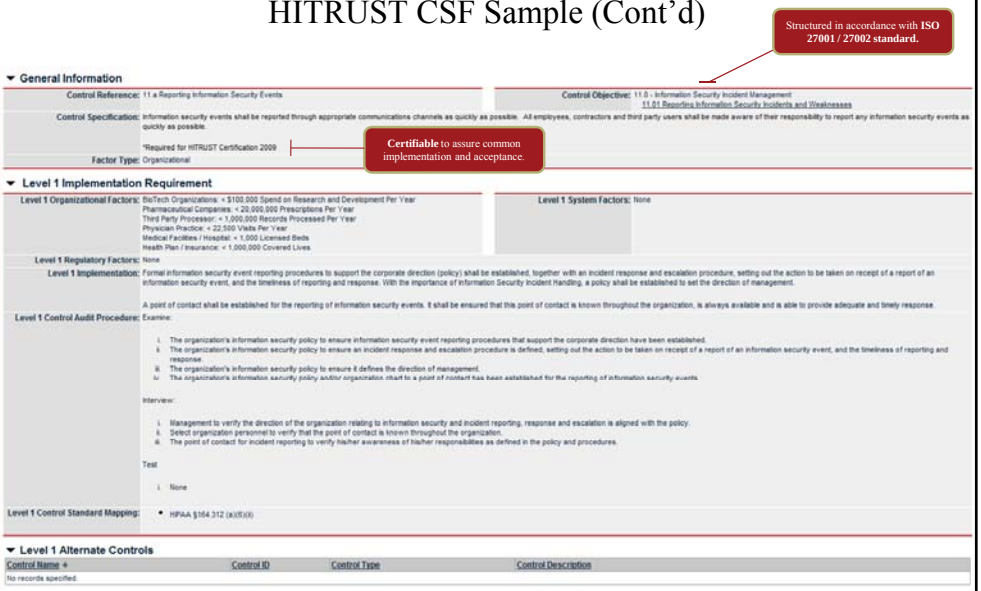
Page 61

HITRUST CSF Sample (Cont'd)



Page 62

HITRUST CSF Sample (Cont'd)



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

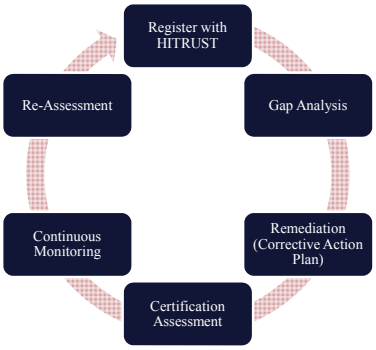
The requirements imposed on HITRUST CSF Certifiers include:

- 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

Page 64

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

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?

Page 66

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**

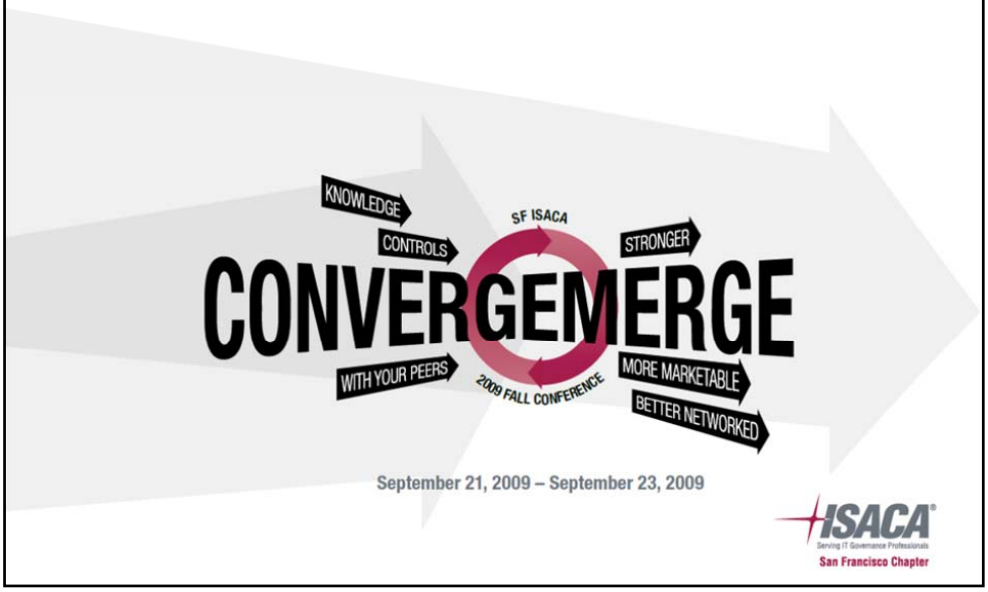
"The HITRUST CSF program is creating what has been lacking in the healthcare industry relating to information security guidance and clarity. It removes the confusion, inconsistencies and variability that have existed to date in how organizations have implemented security measures." – G. Christopher Hall,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

BACKUP SLIDES



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 out-sourcing 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(Threat, Vulnerability) ≐ 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(Asset, Loss) ≐ 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
  - Residual Risk = Inherent Risk – Controlled Risk
- Residual risk is made up of two components: acceptable and unacceptable
  - (Residual Risk_A + Residual Risk_U) = Inherent Risk – 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
  - (Control Risk + Uncontrolled Risk) + Residual Risk_U = Inherent Risk – 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
  - Residual Risk_U = Inherent Risk – Controlled Risk – Control Risk – Uncontrolled Risk

72

Residual Risk

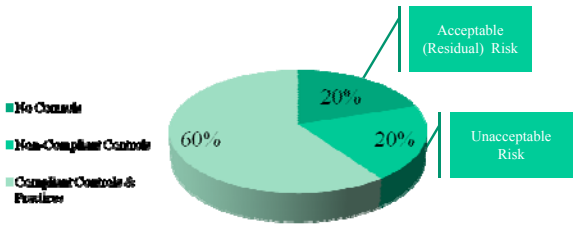
- In order to minimize unacceptable residual risk, one must either mitigate more risk through the application of additional controls (or more rigorous control practices) OR accept more residual risk through the application of fewer controls (or less rigorous control practices)
  - Residual Risk $_U$ = Inherent Risk – Controlled Risk – (Control Risk + 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 $_U$ ≐ F(Level of Control Compliance, Impact of Control Failure)
    ≐ $[\sum^n$ Compliance · Impact$]$ / n, where n = 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

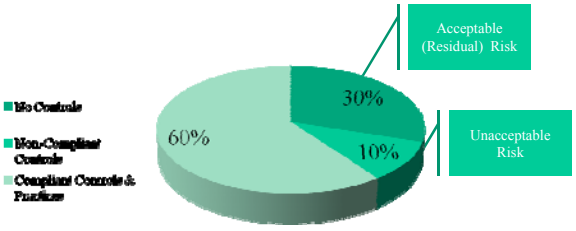


Risk Index ≐ 75.0 (C)

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 ≐ 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. 6)

76

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:

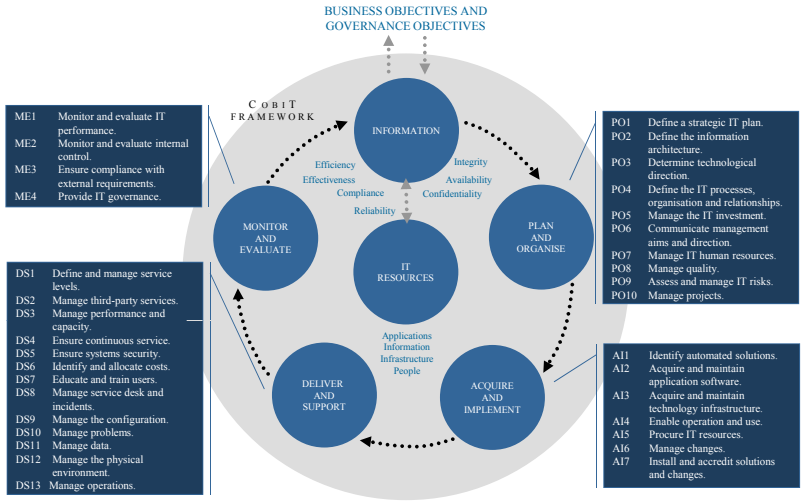
- *Starts from business requirements*
- Is process-oriented, organizing IT activities into a generally accepted process model
- Identifies the major IT resources to be leveraged
- Defines the management control objectives to be considered
- Incorporates major international standards
- Has become the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