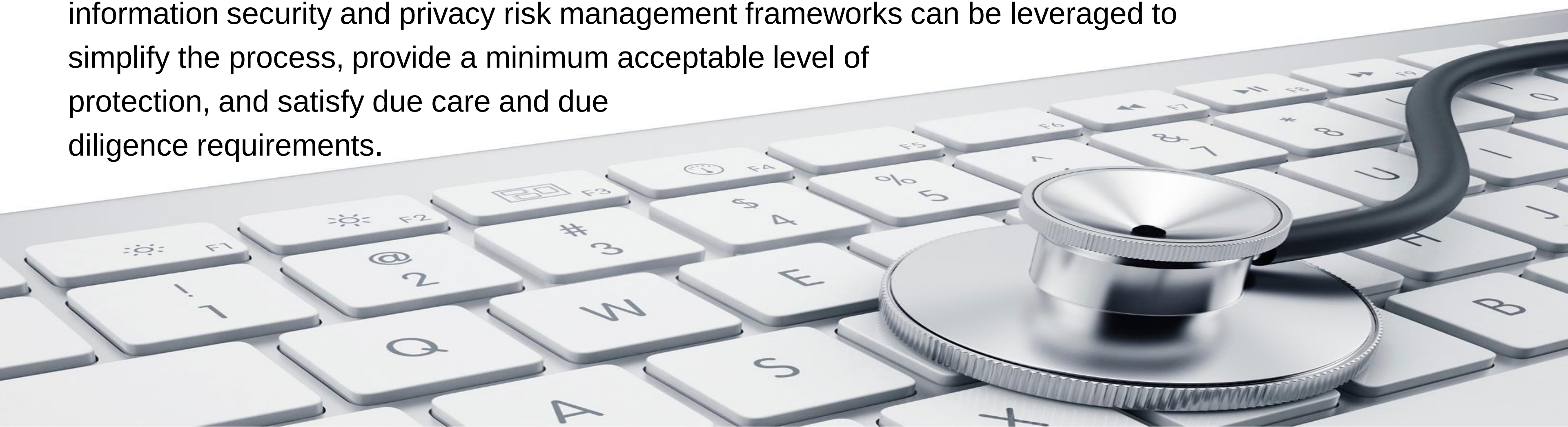
HITRUST CSF:

Leveraging Control-based Risk Management Frameworks to Support a HIPAA Compliant Risk Analysis

Dr. Bryan Cline, CISSP-ISSEP, CISM, CISA, CCSFP, HCISPP
VP Standards & Analytics, Health Information Trust Alliance
Adjunct Professor, University of Fairfax

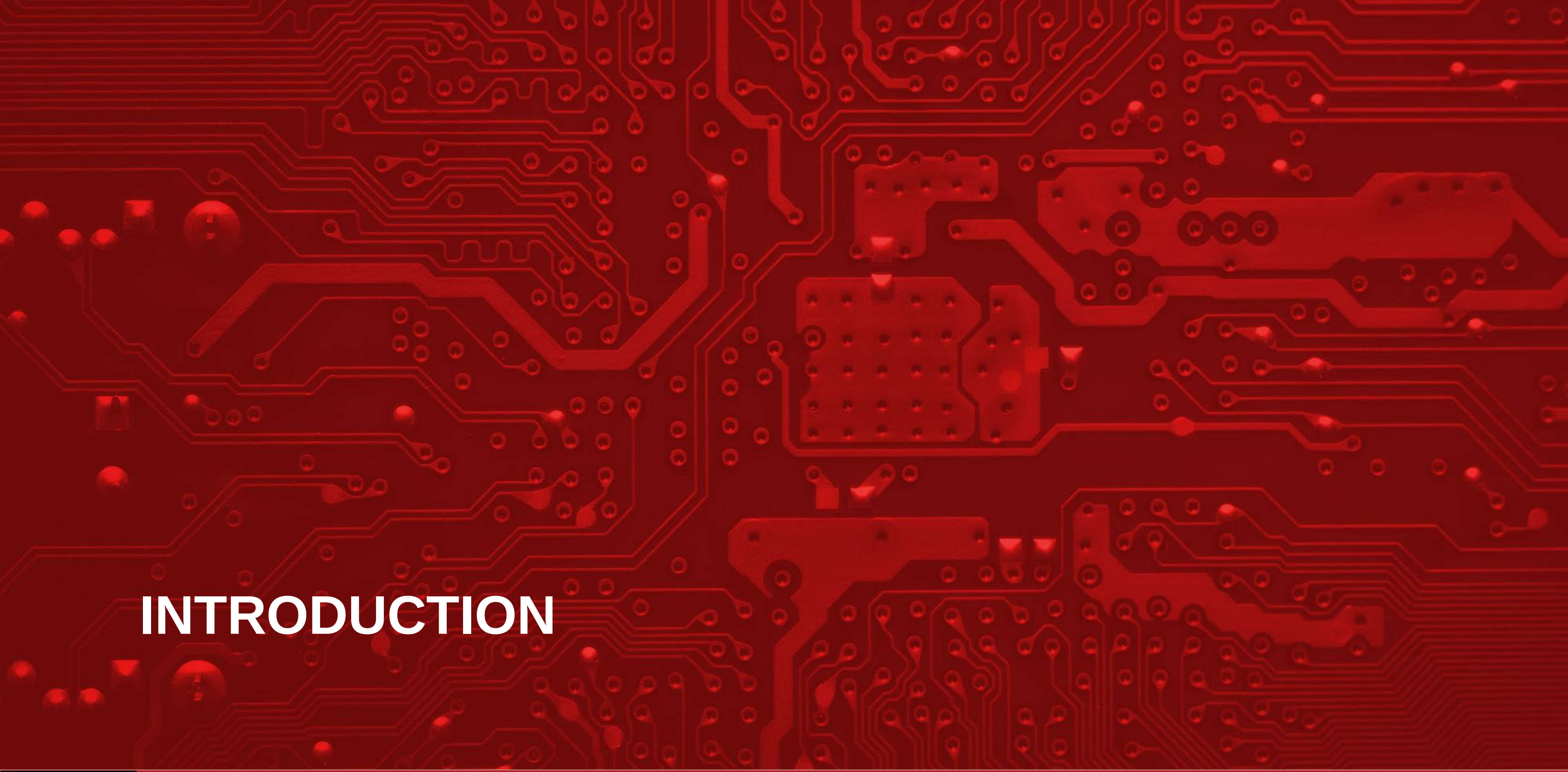
Abstract

The increasing digitization of health information and the ever changing cybersecurity threat environment has led to some rather public health data breaches over the past few years. And this trend will likely continue as healthcare organizations struggle to determine and implement a reasonable and appropriate set of safeguards. This presentation will show how industry-recognized, control-based information security and privacy risk management frameworks can be leveraged to simplify the process, provide a minimum acceptable level of protection, and satisfy due care and due diligence requirements.



Topics to Cover

- Introduction
- Threat Environment
- Risk Management
- Risk Analysis (RA) & Control Selection
- Control-based Risk Mgmt. Frameworks
- Framework-based RA & Control Selection
- Top 3 Tips for Leveraging a Framework
- Q&A



INTRODUCTION

Multitude of Challenges Managing Risk

- Cost and complexity
  - Redundant/inconsistent requirements/standards
- Confusion
  - What is reasonable, appropriate or adequate?
- Audit fatigue
  - Too many audits with subjective requirements
- Increased scrutiny and oversight
  - Regulators, auditors, and other stakeholders
- Growing risk and liability
  - Breach and legal costs; regulatory penalties
- Lack of resources
  - Limited budgets and trained personnel
- *Constantly changing threat environment …*

HEALTH IT

CMS to check hospitals for HIPAA security compliance

WellPoint probing data breach for 130,000 members

Business Journal

Providence to pay $100K for HIPAA violations

TJX data breach: At 45.6M card numbers, it's the biggest ever

3 accused of inducing ill effects on computers at local hospital

California's Data Breach Notification Law Now Covers Medical and Health Insurance Information

HITRUST Mission

In 2007, the Health Information Trust Alliance (HITRUST) was formed by a group of concerned healthcare organizations out of the belief improvements in the state of information security and privacy in the industry are critical to the broad adoption, utilization and confidence in health information systems, medical technologies and electronic exchanges of health information, all of which are necessary to improve the quality of patient care while lowering the cost of healthcare delivery.

Key Objectives:

- Increase the protection of health & other sensitive information
- Mitigate & aid in the management of risk associated with health information
- Contain & manage costs associated with appropriately protecting sensitive information
- Increase consumer & governments' confidence in the industry's ability to safeguard health information
- Address increasing concerns associated with business associate and 3rd party privacy, security and compliance
- Work with federal & state governments / agencies and other oversight bodies to collaborate with industry on information protection
- Facilitate sharing & collaboration relating to information protection amongst healthcare organizations of varying types & sizes
- Enhance and mature the knowledge and competency of health information protection professionals

HITRUST “In a Snapshot”

Best known for:

- Developing HITRUST CSF—in 7th major release—and supporting CSF Assurance Program
- Local, regional and national-level cyber preparedness and response exercises for healthcare organizations—CyberRX

Adoption of CSF

- By 83% of hospitals[1] (most widely adopted); by 82% of health plans[2] (most widely adopted)

Adoption of CSF Assurance

- Over 23,000 CSF assessments in last three years (10,000 in 2014); most widely utilized approach by healthcare organizations and 3rd parties
- Supports the State of Texas Healthcare Information Privacy and Security Certification–SECURETexas

Supporting Cyber Threat Intelligence Sharing and Incident Preparedness and Response

- Operates Cyber Threat Exchange (CTX) as industry cyber threat early warning system and to automate indicator of compromise distribution
- Federally recognized Information Sharing and Analysis Organization (ISAO)
- Information sharing agreement with HHS and DHS as part of critical infrastructure program
- Partnership with HHS for monthly industry cyber threat briefings and industry cyber threat preparedness and response exercises (CyberRX)

Information Protection Education and Training

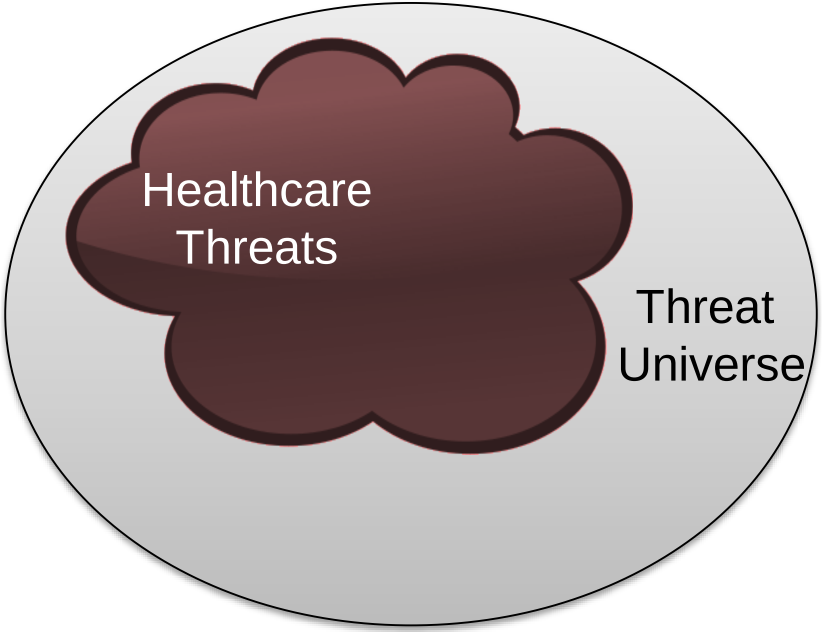
- Over 1500 professionals obtained Certified Common Security Framework Practitioner (CCSFP) designation—CSF specific
- Partnered with International Information System Security Certification Consortium, Inc., (ISC)^2 to develop broader healthcare certified information security professional credential—HealthCare Information Security and Privacy Practitioner (HCISPP)
- In 2012, HITRUST began holding an annual nationally-attended conference specifically for health information protection professionals

1 – Based on facilities in the 2011 AHA hospital and health system data as of Dec 2012 that have licensed the CSF; 2 – Based on health plans with over 500,000 members as of Dec 2012 that have licensed the CSF

THREAT ENVIRONMENT

Threat Environment

The constantly changing threat environment in healthcare …

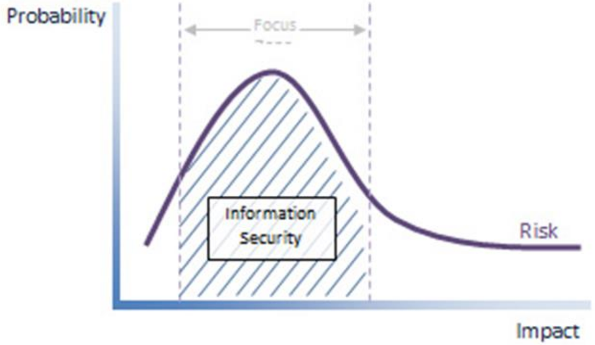


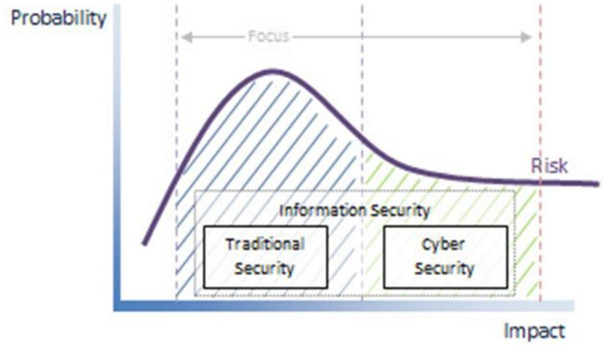
Healthcare Threats

Threat Universe

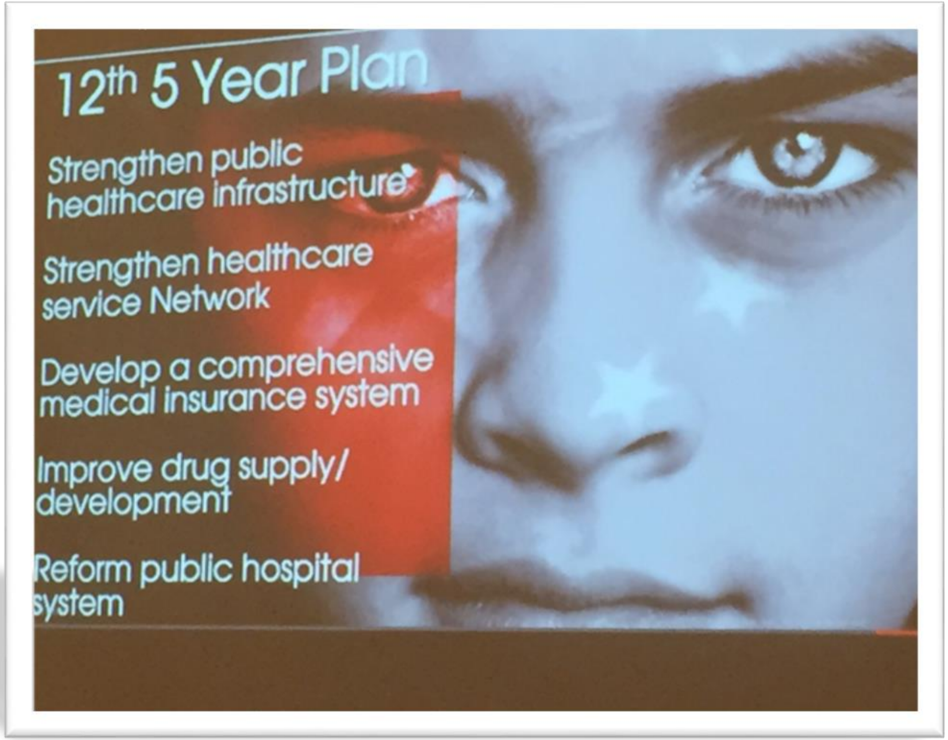
Threat Environment

- Intended to depict risk as a function of the probability a threat will successfully exploit a vulnerability and its potential impact
- Historically cyber security threats to healthcare entities has been relatively low
- The threat landscape has now evolved to the point where cyber threats once considered unlikely occur with unfortunate regularity
  - Higher maturity of detection & attack tools and methods (exploits)
  - Increased diversity and motivation of attackers (threat actors)
  - More electronic information and networked applications (vulnerabilities)





Threat Environment



12th 5 Year Plan

Strengthen public healthcare infrastructure

Strengthen healthcare service Network

Develop a comprehensive medical insurance system

Improve drug supply/ development

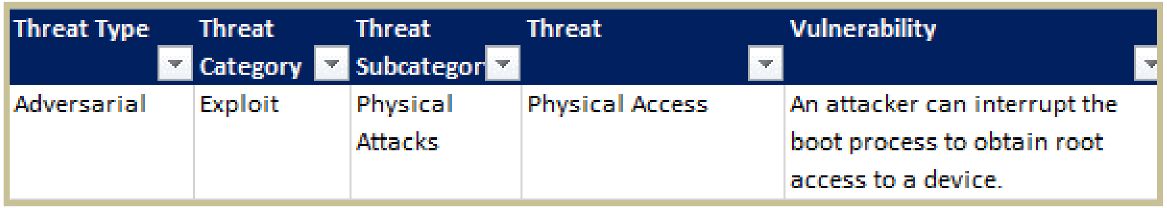
Reform public hospital system

- China is coming for you
- Other adversaries are also active against the healthcare industry
  - Opportunistic
  - Targeted

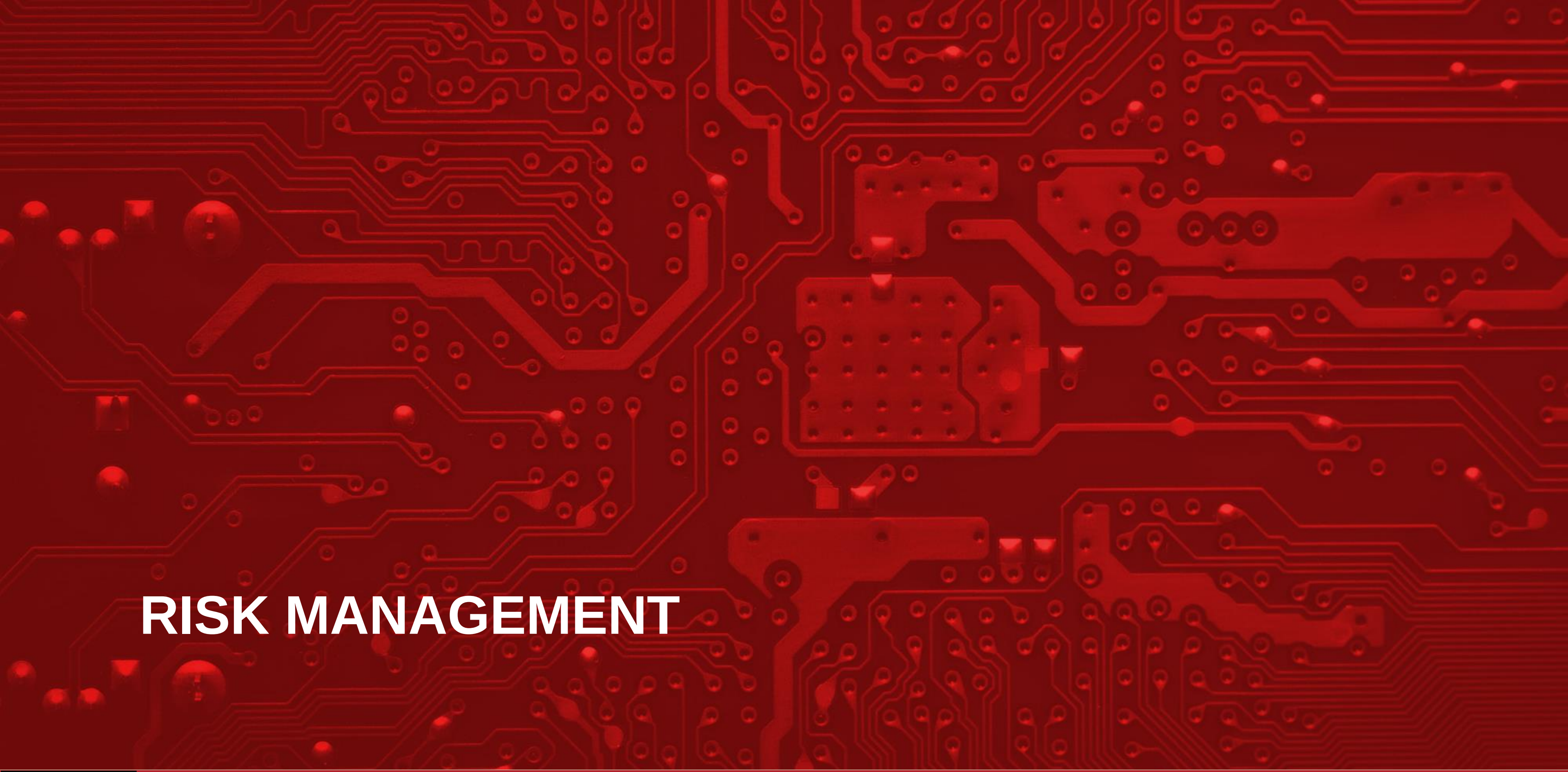
From the CrowdStrike presentation at HITRUST 2015

Threat Environment

- Some sources for threat information exist in various forms
- Complete threat-vulnerability pair enumeration can
  - Result in literally thousands of threat-vulnerability pairs
  - Require expertise and $$ to build and maintain



Threat Type	Threat Category	Threat Subcategor	Threat	Vulnerability
Adversarial	Exploit	Physical Attacks	Physical Access	An attacker can interrupt the boot process to obtain root access to a device.



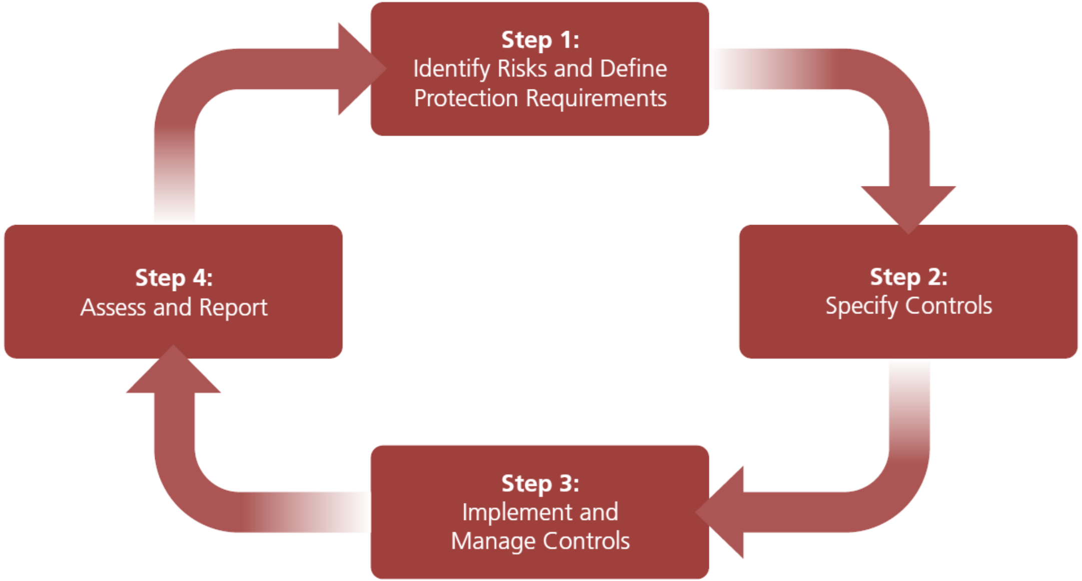
RISK MANAGEMENT

Risk Management

Risk management may be defined as …

- “The process whereby organizations methodically address the risks attach[ed] to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.” (IRM)
- “The process of managing risks to organizational operations[,]… organizational assets or individuals resulting from the operation of an information system, and includes:
  - the conduct of a risk assessment;
  - the implementation of a risk mitigation strategy; and
  - employment of techniques and procedures for the continuous monitoring of the security state of the information system.” (FIPS 200)

Risk Management Process (Life Cycle)

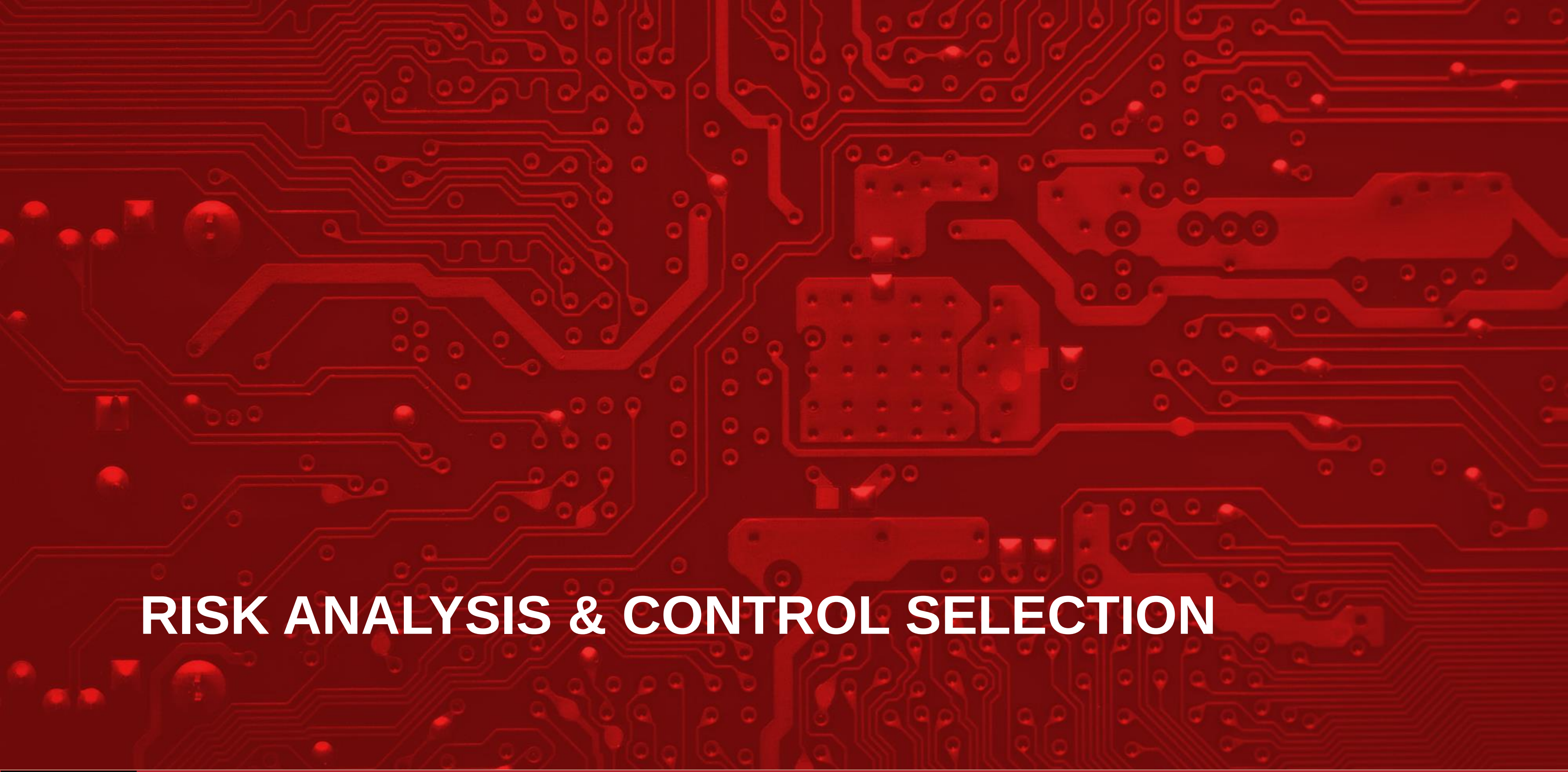


Step 1:
Identify Risks and Define Protection Requirements

Step 2:
Specify Controls

Step 3:
Implement and Manage Controls

Step 4:
Assess and Report



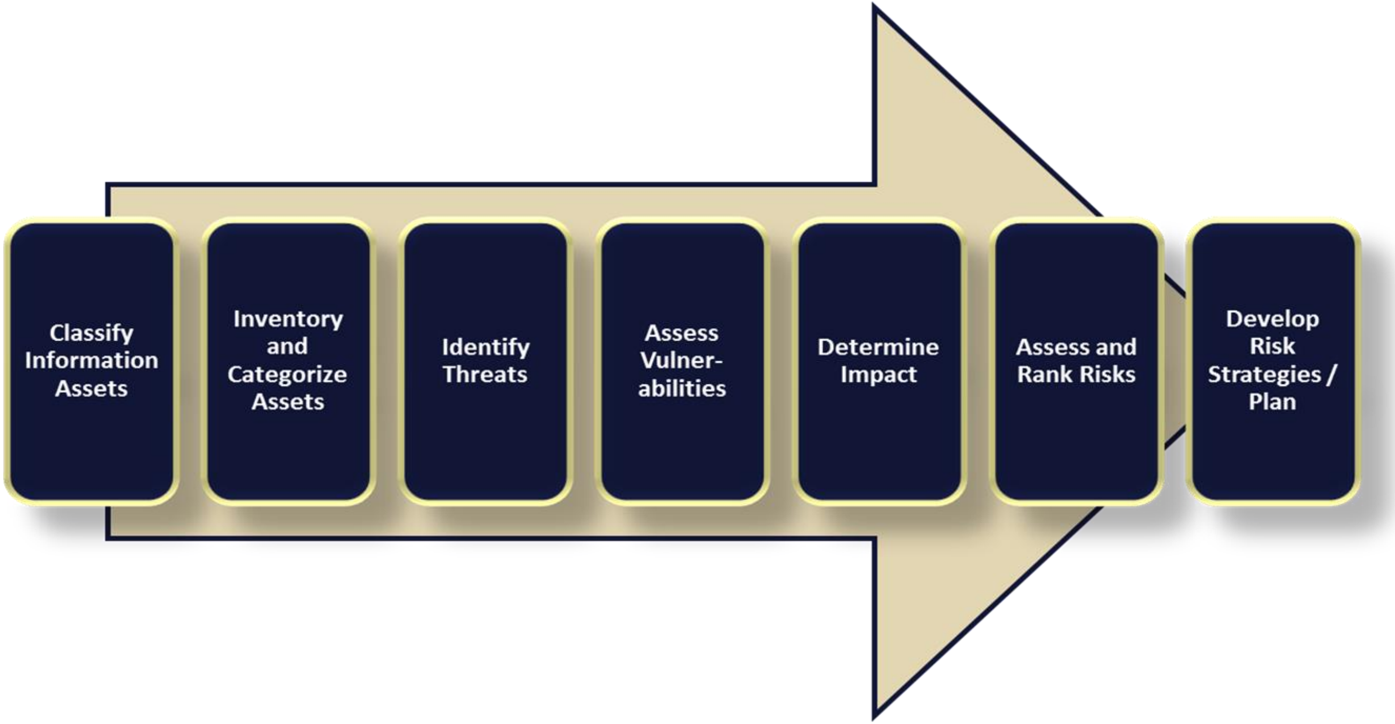
RISK ANALYSIS & CONTROL SELECTION

Risk Analysis

What is risk analysis (RA)?

- Synonymous with ‘risk assessment’ *(CNSSI No. 4009)*
- The process of identifying, estimating, and prioritizing risks … resulting from the operation of an information system; part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place *(NIST SP 800-39)*
- The first step in identifying and implementing safeguards *(HHS Guidance on Risk Analysis Requirements under the HIPAA Security Rule)*

Risk Analysis/Assessment Process (1)



Classify Information Assets

Inventory and Categorize Assets

Identify Threats

Assess Vulner-abilities

Determine Impact

Assess and Rank Risks

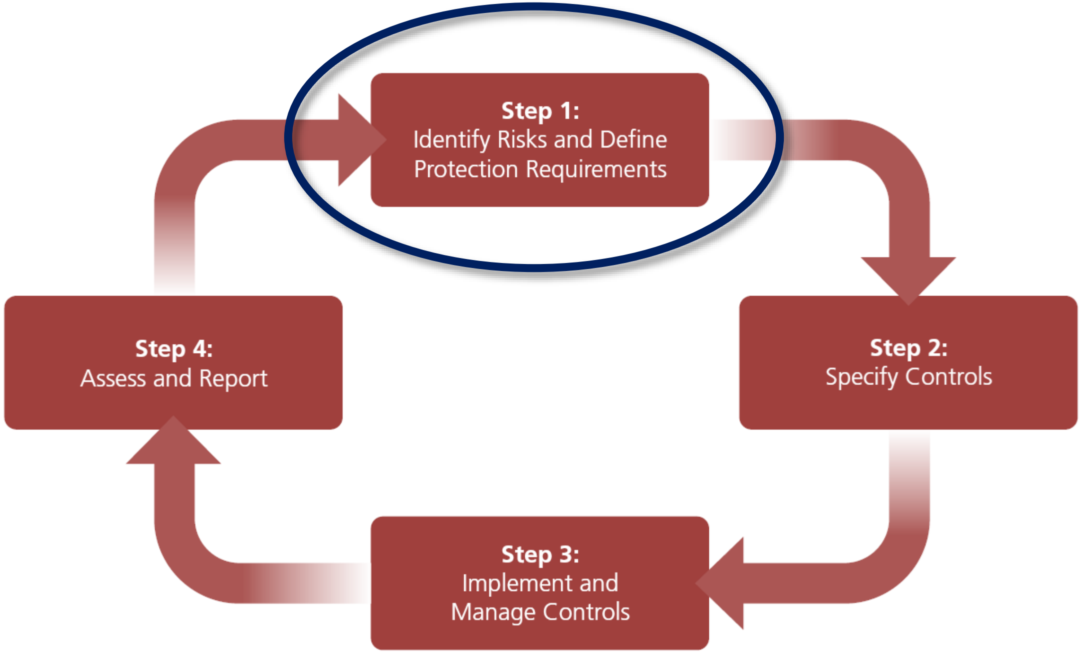
Develop Risk Strategies / Plan

Risk Analysis/Assessment Process (2)

NIST process is consistent with DHHS guidance on RA.

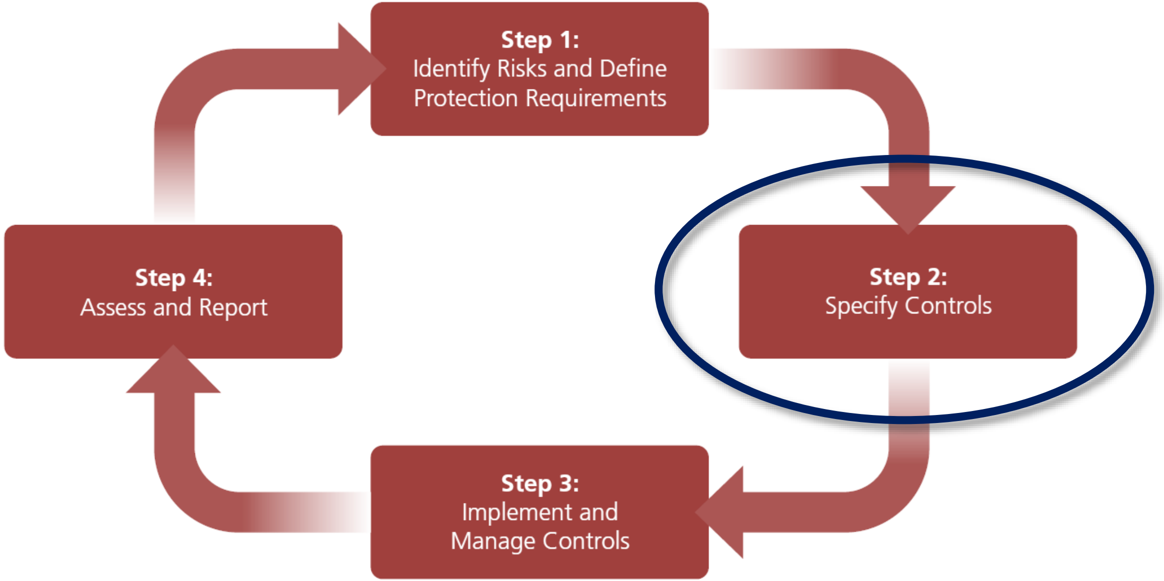
- Scope the assessment to include all ePHI
- Identify & document all assets with ePHI
- Identify & document all reasonably anticipated threats to ePHI
- Assess all current security measures
- Determine the likelihood of threat occurrence
- Determine the potential impact of a threat occurrence
- Determine the level of risk
- Document assigned risk levels and corrective actions

Risk Analysis/Assessment Process (3)


Step 1:
Identify Risks and Define Protection Requirements
Step 2:
Specify Controls
Step 3:
Implement and Manage Controls
Step 4:
Assess and Report

Risk Analysis & Control Selection

Objective of RA is to support control specification/selection.



Step 1:
Identify Risks and Define Protection Requirements
Step 2:
Specify Controls
Step 3:
Implement and Manage Controls
Step 4:
Assess and Report

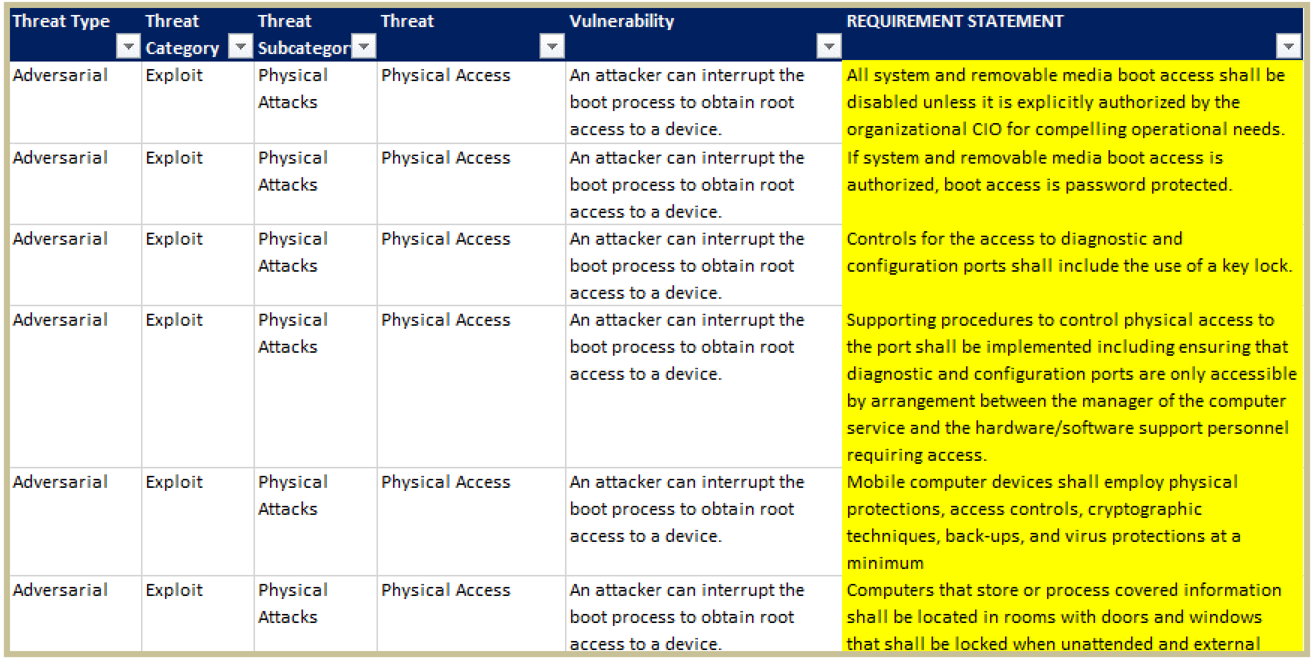
Approaches to Control Selection (1)

There are two general approaches to initial / baseline control selection.

1) Conduct comprehensive risk analysis
   - Threat & vulnerability assessment
   - Information asset valuation
   - Information protection control selection
2) Leverage a framework and modify a baseline control standard
   - Threat modeling / control selection performed by capable, 3rd party for general threats, vulnerabilities
   - Baseline controls based on confidentiality/criticality
   - Limited RA performed for organization-unique requirements

Approaches to Control Selection (2)

Two Approaches To Initial/Baseline Control Selection (Continued)

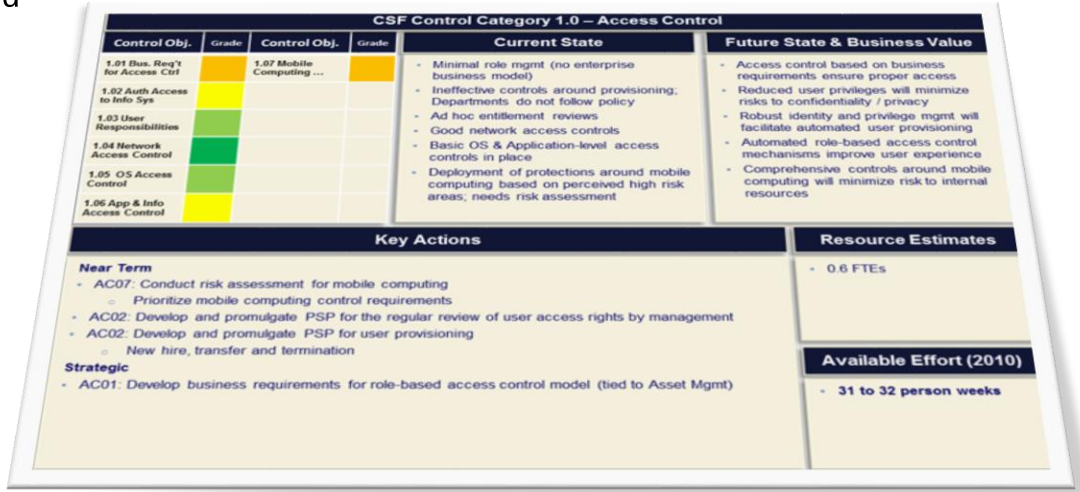


Threat Type	Threat Category	Threat Subcategor	Threat	Vulnerability	REQUIREMENT STATEMENT
Adversarial	Exploit	Physical Attacks	Physical Access	An attacker can interrupt the boot process to obtain root access to a device.	All system and removable media boot access shall be disabled unless it is explicitly authorized by the organizational CIO for compelling operational needs.
Adversarial	Exploit	Physical Attacks	Physical Access	An attacker can interrupt the boot process to obtain root access to a device.	If system and removable media boot access is authorized, boot access is password protected.
Adversarial	Exploit	Physical Attacks	Physical Access	An attacker can interrupt the boot process to obtain root access to a device.	Controls for the access to diagnostic and configuration ports shall include the use of a key lock.
Adversarial	Exploit	Physical Attacks	Physical Access	An attacker can interrupt the boot process to obtain root access to a device.	Supporting procedures to control physical access to the port shall be implemented including ensuring that diagnostic and configuration ports are only accessible by arrangement between the manager of the computer service and the hardware/software support personnel requiring access.
Adversarial	Exploit	Physical Attacks	Physical Access	An attacker can interrupt the boot process to obtain root access to a device.	Mobile computer devices shall employ physical protections, access controls, cryptographic techniques, back-ups, and virus protections at a minimum
Adversarial	Exploit	Physical Attacks	Physical Access	An attacker can interrupt the boot process to obtain root access to a device.	Computers that store or process covered information shall be located in rooms with doors and windows that shall be locked when unattended and external

Approaches to Control Selection (3)

Two Approaches To Initial/Baseline Control Selection (Continued)

- Comprehensive RA is difficult for most organizations
- Lack of skilled resources, funding, time; limited information
- Baseline control approach most widely used
  - ISO/IEC 27001/27002
  - NIST SP 800-53
  - HITRUST CSF



CSF Control Category 1.0 – Access Control

Control Obj.	Grade	Control Obj.	Grade
1.01 Bus. Req't for Access Ctrl	🟧	1.07 Mobile Computing …	🟧
1.02 Auth Access to Info Sys	🟨		
1.03 User Responsibilities	🟩		
1.04 Network Access Control	🟩		
1.05 OS Access Control	🟩		
1.06 App & Info Access Control	🟨		

Current State

- Minimal role mgmt (no enterprise business model)
- Ineffective controls around provisioning; Departments do not follow policy
- Ad hoc entitlement reviews
- Good network access controls
- Basic OS & Application-level access controls in place
- Deployment of protections around mobile computing based on perceived high risk areas; needs risk assessment

Future State & Business Value

- Access control based on business requirements ensure proper access
- Reduced user privileges will minimize risks to confidentiality / privacy
- Robust identity and privilege mgmt will facilitate automated user provisioning
- Automated role-based access control mechanisms improve user experience
- Comprehensive controls around mobile computing will minimize risk to internal resources

Key Actions

Near Term

- AC07: Conduct risk assessment for mobile computing
  - Prioritize mobile computing control requirements
- AC02: Develop and promulgate PSP for the regular review of user access rights by management
- AC02: Develop and promulgate PSP for user provisioning
  - New hire, transfer and termination

Strategic

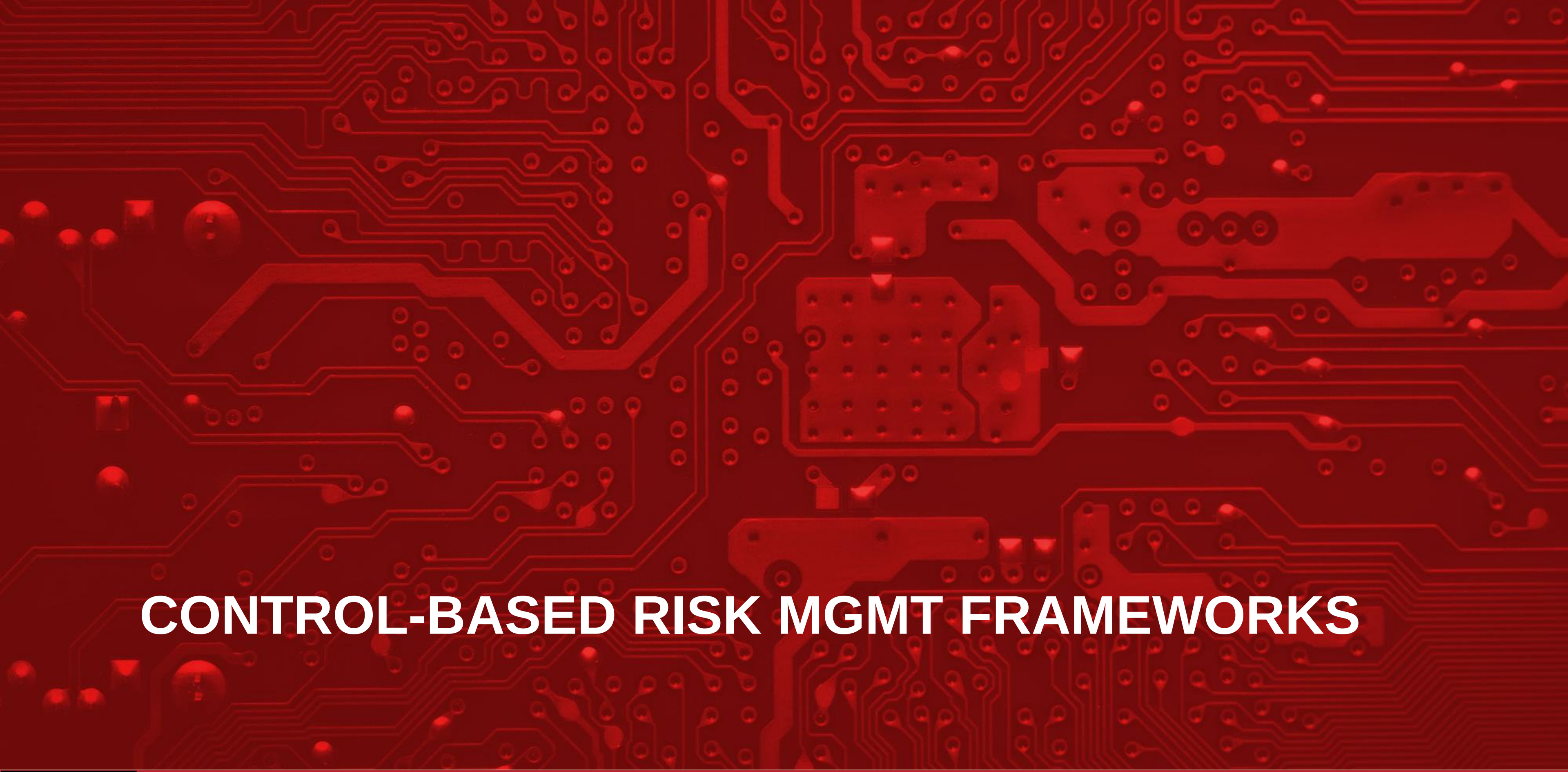
- AC01: Develop business requirements for role-based access control model (tied to Asset Mgmt)

Resource Estimates

- 0.6 FTEs

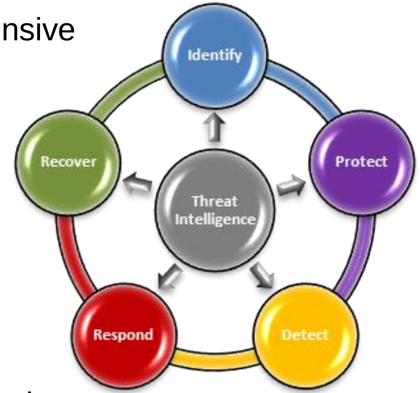
Available Effort (2010)

- **31 to 32 person weeks**



CONTROL-BASED RISK MGMT FRAMEWORKS

Cybersecurity and Risk Management Frameworks

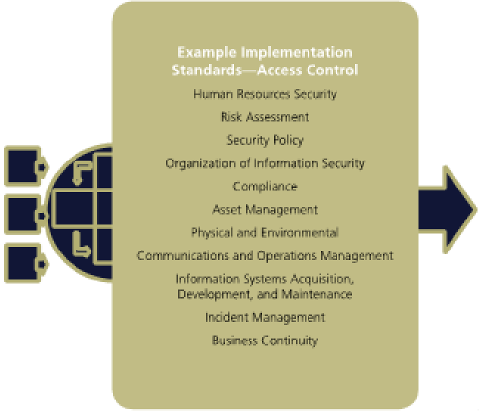


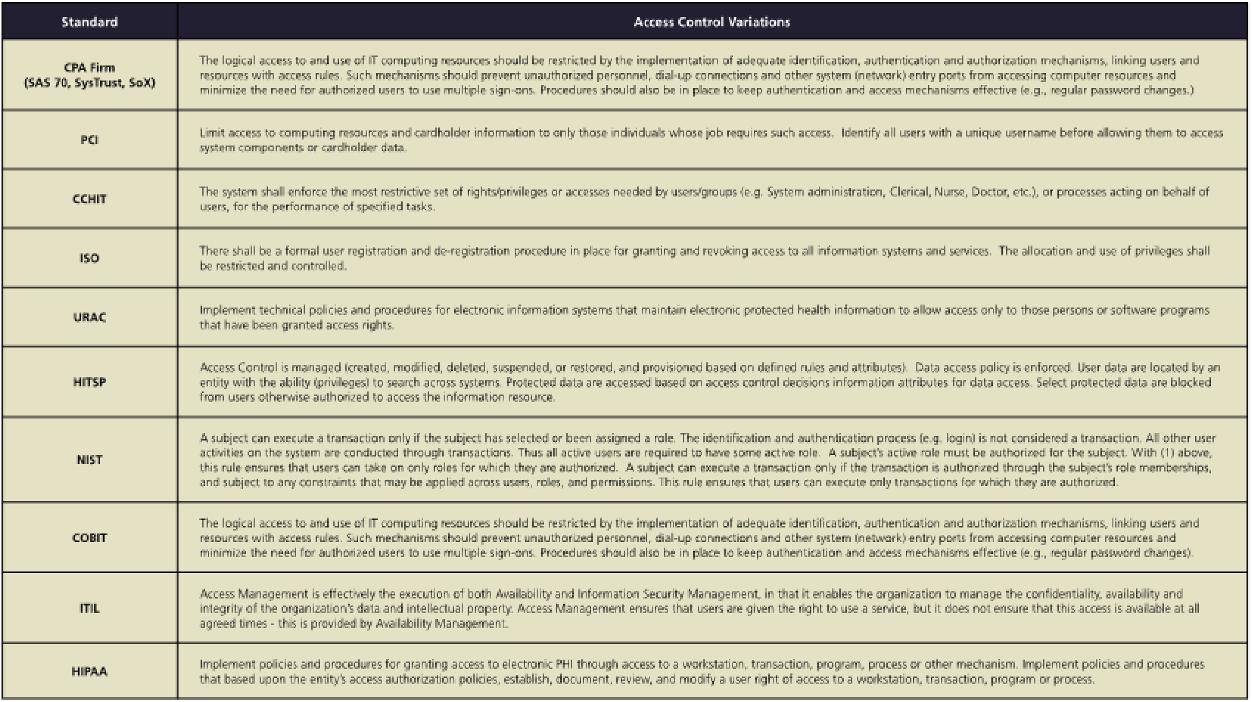
- Supported by threat intelligence, key components or functions of a robust and comprehensive cybersecurity program include
  - Risk analysis (Identify)
  - Control selection, implementation and maintenance (Protect)
  - Monitor and audit (Detect)
  - Incident management (Respond and Recover)
- Controls may be selected based on a traditional risk analysis, as described by NIST and DHHS, or selected & tailored from a control baseline contained in a suitable framework
- An information security risk management framework provides a set of principles, tools and practices to help:
  - Ensure people, process and technology elements completely and comprehensively address risks consistent with their business objectives, including legislative, regulatory and best practice requirements
  - Identify risks from the use of information by the organization’s business units and facilitate the avoidance, transfer, reduction or acceptance of risk
  - Support policy definition, enforcement, measurement, monitoring and reporting for each component of the security program are adequately addressed

Federal Guidance for Improving Cybersecurity

- The NIST Framework for Critical Infrastructure Cybersecurity provides an overarching set of guidelines to critical infrastructure industries to provide a minimal level of consistency as well as depth, breadth and rigor
  - Complements rather than replaces an organization's existing business or cybersecurity risk management process and cybersecurity program
  - Organizations can leverage the NIST CsF to identify opportunities to improve management processes for cybersecurity risk, or if no cybersecurity program exists, use the it as a reference to establish one
- The NIST CsF provides critical infrastructure industries:
  - A "Framework Core" set of cybersecurity activities, outcomes and references
  - A model for the evaluation of an organization's maturity or readiness using "Framework Implementation Tiers"
  - A common taxonomy and mechanism to:
    - Describe their current and target cybersecurity posture using a "Framework Profile"
    - Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
    - Assess progress toward the target state
    - Communicate among internal and external stakeholders about cybersecurity risk

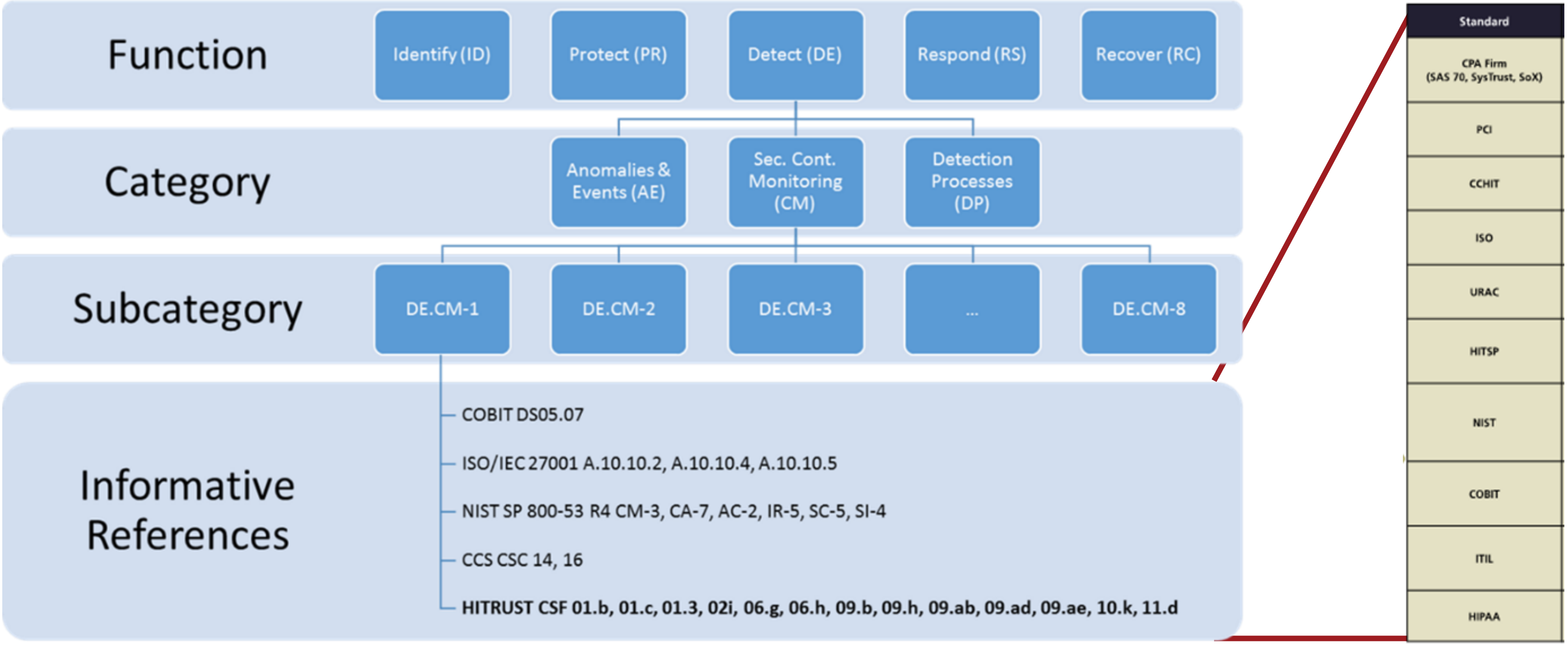
Multitude of Standards & Regulations to Choose


Example Implementation Standards—Access Control
Human Resources Security
Risk Assessment
Security Policy
Organization of Information Security
Compliance
Asset Management
Physical and Environmental
Communications and Operations Management
Information Systems Acquisition, Development, and Maintenance
Incident Management
Business Continuity



Standard	Access Control Variations
CPA Firm (SAS 70, SysTrust, SoX)	The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication and authorization mechanisms, linking users and resources with access rules. Such mechanisms should prevent unauthorized personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimize the need for authorized users to use multiple sign-ons. Procedures should also be in place to keep authentication and access mechanisms effective (e.g., regular password changes.)
PCI	Limit access to computing resources and cardholder information to only those individuals whose job requires such access. Identify all users with a unique username before allowing them to access system components or cardholder data.
CCHIT	The system shall enforce the most restrictive set of rights/privileges or accesses needed by users/groups (e.g. System administration, Clerical, Nurse, Doctor, etc.), or processes acting on behalf of users, for the performance of specified tasks.
ISO	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. The allocation and use of privileges shall be restricted and controlled.
URAC	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.
HITSP	Access Control is managed (created, modified, deleted, suspended, or restored, and provisioned based on defined rules and attributes). Data access policy is enforced. User data are located by an entity with the ability (privileges) to search across systems. Protected data are accessed based on access control decisions information attributes for data access. Select protected data are blocked from users otherwise authorized to access the information resource.
NIST	A subject can execute a transaction only if the subject has selected or been assigned a role. The identification and authentication process (e.g. login) is not considered a transaction. All other user activities on the system are conducted through transactions. Thus all active users are required to have some active role. A subject's active role must be authorized for the subject. With (1) above, this rule ensures that users can take on only roles for which they are authorized. A subject can execute a transaction only if the transaction is authorized through the subject's role memberships, and subject to any constraints that may be applied across users, roles, and permissions. This rule ensures that users can execute only transactions for which they are authorized.
COBIT	The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication and authorization mechanisms, linking users and resources with access rules. Such mechanisms should prevent unauthorized personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimize the need for authorized users to use multiple sign-ons. Procedures should also be in place to keep authentication and access mechanisms effective (e.g., regular password changes).
ITIL	Access Management is effectively the execution of both Availability and Information Security Management, in that it enables the organization to manage the confidentiality, availability and integrity of the organization's data and intellectual property. Access Management ensures that users are given the right to use a service, but it does not ensure that this access is available at all agreed times - this is provided by Availability Management.
HIPAA	Implement policies and procedures for granting access to electronic PHI through access to a workstation, transaction, program, process or other mechanism. Implement policies and procedures that based upon the entity's access authorization policies, establish, document, review, and modify a user right of access to a workstation, transaction, program or process.

NIST Cybersecurity Framework (CsF)



Function

Identify (ID)

Protect (PR)

Detect (DE)

Respond (RS)

Recover (RC)

Category

Anomalies & Events (AE)

Sec. Cont. Monitoring (CM)

Detection Processes (DP)

Subcategory

DE.CM-1

DE.CM-2

DE.CM-3

...

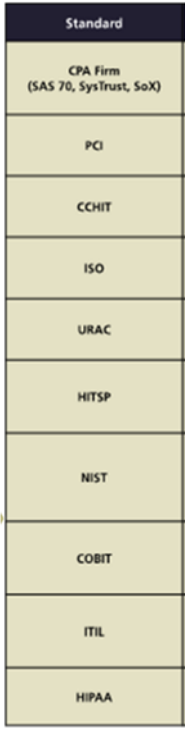
DE.CM-8

Informative References

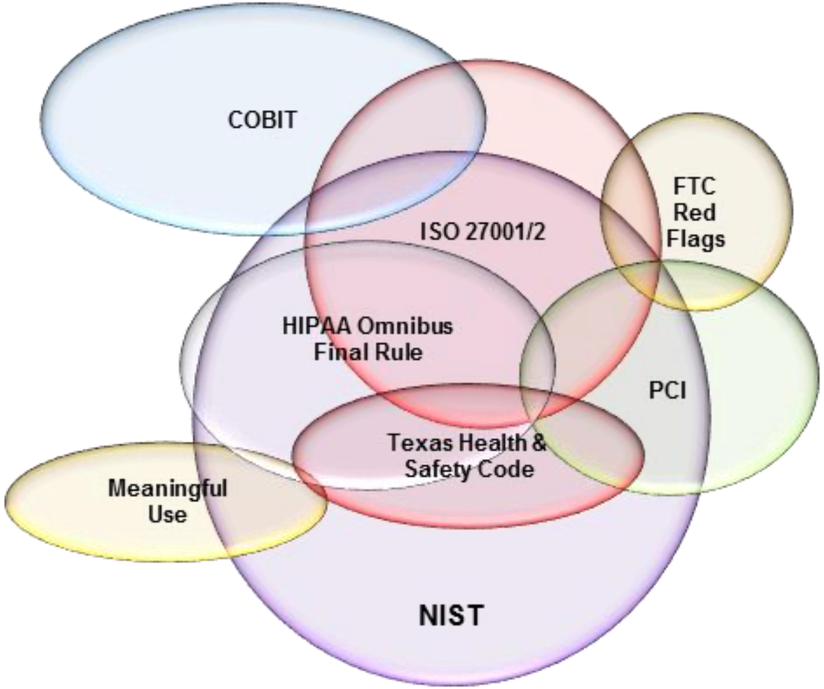
- COBIT DS05.07
- ISO/IEC 27001 A.10.10.2, A.10.10.4, A.10.10.5
- NIST SP 800-53 R4 CM-3, CA-7, AC-2, IR-5, SC-5, SI-4
- CCS CSC 14, 16
- **HITRUST CSF 01.b, 01.c, 01.3, 02i, 06.g, 06.h, 09.b, 09.h, 09.ab, 09.ad, 09.ae, 10.k, 11.d**

Standard
CPA Firm (SAS 70, SysTrust, SoX)
PCI
CCHIT
ISO
URAC
HITSP
NIST
COBIT
ITIL
HIPAA

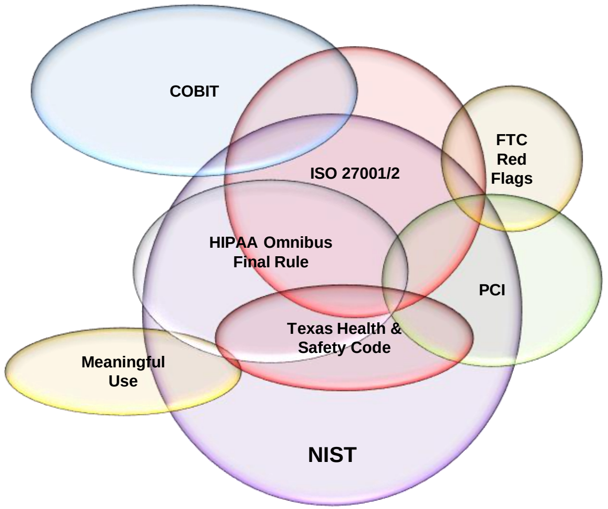
Multiple Requirements (1)



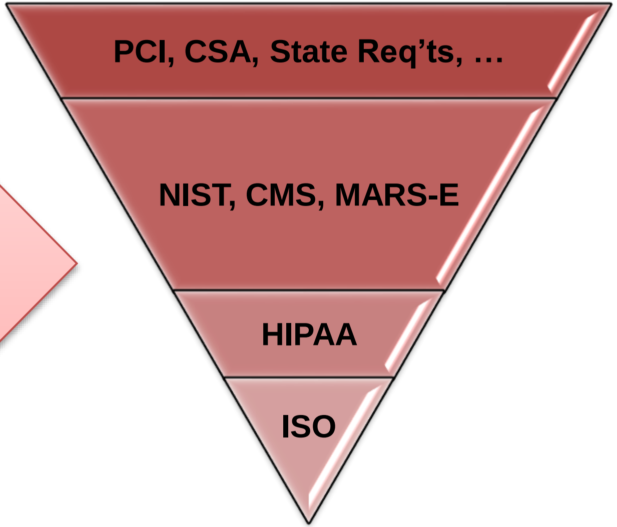
Standard
CPA Firm (SAS 70, SysTrust, SoX)
PCI
CCHIT
ISO
URAC
HITSP
NIST
COBIT
ITIL
HIPAA



Multiple Requirements (2)



Initial “high-level” ISO content reinforced with additional, often more prescriptive language from relevant authoritative sources, harmonized, and fully integrated into the CSF



One Program (1)

The HITRUST CSF provides coverage across multiple healthcare specific standards and includes significant components from other well-respected IT security standards bodies and governance sources

Included Standards

HIPAA Security, Data Breach Notification, & Privacy
ISO/IEC 27001:2005 2013, 27002:2005, 2013, 27799:2008
CFR Part 11
COBIT 4.1
NIST SP 800-53 Revision 4
NIST Cybersecurity Framework (CsF)

NIST SP 800-66
PCI DSS version 3
FTC Red Flags Rule
JCAHO IM
201 CMR 17.00 (State of Mass.)
NRS 603A (State of Nev.)

CSA Cloud Controls Matrix version 1.1
CMS IS ARS version 2
Texas Health and Safety Code (THSC) 181
Title 1 Texas Administrative Code (TAC) 390.2
MARS-E version 1
IRS Pub 1075 (2014)

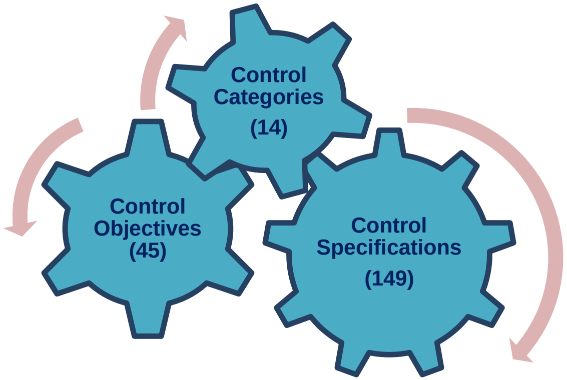
Analyzed, Rationalized & Consolidated

Scoping Factors

Regulatory
- Federal, state and domain specific compliance requirements

Organization
- Geographic factors
- Number of covered lives

System
- Data stores
- External connections
- Number of users/transactions

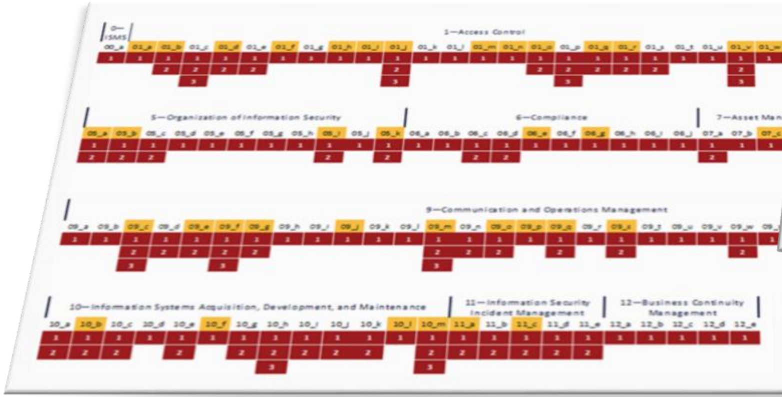


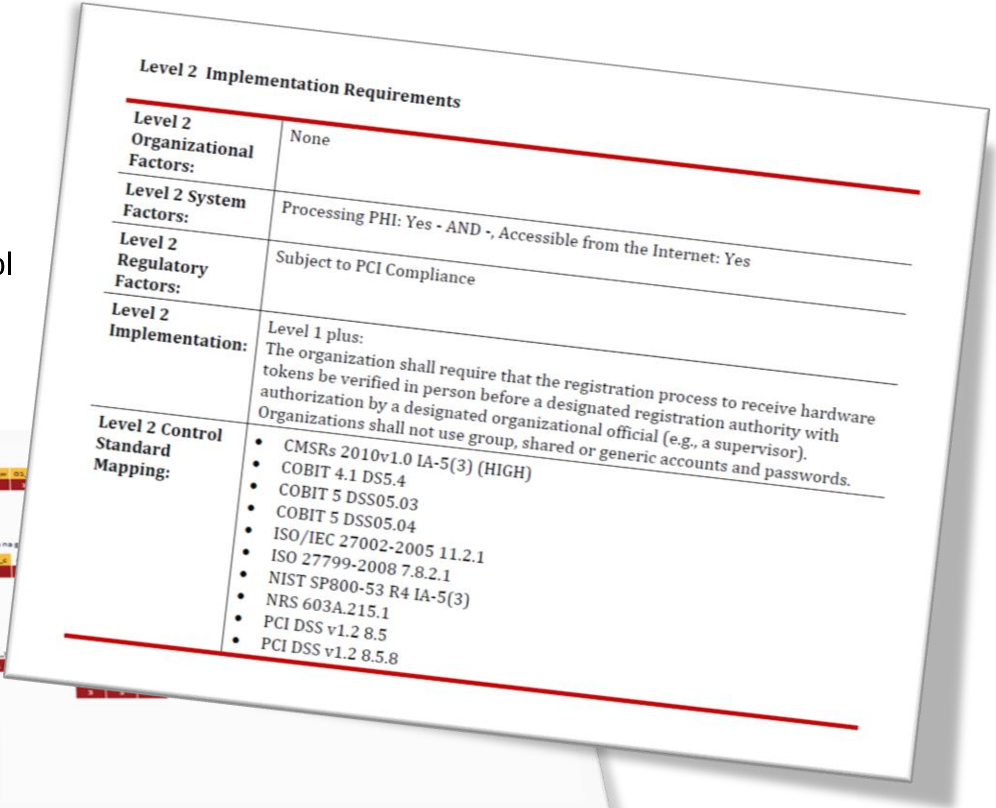
Control Categories

0. Information Security Management Program
1. Access Control
2. Human Resources Security
3. Risk Management
4. Security Policy
5. Organization of Information Security
6. Compliance
7. Asset Management
8. Physical and Environmental Security
9. Communications and Operations Management
10. Information Systems Acquisition, Development & Maintenance
11. Information Security Incident Management
12. Business Continuity Management
13. Privacy Practices

One Program (2)

- The CSF structure based on ISO 27001:2005
- Adds additional CSF Categories 0.0, 3.0 and 13.0
- 149 Controls, with up to three (3) levels per Control
- **Multiple authoritative sources mapped to each Control by implementation level**

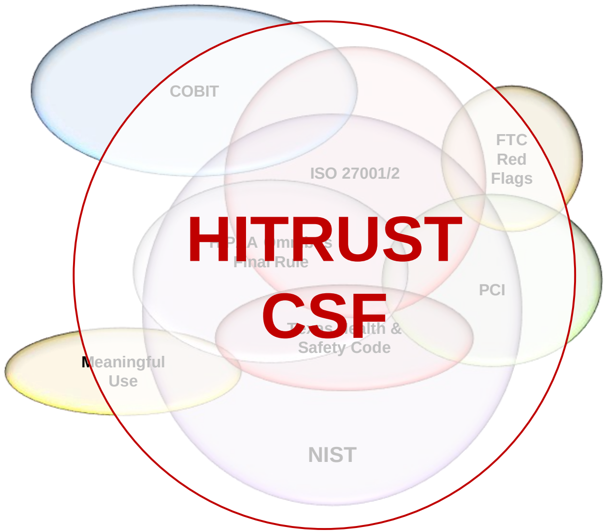

0—ISMS
1—Access Control
5—Organization of Information Security
6—Compliance
7—Asset Manag
9—Communication and Operations Management
10—Information Systems Acquisition, Development, and Maintenance
11—Information Security Incident Management
12—Business Continuity Management

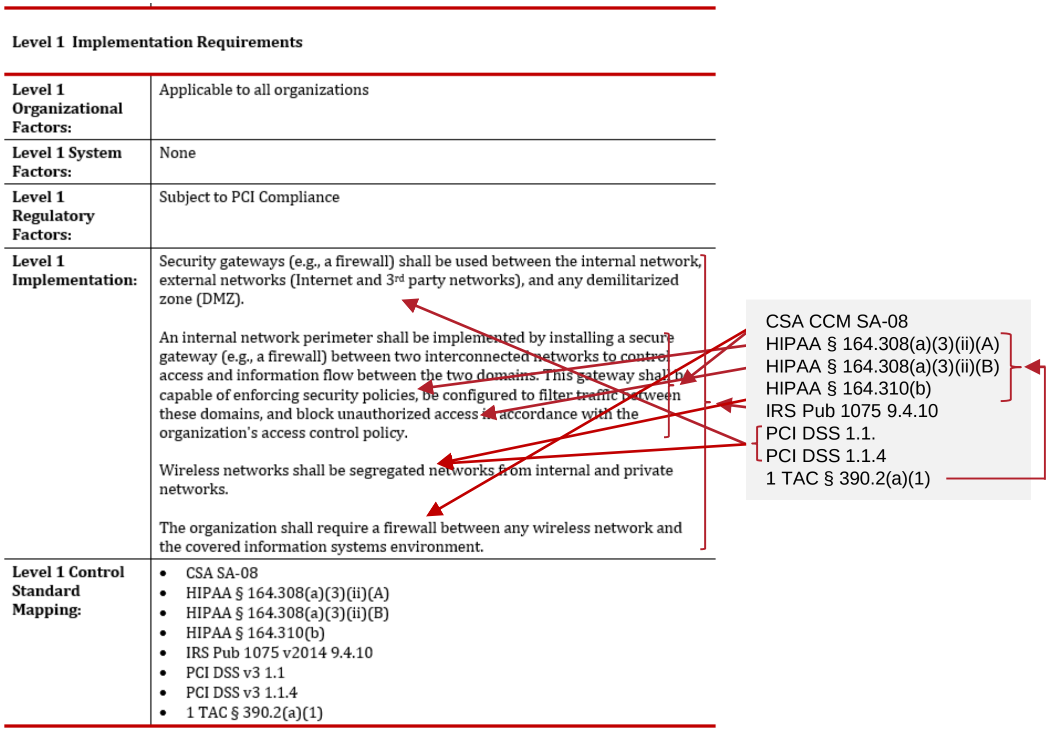


Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Accessible from the Internet: Yes
Level 2 Regulatory Factors:	Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: The organization shall require that the registration process to receive hardware tokens be verified in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor). Organizations shall not use group, shared or generic accounts and passwords.
Level 2 Control Standard Mapping:	• CMSRs 2010v1.0 IA-5(3) (HIGH) • COBIT 4.1 DS5.4 • COBIT 5 DSS05.03 • COBIT 5 DSS05.04 • ISO/IEC 27002-2005 11.2.1 • ISO 27799-2008 7.8.2.1 • NIST SP800-53 R4 IA-5(3) • NRS 603A.215.1 • PCI DSS v1.2 8.5 • PCI DSS v1.2 8.5.8

One Program (3)



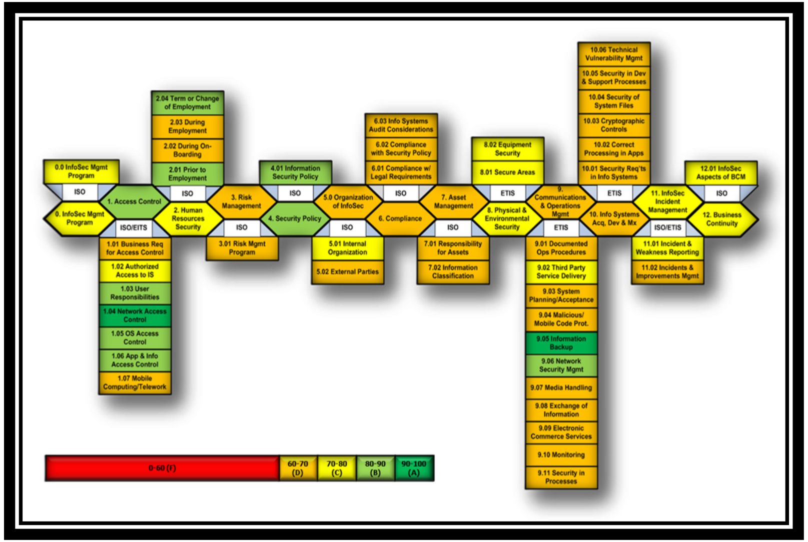


Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance
Level 1 Implementation:	Security gateways (e.g., a firewall) shall be used between the internal network, external networks (Internet and 3rd party networks), and any demilitarized zone (DMZ). An internal network perimeter shall be implemented by installing a secure gateway (e.g., a firewall) between two interconnected networks to control access and information flow between the two domains. This gateway shall be capable of enforcing security policies, be configured to filter traffic between these domains, and block unauthorized access in accordance with the organization's access control policy. Wireless networks shall be segregated networks from internal and private networks. The organization shall require a firewall between any wireless network and the covered information systems environment.
Level 1 Control Standard Mapping:	• CSA SA-08 • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.308(a)(3)(ii)(B) • HIPAA § 164.310(b) • IRS Pub 1075 v2014 9.4.10 • PCI DSS v3 1.1 • PCI DSS v3 1.1.4 • 1 TAC § 390.2(a)(1)

CSA CCM SA-08
HIPAA § 164.308(a)(3)(ii)(A)
HIPAA § 164.308(a)(3)(ii)(B)
HIPAA § 164.310(b)
IRS Pub 1075 9.4.10
PCI DSS 1.1.
PCI DSS 1.1.4
1 TAC § 390.2(a)(1)

Assess Once

Assessing against the CSF necessarily implies one is assessing against the multiple regulations, standards and best practice frameworks upon which it's built


0.0 InfoSec Mgmt Program
ISO
0. InfoSec Mgmt Program
1. Access Control
ISO/EITS
1.01 Business Req for Access Control
1.02 Authorized Access to IS
1.03 User Responsibilities
1.04 Network Access Control
1.05 OS Access Control
1.06 App & Info Access Control
1.07 Mobile Computing/Telework
2.04 Term or Change of Employment
2.03 During Employment
2.02 During On-Boarding
2.01 Prior to Employment
ISO
2. Human Resources Security
3. Risk Management
ISO
3.01 Risk Mgmt Program
4.01 Information Security Policy
ISO
4. Security Policy
5.0 Organization of InfoSec
ISO
5.01 Internal Organization
5.02 External Parties
6.03 Info Systems Audit Considerations
6.02 Compliance with Security Policy
6.01 Compliance w/ Legal Requirements
ISO
6. Compliance
7. Asset Management
ISO
7.01 Responsibility for Assets
7.02 Information Classification
8.02 Equipment Security
8.01 Secure Areas
ETIS
8. Physical & Environmental Security
9. Communications & Operations Mgmt
ETIS
9.01 Documented Ops Procedures
9.02 Third Party Service Delivery
9.03 System Planning/Acceptance
9.04 Malicious/ Mobile Code Prot.
9.05 Information Backup
9.06 Network Security Mgmt
9.07 Media Handling
9.08 Exchange of Information
9.09 Electronic Commerce Services
9.10 Monitoring
9.11 Security in Processes
10.06 Technical Vulnerability Mgmt
10.05 Security in Dev & Support Processes
10.04 Security of System Files
10.03 Cryptographic Controls
10.02 Correct Processing in Apps
10.01 Security Req'ts in Info Systems
ETIS
10. Info Systems Acq, Dev & Mx
11. InfoSec Incident Management
ISO/ETIS
11.01 Incident & Weakness Reporting
11.02 Incidents & Improvements Mgmt
12.01 InfoSec Aspects of BCM
ISO
12. Business Continuity
0-60 (F)
60-70 (D)
70-80 (C)
80-90 (B)
90-100 (A)

The CSF's extensive mappings allow traceability from a CSF assessment to each of these multiple authoritative sources, which allows the control maturity and risk information from a single assessment to be parsed accordingly

Report Many

Standardized CSF-based reporting, e.g., CSF Certification

Custom source-based reporting

- Roll up control maturity or risk based on authoritative sources
- Produce source-specific scorecards
  - e.g., HIPAA, NIST CsF
- Support or produce source-specific reports
  - e.g., NIST SSP, PCI SAQ, SecureTexas, SSAE 16 SOC 2 (Trust Principles)

HITRUST Health Information Trust Alliance

05/11 NIST

NIST Cyber Security Framework Scorecard

Created On: 05/13/2015

Function	Category	Subcategory		
IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-1: Physical devices and syster organization are inventoried		
		ID.AM-2: Software platforms and app the organization are inventoried		
		ID.AM-3: Organizational com flows are mapped		
		ID.AM-4: External informat		
		ID.AM-5: Resources (e.g., h software) are prioritized based criticality, and business value		
		ID.AM-6: Cybersecurity role the entire workforce and third suppliers, customers, partners		
	Business Environment (ID.BE)	ID.BE-1: The organization's identified and communicated		
		ID.BE-2: The organization's infrastructure and its industry communicated		
		ID.BE-3: Priorities for organ objectives, and activities are e communicated		
		ID.BE-4: Dependencies and delivery of critical services are		
		ID.BE-5: Resilience requirements to support delivery of critical services are established		
	Governance (ID.GV)	ID.GV-1: Organizational information security policy is established	🟩	Very Low
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	🟨	Low
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	🟥	Low

1

Created in MyCSF. © 2015 HITRUST, Frisco, TX. All Rights Reserved.

NIST Special Publication 800-18 Revision 1

Guide for Developing Security Plans for Federal Information Systems

Marianne Swanson
Joan Hash
Pauline Bowen

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

AICPA Service Organization Control Reports℠
AICPA
SOC
aicpa.org/soc
Formerly SAS 70 Reports

Payment Card Industry (PCI) Data Security Standard

Self-Assessment Questionnaire

PCI Security Standards Council™

SECURETexas

HEALTH INFORMATION PRIVACY & SECURITY CERTIFICATION

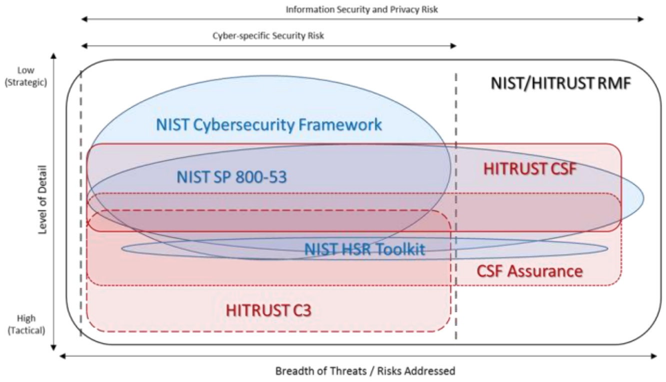
A Model Implementation of the NIST Framework

HITRUST CSF provides an implementation applicable to healthcare organizations leveraging the NIST Cybersecurity Framework

HITRUST provides an RMF that is consistent with the NIST Cybersecurity Framework for the healthcare industry and either meets or exceeds the requirements, addresses non-cyber threats, and incorporates a robust assurance program.

More specifically:

- NIST Cybersecurity Framework categorizes cybersecurity controls according to an incident response process (functions and sub-functions) as opposed to a traditional RMF
- HITRUST CSF provides an integrated, harmonized set of requirements specific to healthcare as compared to individual references to controls in NIST and other frameworks
- HITRUST CSF Assurance Program provides a standardized evaluation & reporting approach fully supported by an integrated maturity model
- HITRUST CSF Assurance Program provides a pool of vetted assessor organizations and centralized quality assurance processes to ensure consistent and repeatable assessments


Information Security and Privacy Risk
Cyber-specific Security Risk
Low (Strategic)
Level of Detail
High (Tactical)
NIST/HITRUST RMF
NIST Cybersecurity Framework
NIST SP 800-53
HITRUST CSF
NIST HSR Toolkit
CSF Assurance
HITRUST C3
Breadth of Threats / Risks Addressed

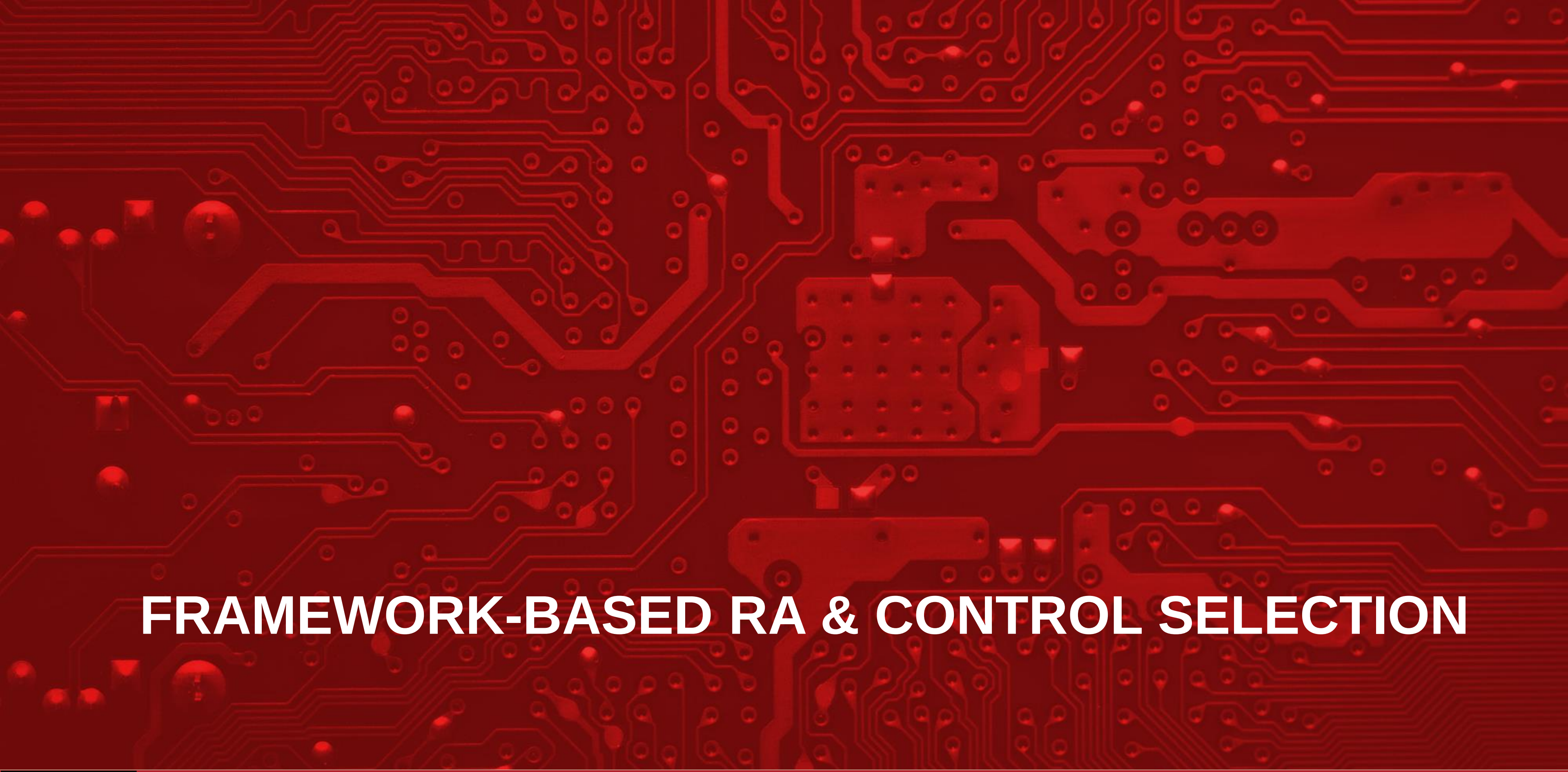
Key Comparison with Other Frameworks

The CSF is specific to, built and maintained by, and simply better for the healthcare industry.

Requirement	CSF	COBIT	PCI	ISO	NIST	HIPAA
Comprehensive – general security	Yes	Yes	Yes	Yes	Yes	Partial
Comprehensive – regulatory, statutory, and business requirements	Yes	No	No	No	No	No
Prescriptive	Yes	No	Yes	Partial	Yes	No
Risk-based (rather than compliance-based)	Yes	Yes	Partial	Yes	Yes	Partial
Practical and scalable	Yes	Yes	No	No	No	Yes
Supported and maintained	Yes	Yes	Yes	Yes	Yes	No
Vetted by healthcare and industry experts	Yes	No	No	Yes**	Yes**	No
Open and transparent update process	Yes	No	Yes	Yes	Yes	Yes
Audit or assessment guidelines	Yes	Yes	Yes	Yes	Yes	No
Consistency and accuracy (in assessment/evaluation)	Yes	Partial	Partial	Partial	Yes	No
Certifiable	Yes	Yes	Yes	Yes	No*	No
Assess once and report many	Yes	No	No	Partial	Partial	No
Support for third-party assurance	Yes	Yes	Yes	Yes	No	No

*NIST controls are typically certified by a specific information system or type of system rather than at the organizational-level

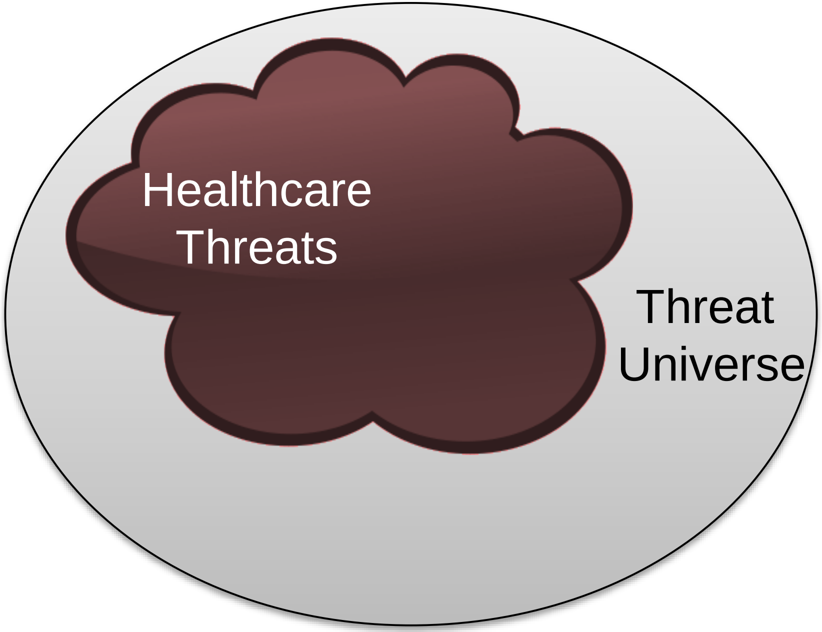
** ISO 27799 and NIST SP 800-66 both subject to comment period prior to release



FRAMEWORK-BASED RA & CONTROL SELECTION

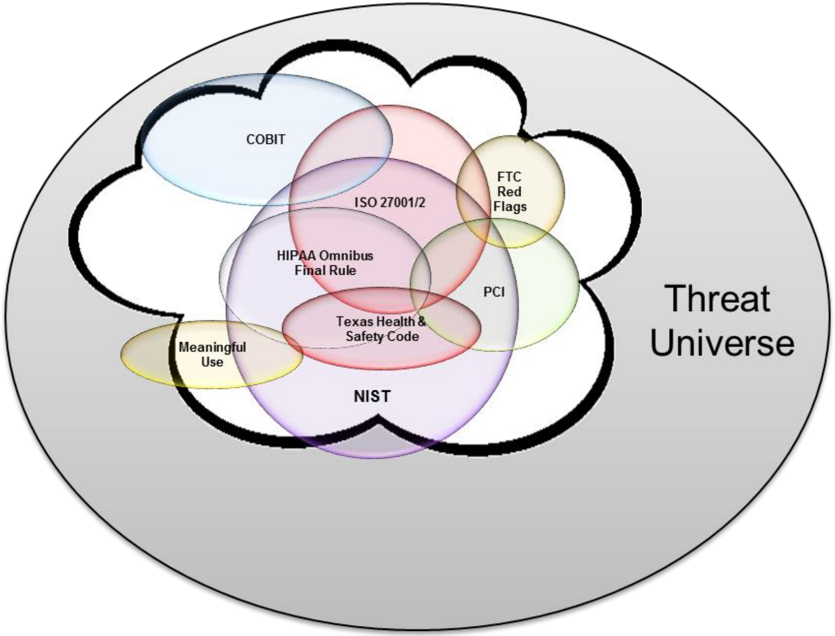
Framework-based Risk Analysis (1)

The threats are ever-changing but remain the same regardless of RA approach chosen.



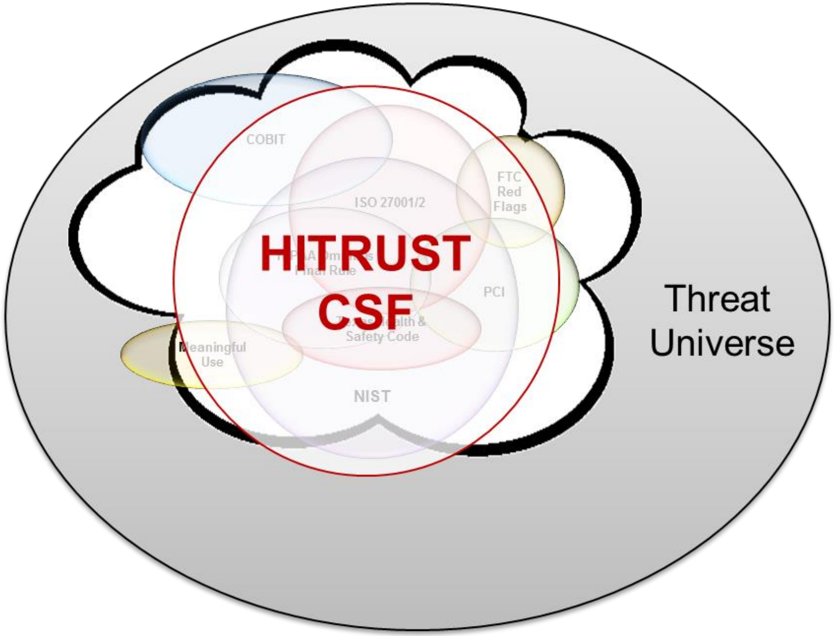
Framework-based Risk Analysis (2)

Leveraging the threat analyses of supporting control-based frameworks like ISO & NIST ...

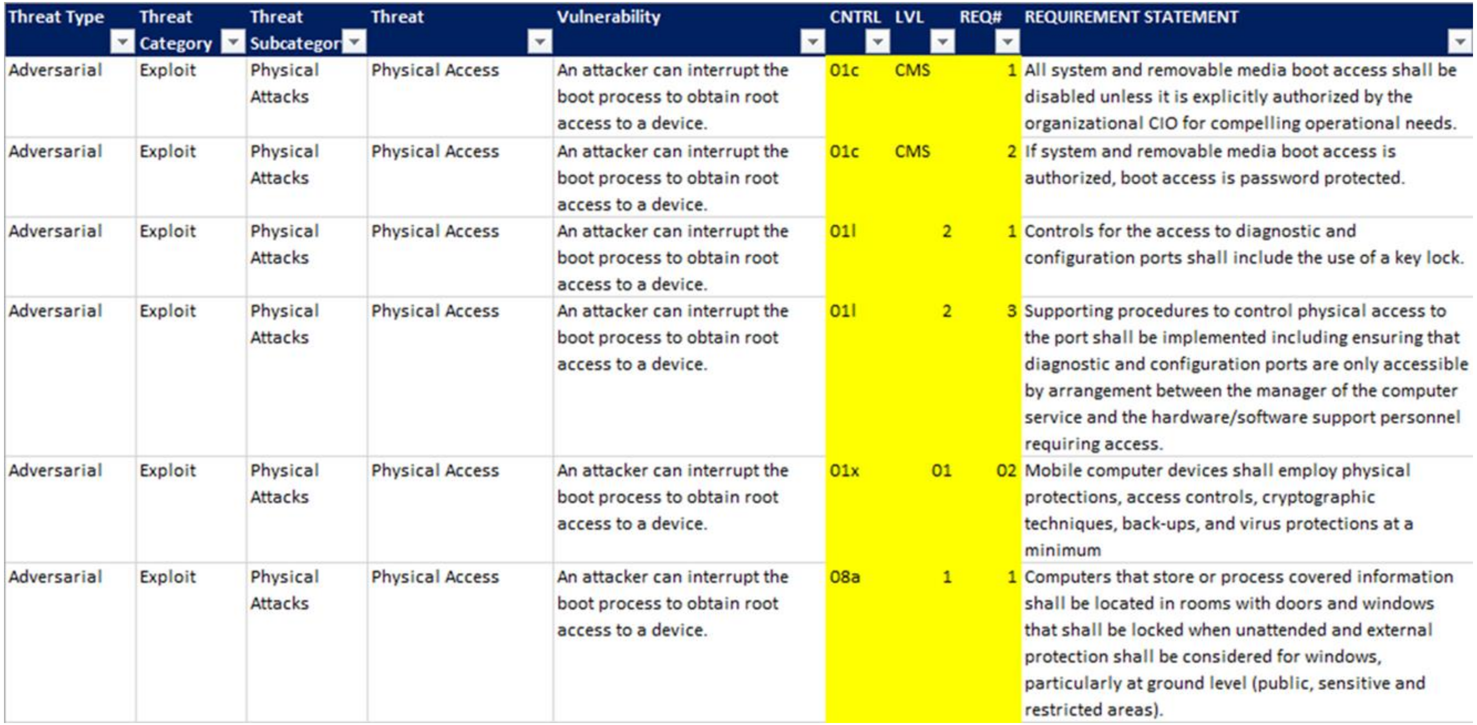


Framework-based Risk Analysis (3)

… and leveraging a comprehensive, control-based frameworks like HITRUST.



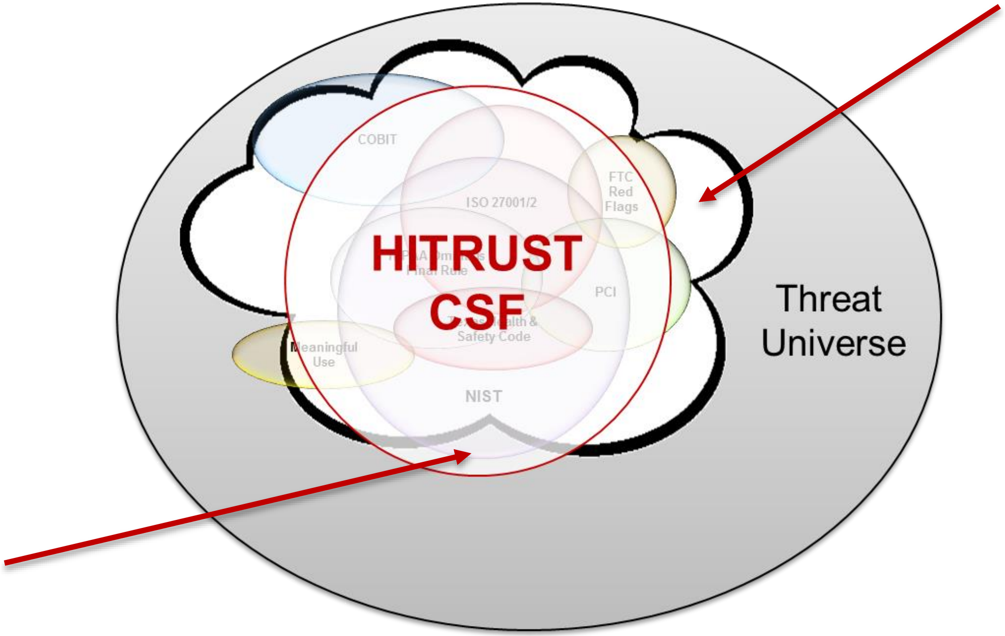
Framework-based Control Selection



Threat Type	Threat Category	Threat Subcategor	Threat	Vulnerability	CNTRL	LVL	REQ#	REQUIREMENT STATEMENT
Adversarial	Exploit	Physical Attacks	Physical Access	An attacker can interrupt the boot process to obtain root access to a device.	01c	CMS	1	All system and removable media boot access shall be disabled unless it is explicitly authorized by the organizational CIO for compelling operational needs.
Adversarial	Exploit	Physical Attacks	Physical Access	An attacker can interrupt the boot process to obtain root access to a device.	01c	CMS	2	If system and removable media boot access is authorized, boot access is password protected.
Adversarial	Exploit	Physical Attacks	Physical Access	An attacker can interrupt the boot process to obtain root access to a device.	01l	2	1	Controls for the access to diagnostic and configuration ports shall include the use of a key lock.
Adversarial	Exploit	Physical Attacks	Physical Access	An attacker can interrupt the boot process to obtain root access to a device.	01l	2	3	Supporting procedures to control physical access to the port shall be implemented including ensuring that diagnostic and configuration ports are only accessible by arrangement between the manager of the computer service and the hardware/software support personnel requiring access.
Adversarial	Exploit	Physical Attacks	Physical Access	An attacker can interrupt the boot process to obtain root access to a device.	01x	01	02	Mobile computer devices shall employ physical protections, access controls, cryptographic techniques, back-ups, and virus protections at a minimum
Adversarial	Exploit	Physical Attacks	Physical Access	An attacker can interrupt the boot process to obtain root access to a device.	08a	1	1	Computers that store or process covered information shall be located in rooms with doors and windows that shall be locked when unattended and external protection shall be considered for windows, particularly at ground level (public, sensitive and restricted areas).

Tailoring the Control Selection (1)

Additional Tailoring Required



Additional Tailoring Required

Tailoring the Control Selection (2)

- Focus on risk(s) unique to the organization wrt the criteria for the selected baseline
  - Threat(s), vulnerability(ies), impact(s)
- Identify gap(s) in the protections specified / risks managed by the baseline controls
- Select/design additional controls/enhancements as needed
  - May also eliminate controls as N/A or formally accept additional risk
- Example
  - Threat: Pharma actively targeted for industrial espionage
  - Vulnerability: Employees not able to recognize social engineering
  - Add'l control: The organization includes practical exercises in security awareness training that simulate actual cyber attacks (CSF Control 02.e; Cross reference NIST SP 800-53 R4, AT-2(1))
- For more information on the tailoring process, refer to NIST SP 800-53 r4

Risk Analysis/Assessment Process (Modified)

Leveraging a control-based risk management framework in the RA process

- Conduct a complete inventory of where health information ‘lives’
- Perform a BIA on all systems with health information (criticality)
- Categorize & valuate systems based on sensitivity & criticality
- **Select an appropriate framework baseline set of controls**
- **Apply an overlay and/or tailor based on a targeted risk analysis**
- Evaluate residual risk using control maturity & impact ratings
- Rank risks and determine risk treatments
- Make contextual adjustments to likelihood & impact, if needed, as part of the corrective action planning process

Necessary Due Diligence & Due Care (1)

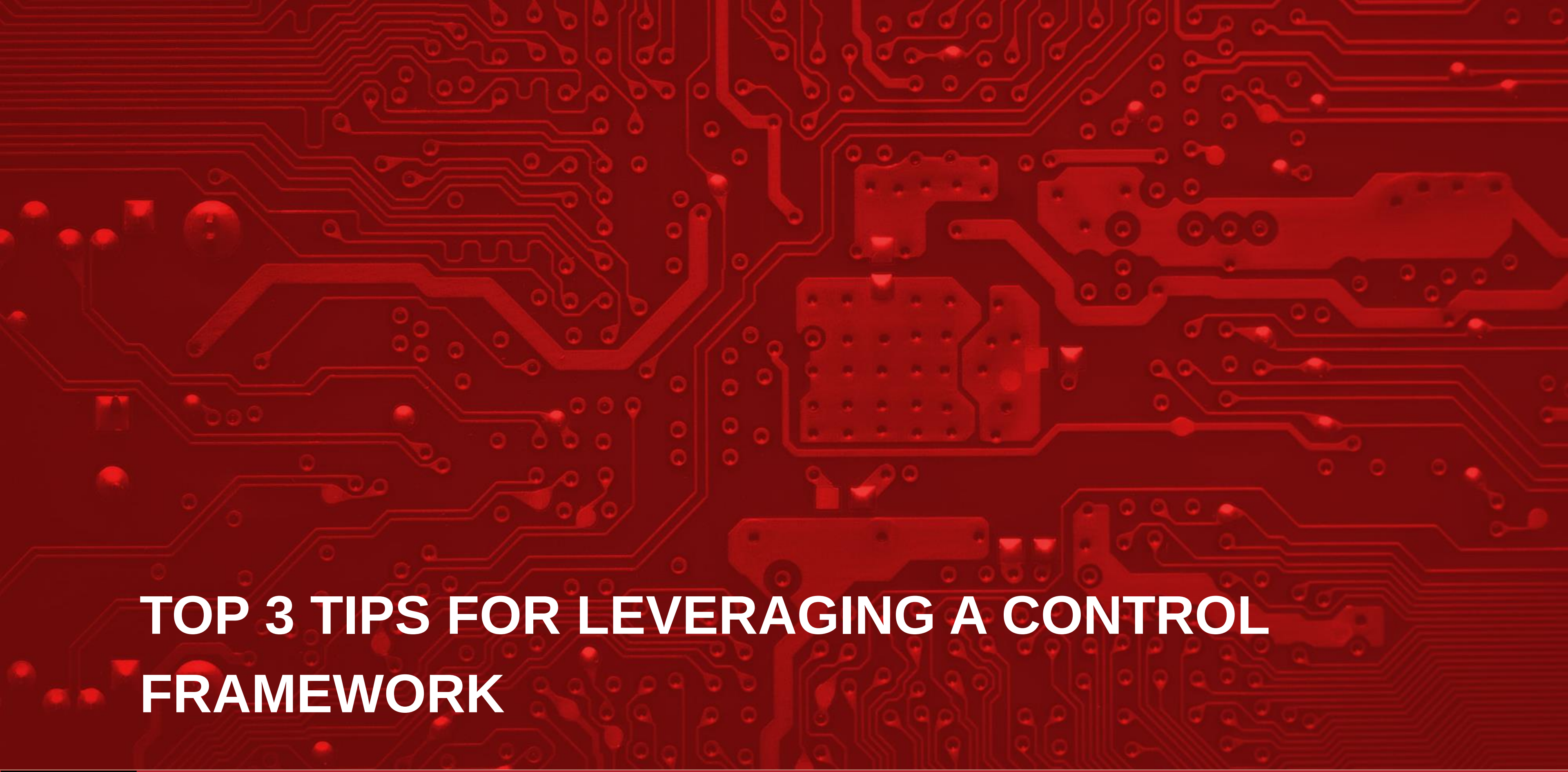
- 45 CFR § 164.308(a)(1)
  - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the [CIA] of [ePHI] held by the covered entity or BA
- 45 CFR § 164.306(a)
  - (1) Ensure the [CIA] of all [ePHI] the covered entity or BA creates, receives, maintains or transmits
  - (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information

Necessary Due Diligence & Due Care (2)

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

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

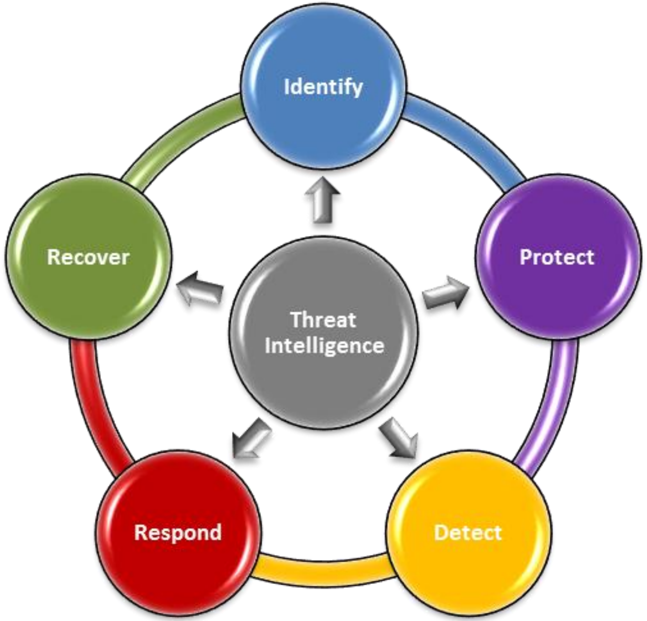
- Integrated risk management frameworks help provide a standard of due care & due diligence for the management of information-related risk
  - Harmonized set of information protection safeguards
  - Baselines determined based on organizational risk
  - Additional RA used at multiple points in the risk management process
    - Initial / baseline control selection (baseline tailoring)
    - Alternate control analysis
    - Remediation planning



TOP 3 TIPS FOR LEVERAGING A CONTROL FRAMEWORK

Top 3 Tips for Leveraging a RM Framework

- Frameworks help define a minimum baseline of protection in the general case but may not address risks that are particular to a specific organization (Tailor, Tailor, Tailor!)
- Ensure the framework’s processes are integrated into normal operational and project processes such as project management, acquisition / supply chain, and change management
- Integrate routine threat intelligence into organizational risk management programs and update framework-based information protection requirements as needed



Dr. Bryan Cline, CISSP-ISSEP, CISM, CISA, CCSFP, HCISPP

Senior Advisor, HITRUST

✉ *Bryan.Cline@HITRUSTAlliance.net*

Q&A

HITRUST

Health Information Trust Alliance

Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Content Spotlight