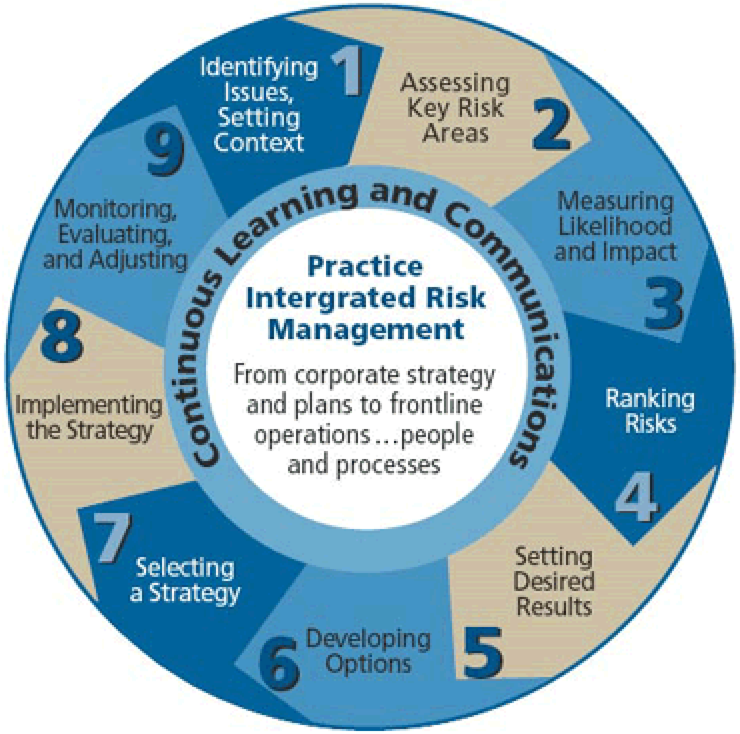
Cybersecurity for Meaningful Use


Identifying Issues, Setting Context
1
Assessing Key Risk Areas
2
Measuring Likelihood and Impact
3
Ranking Risks
4
Setting Desired Results
5
Developing Options
6
Selecting a Strategy
7
Implementing the Strategy
8
Monitoring, Evaluating, and Adjusting
9
Continuous Learning and Communications
Practice Intergrated Risk Management
From corporate strategy and plans to frontline operations…people and processes

2013 FRHA Annual Summit

"Setting the Health Care Table: Politics, Economics, Health"

November 20-22, 2013

Healthcare Sector Vulnerable to Hackers

The Washington Post

By Robert O’Harrow Jr., Published: December 25, 2012

The American Recovery and Reinvestment Act mandated the widespread adoption of electronic health records (EHR) computer systems.

- Tens of thousands of doctors and hospitals are using the systems to digitize and share millions of patients’ records.
- Certification of the EHR systems included few security provisions.
- Health care has a culture in which physicians, nurses and other health-care workers sidestep basic security measures, such as passwords, in favor of convenience.

Healthcare Sector Vulnerable to Hackers

- Health care is among the most vulnerable industries in the country, and it lags behind in addressing known problems.
- Health care facilities show a routine failure to fix known software flaws in aging technology
- Medical devices at Veterans Affairs facilities were infected by malicious viruses at least 181 times from 2009 to 2011.
- 94% of hospitals had at least one breach in the last two years. (Ponemon Institute, 2012)
- 54% of health care firms have little confidence that they can detect all data loss or theft. (Ponemon Institute, 2012)
- The Department of Homeland Security concludes that health care presents an inviting target to activist hackers, cyberwarriors, criminals and terrorists.

The Downside of Heath IT Promotion

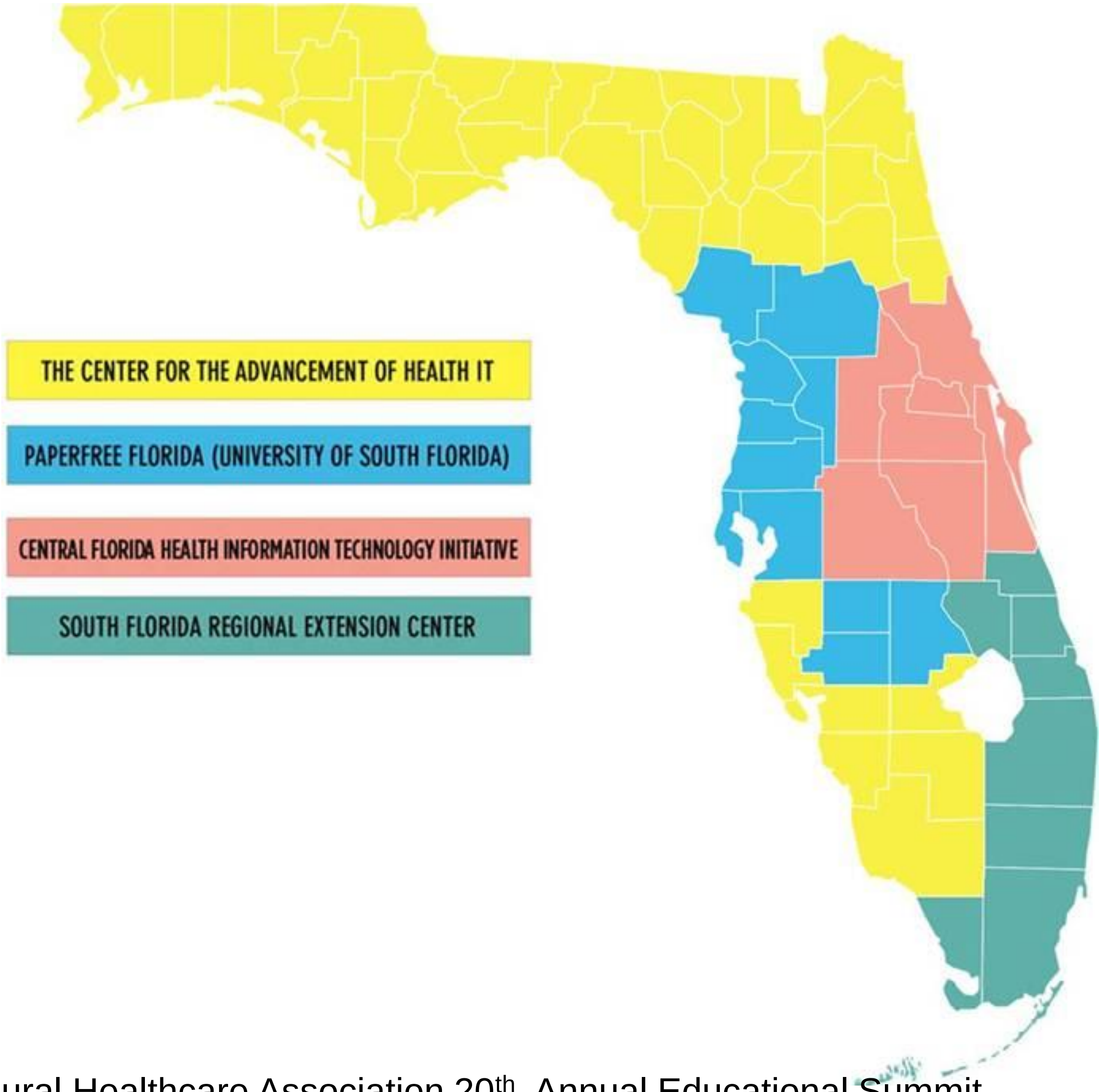
American Recovery and Reinvestment Act took some very positive steps toward promoting the adoption of health IT for improved patient care. Some of the important initiatives sponsored by the federal government include:

- CMS Incentive payments for providers to implement Electronic Health Records.
- ONC investment in state-level Health Information Exchange.
- FCC programs supporting broadband telecommunications.

There are correlated realities that have followed these initiatives:

- Increasing Cybercrime
- Increased HIPAA penalties for data breach

Regional Extension Centers in Florida


THE CENTER FOR THE ADVANCEMENT OF HEALTH IT
PAPERFREE FLORIDA (UNIVERSITY OF SOUTH FLORIDA)
CENTRAL FLORIDA HEALTH INFORMATION TECHNOLOGY INITIATIVE
SOUTH FLORIDA REGIONAL EXTENSION CENTER

Florida Providers Implementing EHRs

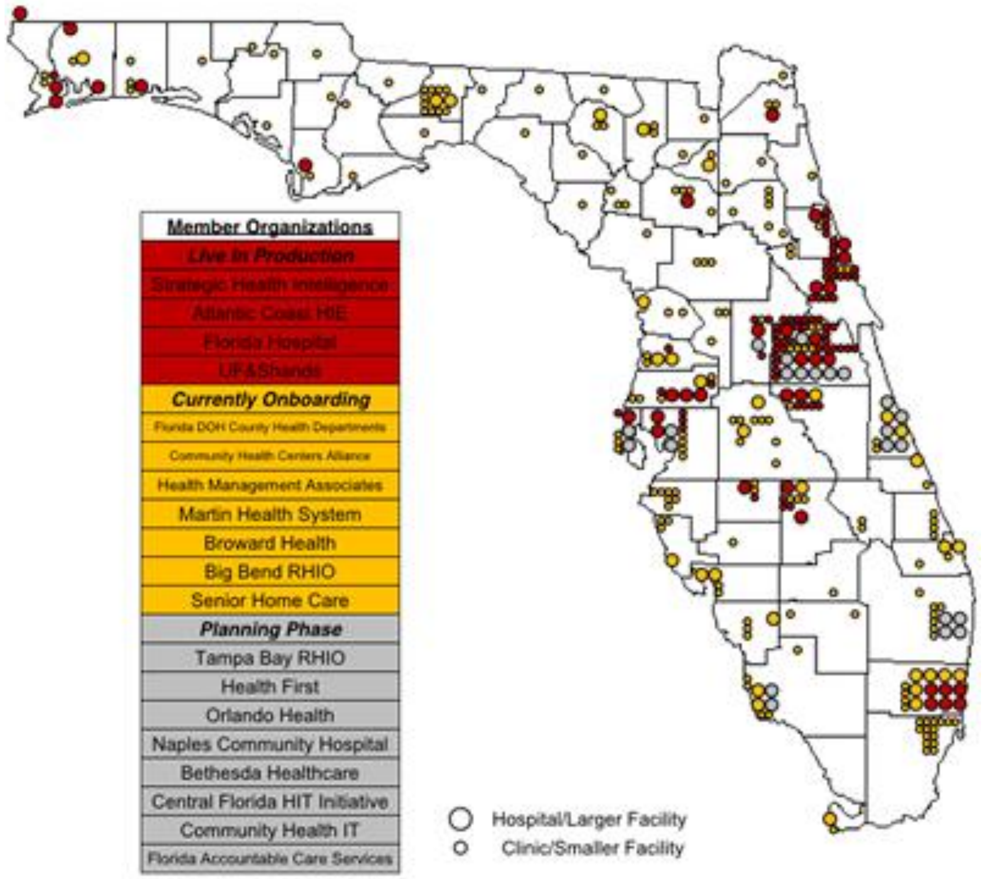
-	ONC Milestone 1: Membership in REC		ONC Milestone 2: Implement EHR		ONC Milestone 3: Attest to Meaningful Use	
Regional Extension Center	**PPCPs Signed w/ REC**	**% PPCPs Signed w/ REC**	**PPCPs w/ EHR**	**% PPCPs w/ EHR**	**PPCPs at Meaningful Use**	**% PPCPs at Meaningful Use**
Center for the Advancement of Health IT (FL)	2,413	119%	2,113	104%	1,156	57%
Central Florida HIT Initiative	1,514	111%	1,442	106%	906	66%
PaperFree Florida Collaborative IT Technology Regional Extension	1,793	179%	1,479	148%	837	84%
South Florida Regional Extension Center	3,190	128%	2,815	113%	1,824	73%
Total	8,910	134%	7,849	118%	1,743	70%

Health Information Exchange in Florida

FLORIDA HIE

plu patient look-up

Partner
Organization
Onboarding
Status through
May, 2013


Member Organizations
Live In Production
Strategic Health Intelligence
Atlantic Coast HIE
Florida Hospital
UF&Shands
Currently Onboarding
Florida DOH County Health Departments
Community Health Centers Alliance
Health Management Associates
Martin Health System
Broward Health
Big Bend RHIO
Senior Home Care
Planning Phase
Tampa Bay RHIO
Health First
Orlando Health
Naples Community Hospital
Bethesda Healthcare
Central Florida HIT Initiative
Community Health IT
Florida Accountable Care Services
○ Hospital/Larger Facility
○ Clinic/Smaller Facility

AHCA

HARRIS

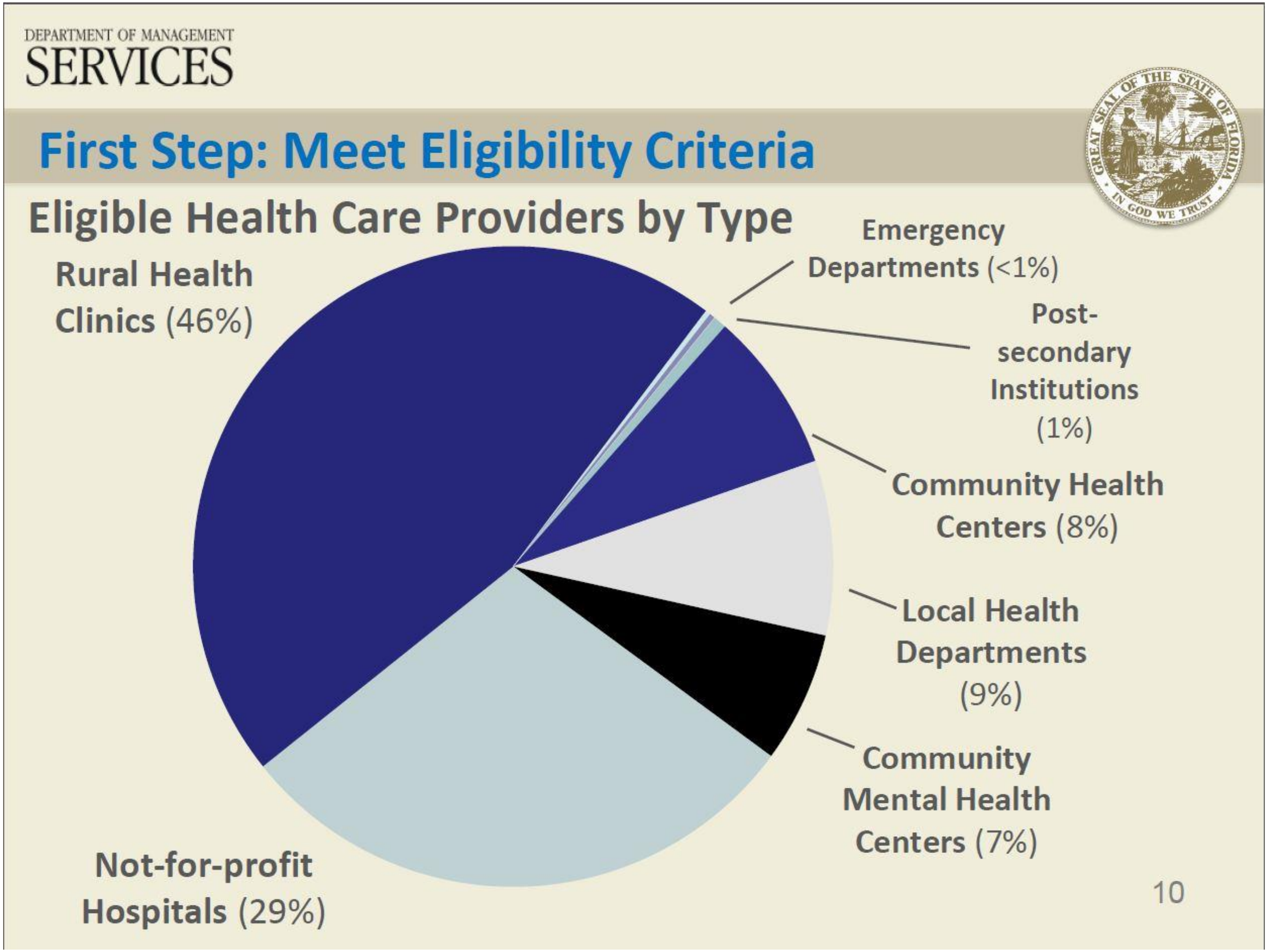
FCC CONNECT Rural Broadband Program

The Rural Broadband Program seeks to increase access to broadband telecommunications networks by rural health care providers.

The FCC will subsidize 65% of the cost of broadband telecommunications connections for rural health care providers out of the FCC CONNECT Fund.

- Equipment necessary to make broadband service functional.
- Reasonable and Customary Installation Charges.
- Lease of lit fiber and recurring charges.
- Connections to research & education networks.
- Connections between off-site data centers and administrative offices.

Eligible Providers for the FCC CONNECT Fund



DEPARTMENT OF MANAGEMENT
SERVICES

First Step: Meet Eligibility Criteria

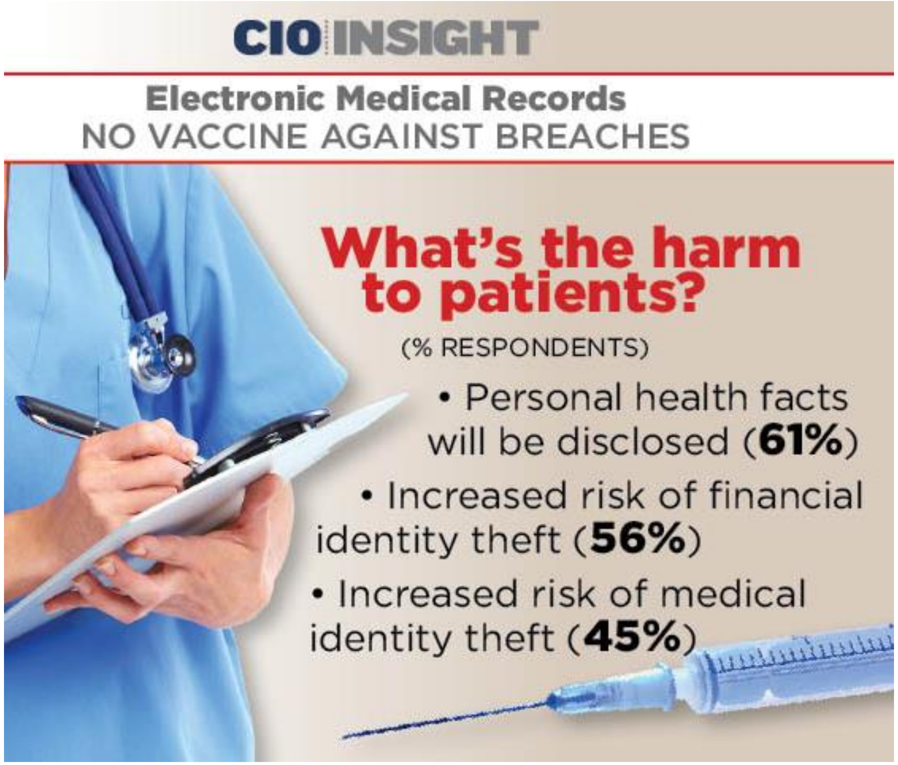
Eligible Health Care Providers by Type

Medical Identity Threat

Medical identity theft is increasing and consumers need to take steps to protect their personal information.

In 2012 an estimated 1.84 million Americans became victims of medical identity theft.

- This is an increase of 19% over the 2011 estimate of 1.52 million individuals.
- Medical identity theft can put victims' lives at risk.
- 50% of victims were not aware that medical identity theft can create inaccuracies in their permanent medical records.



CIO INSIGHT

Electronic Medical Records
NO VACCINE AGAINST BREACHES

What's the harm to patients?

(% RESPONDENTS)

- Personal health facts will be disclosed (**61%**)
- Increased risk of financial identity theft (**56%**)
- Increased risk of medical identity theft (**45%**)

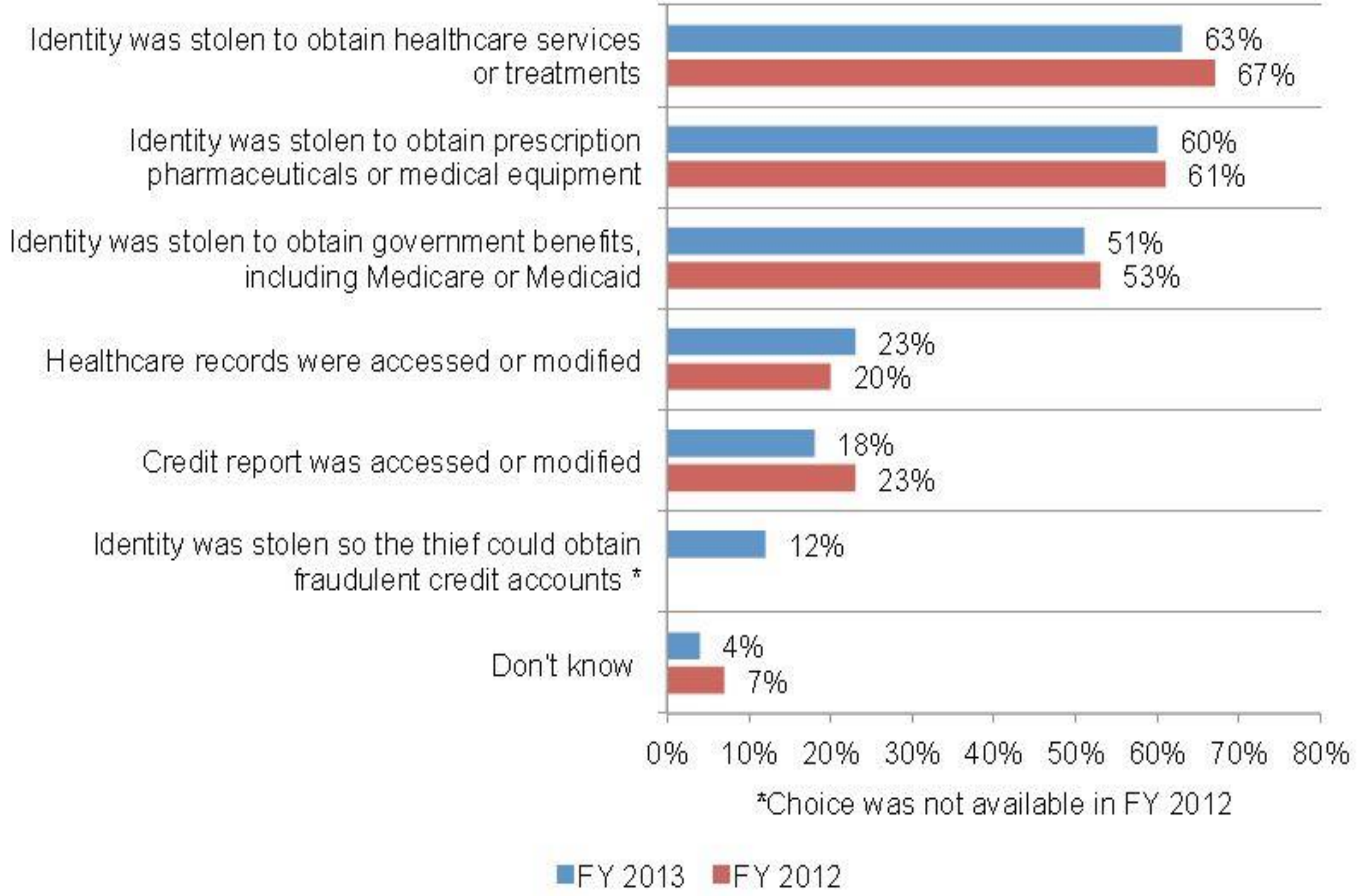
Who is Attacking You and Why?

The threat landscape in health care is similar to that seen in other industries.

- The majority of attackers seek information from which they can directly or indirectly profit. This includes personal details and payment card information.

- Organized criminal groups are behind 92% of breaches
- The majority of attacks on healthcare organizations come from outside of the company.
- Only one fifth of healthcare attacks come from an insider.
- Attackers often use the most basic hacking and malware techniques to break in.

Objectives of Medical Identity Theft



Breach of Unsecured PHI

The HIPAA Omnibus Final Rule issued in January 2013 takes a hard line on the of unsecured Protected Health Information.

- A ‘‘breach’’ of PHI is the unauthorized acquisition, access, use, or disclosure of unsecured PHI that compromises the security or privacy of the PHI.
- “Unsecured” PHI are records that are not rendered unusable, unreadable, or indecipherable to unauthorized individuals using the technology or a methodology specified by HHS guidance.
- The breach is considered to compromise the security of the PHI when there is a significant risk of financial, reputational, or some other harm to the individual whose PHI is taken.

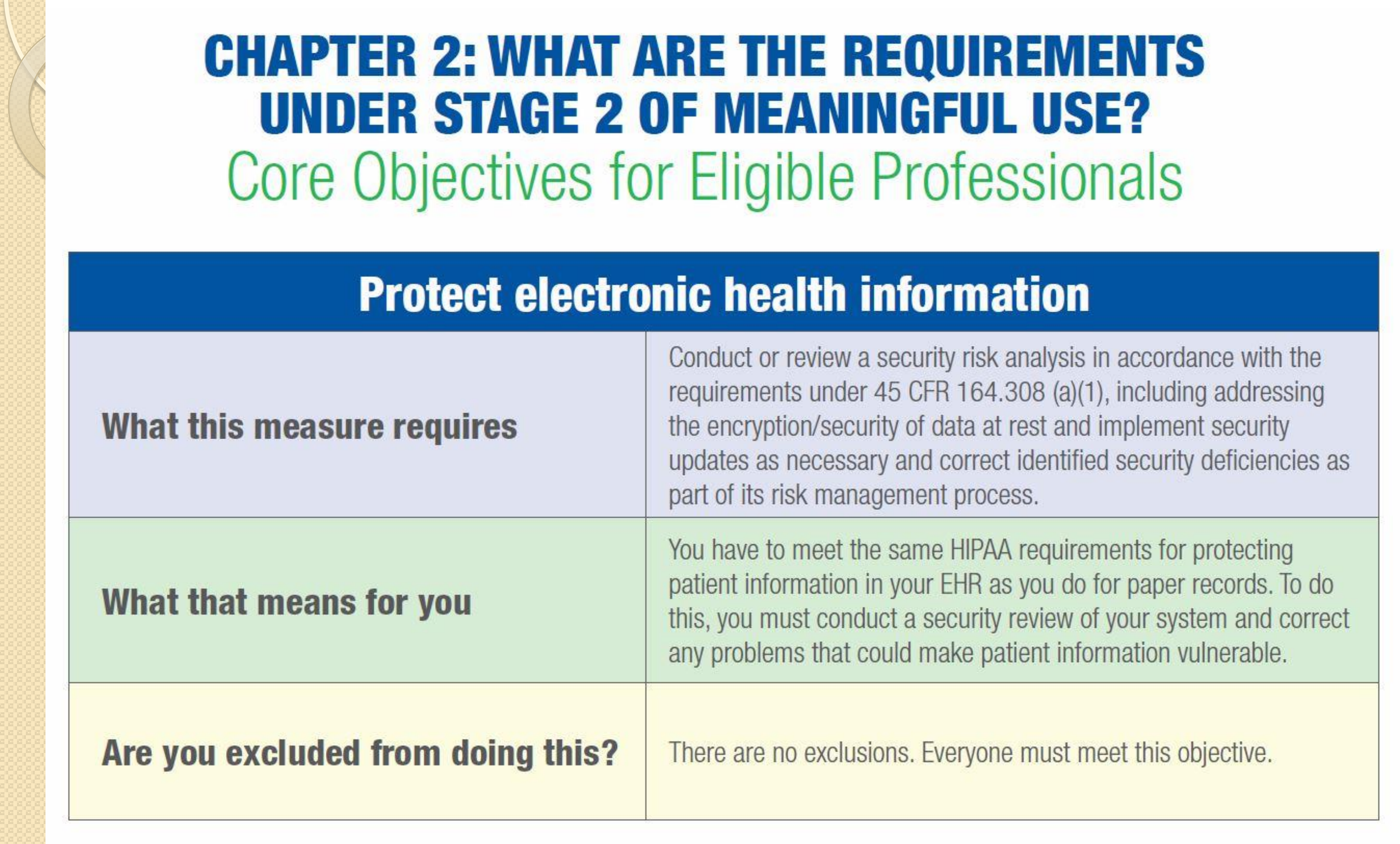
Money Penalties for HIPAA Violations

There are four categories of violations that reflect the increasing seriousness of the HIPAA violation. The corresponding tiers of penalty amounts are shown below.

Violation Category –Section 1176(a)(1)	Each Violation	All Such Violations of an Identical Provision in a Calendar Year
(A) Did Not Know	$100 - $50,000	$1,500,000
(B) Reasonable Cause	$1,000 - $50,000	$1,500,000
(C)(i) Willful Neglect-Corrected	$10,000 - $50,000	$1,500,000
(C)(ii) Willful Neglect-Not Corrected	$50,000	$1,500,000

Business associates of covered entities are now liable for civil money penalties for HIPAA violations

Florida Providers Implementing EHRs

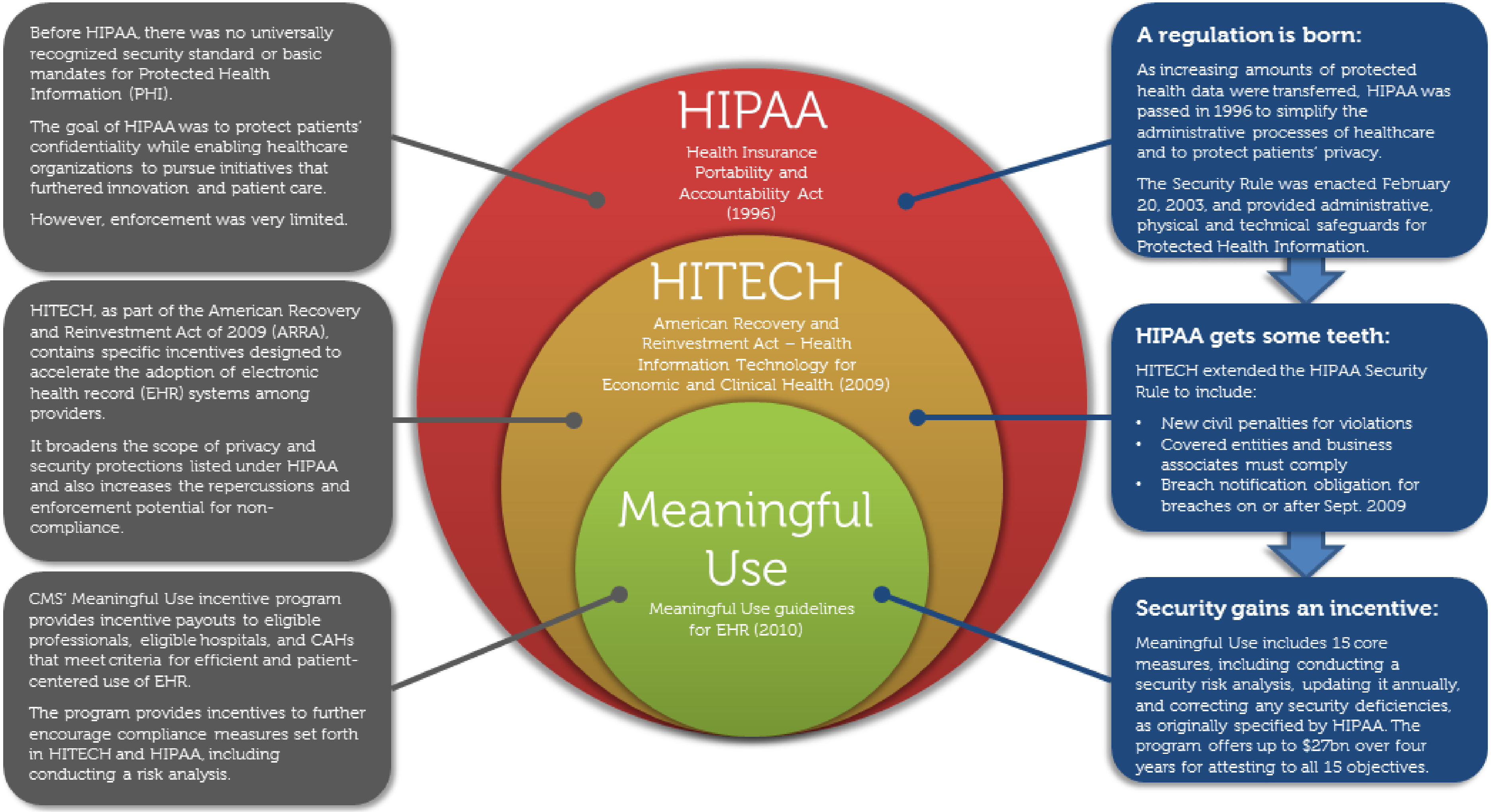


CHAPTER 2: WHAT ARE THE REQUIREMENTS UNDER STAGE 2 OF MEANINGFUL USE?

Core Objectives for Eligible Professionals

Protect electronic health information	
What this measure requires	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308 (a)(1), including addressing the encryption/security of data at rest and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.
What that means for you	You have to meet the same HIPAA requirements for protecting patient information in your EHR as you do for paper records. To do this, you must conduct a security review of your system and correct any problems that could make patient information vulnerable.
Are you excluded from doing this?	There are no exclusions. Everyone must meet this objective.

Meaningful Use and Healthcare IT Security



Before HIPAA, there was no universally recognized security standard or basic mandates for Protected Health Information (PHI).

The goal of HIPAA was to protect patients' confidentiality while enabling healthcare organizations to pursue initiatives that furthered innovation and patient care.

However, enforcement was very limited.

HITECH, as part of the American Recovery and Reinvestment Act of 2009 (ARRA), contains specific incentives designed to accelerate the adoption of electronic health record (EHR) systems among providers.

It broadens the scope of privacy and security protections listed under HIPAA and also increases the repercussions and enforcement potential for non-compliance.

CMS' Meaningful Use incentive program provides incentive payouts to eligible professionals, eligible hospitals, and CAHs that meet criteria for efficient and patient-centered use of EHR.

The program provides incentives to further encourage compliance measures set forth in HITECH and HIPAA, including conducting a risk analysis.

HIPAA

Health Insurance Portability and Accountability Act (1996)

HITECH

American Recovery and Reinvestment Act – Health Information Technology for Economic and Clinical Health (2009)

Meaningful Use

Meaningful Use guidelines for EHR (2010)

A regulation is born:

As increasing amounts of protected health data were transferred, HIPAA was passed in 1996 to simplify the administrative processes of healthcare and to protect patients' privacy.

The Security Rule was enacted February 20, 2003, and provided administrative, physical and technical safeguards for Protected Health Information.

HIPAA gets some teeth:

HITECH extended the HIPAA Security Rule to include:

- New civil penalties for violations
- Covered entities and business associates must comply
- Breach notification obligation for breaches on or after Sept. 2009

Security gains an incentive:

Meaningful Use includes 15 core measures, including conducting a security risk analysis, updating it annually, and correcting any security deficiencies, as originally specified by HIPAA. The program offers up to $27bn over four years for attesting to all 15 objectives.

Risk versus Security

Security and Risk are related concepts that refer to the overall safety of IT systems and the identification of threats and vulnerabilities that might negatively impact the IT system.

Information Security encompasses:

- Administrative, physical, and technical safeguards in an information system
- The protection of information and information systems from unauthorized access, modification, or destruction in order to maintain confidentiality, integrity, and availability.

Risk is a probability measure that estimates the extent to which an entity is threatened by a potential circumstance or event. The estimate of risk is typically a function of:

- The adverse impacts that would arise if an event occurs
- The likelihood of occurrence

Risk Assessment

Risk assessment is the first process in a health care provider's **risk management policy** and is used to determine potential threats and risk associated with an IT system.

The HIPAA Security Rule requires covered entities to evaluate risks and vulnerabilities in their environments and to implement policies and procedures to address those risks and vulnerabilities.

Section § 164.308(a)(1)(ii)(A) is quite specific:

- (A) *Risk analysis (Required).* Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

HIPAA Security Rule: Administration

§ 164.308 Administrative safeguards

(1)(i**)** Standard: **Security management process**

(ii) Implementation specifications:

(A) **Risk analysis** - Required

- Assess potential risks and vulnerabilities to ePHI

(B) **Risk management** - Required

- Security measures to reduce risks and vulnerabilities

(C) **Sanction policy** - Required

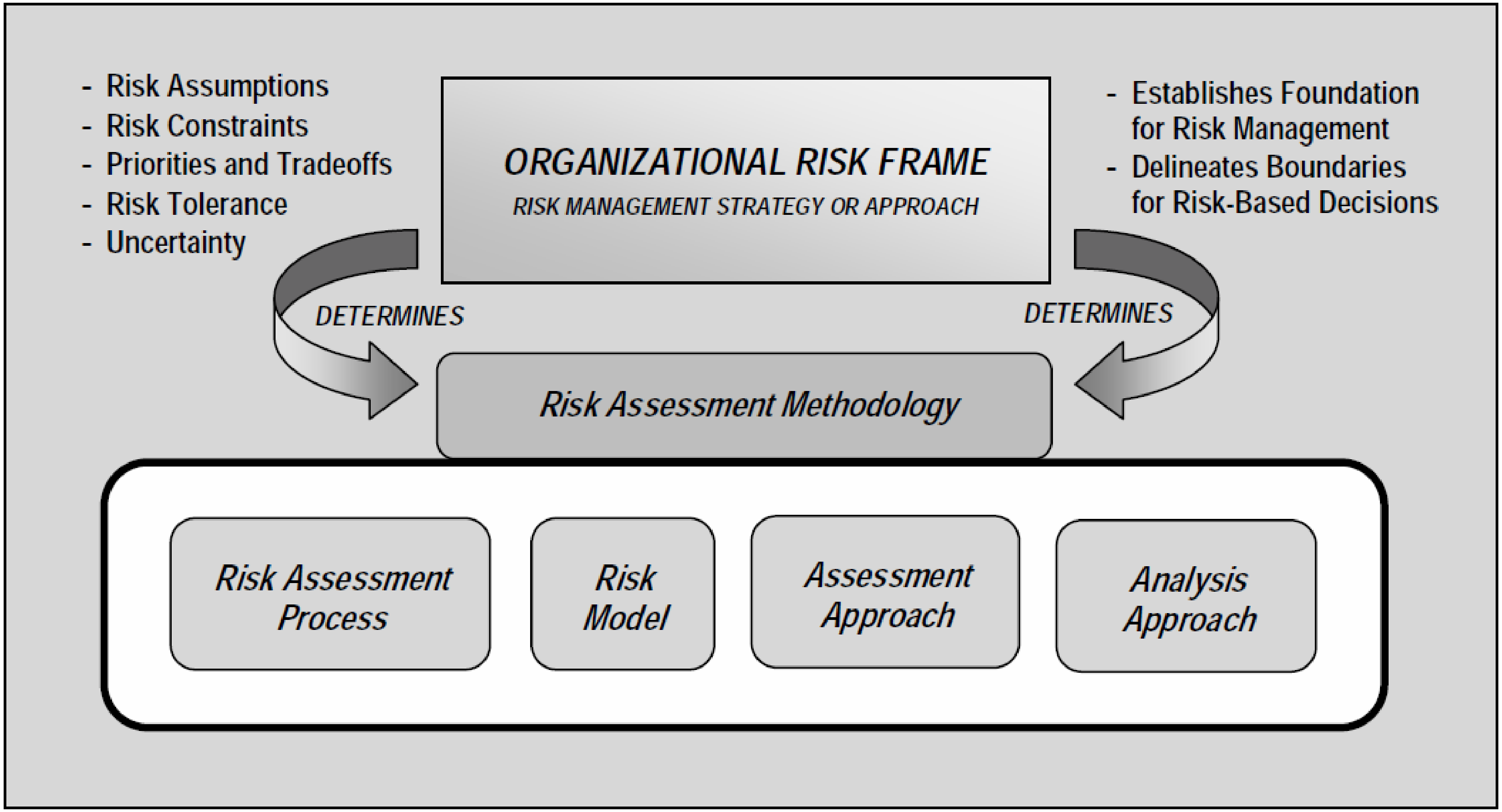
- Apply sanctions against staff who fail to comply with security policies

(D) **Information system activity review** - Required

- Review audit logs, access reports, and security incident tracking reports.

NIST Organizational Risk Frame

Risk framing describes a risk management strategy that addresses how to assess risk, respond to and monitor risk.



- Risk Assumptions
- Risk Constraints
- Priorities and Tradeoffs
- Risk Tolerance
- Uncertainty

ORGANIZATIONAL RISK FRAME

RISK MANAGEMENT STRATEGY OR APPROACH

- Establishes Foundation for Risk Management
- Delineates Boundaries for Risk-Based Decisions

DETERMINES

DETERMINES

Risk Assessment Methodology

Risk Assessment Process

Risk Model

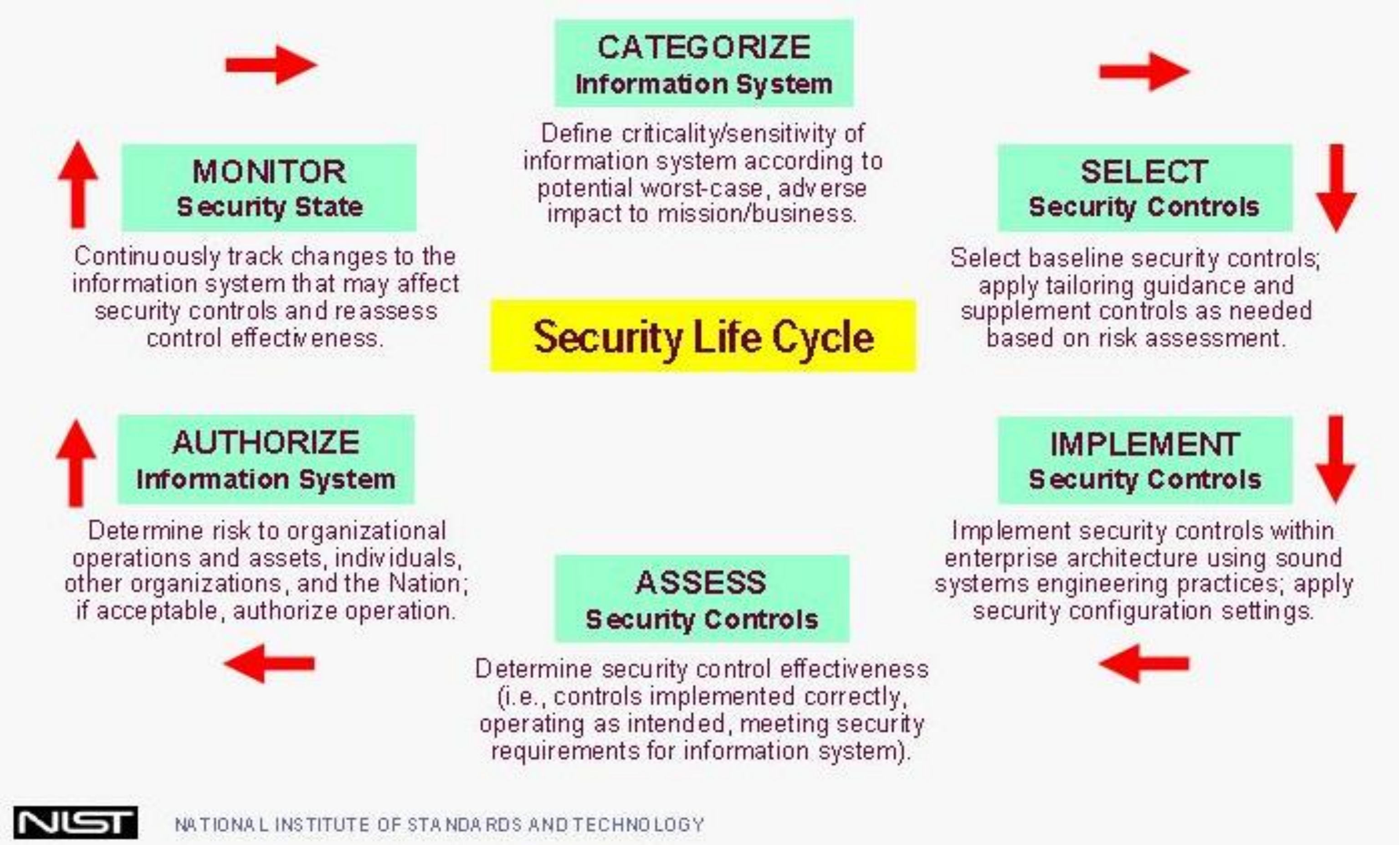
Assessment Approach

Analysis Approach

FIGURE 2: RELATIONSHIP AMONG RISK FRAMING COMPONENTS

Risk Management Framework

The **Risk Management Framework** incorporates the risk analysis into a larger framework that deals with managing risk to ensure security of protected health information. It consists of six recurring steps, of which risk analysis is only one:



CATEGORIZE Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

SELECT Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

IMPLEMENT Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

ASSESS Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

AUTHORIZE Information System

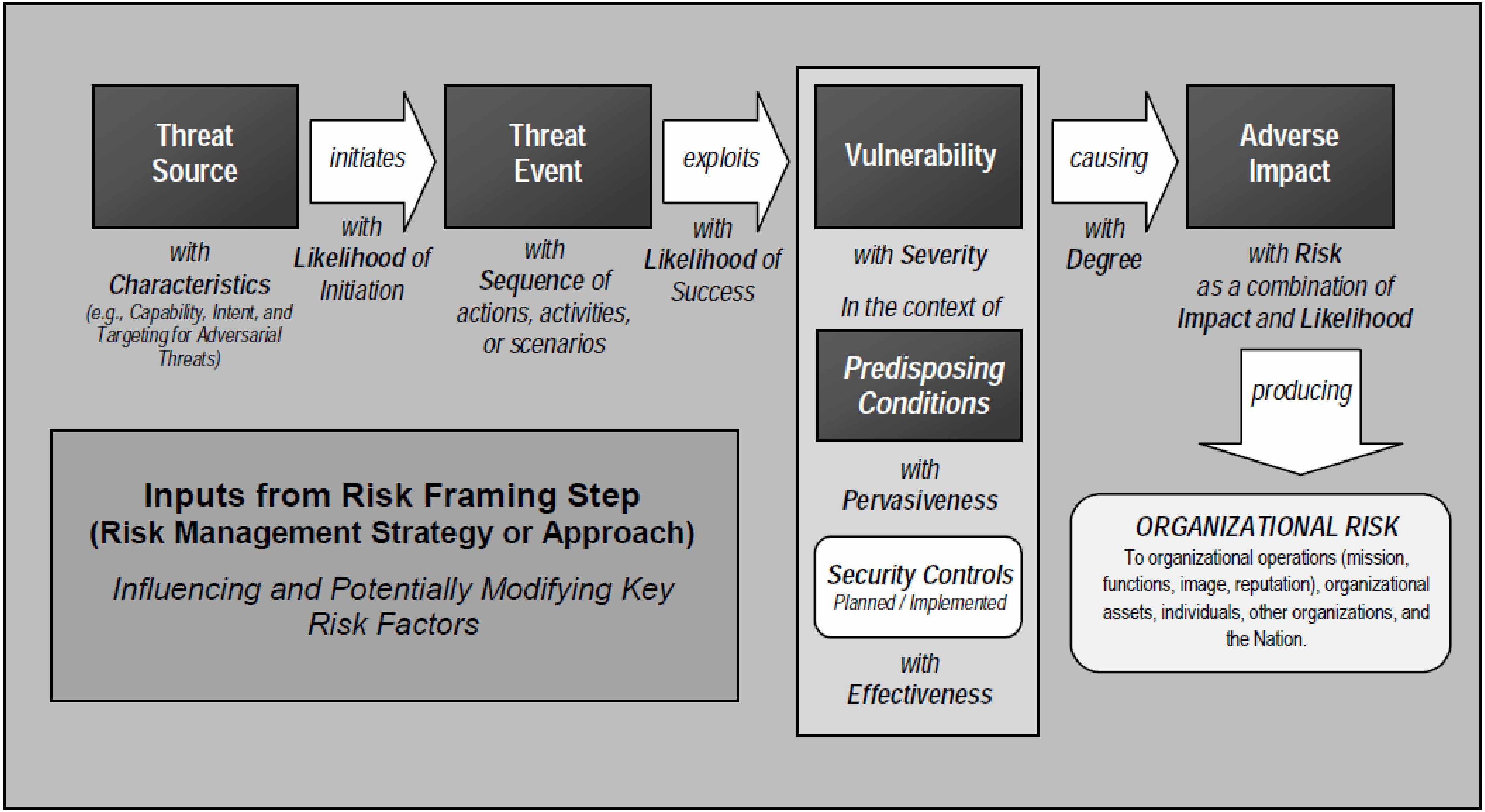
Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

MONITOR Security State

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Key Concepts in Risk Analysis: Risk Models

The NIST Risk Model includes the identification of risk factors and the relationships among those risk factors.



Threat Source

with ***Characteristics***

(e.g., Capability, Intent, and Targeting for Adversarial Threats)

initiates

with ***Likelihood of*** *Initiation*

Threat Event

with ***Sequence of*** *actions, activities, or scenarios*

exploits

with ***Likelihood of*** *Success*

Vulnerability

with ***Severity***

In the context of

Predisposing Conditions

with ***Pervasiveness***

Security Controls

Planned / Implemented

with ***Effectiveness***

causing

with ***Degree***

Adverse Impact

with ***Risk*** *as a combination of* ***Impact*** *and* ***Likelihood***

producing

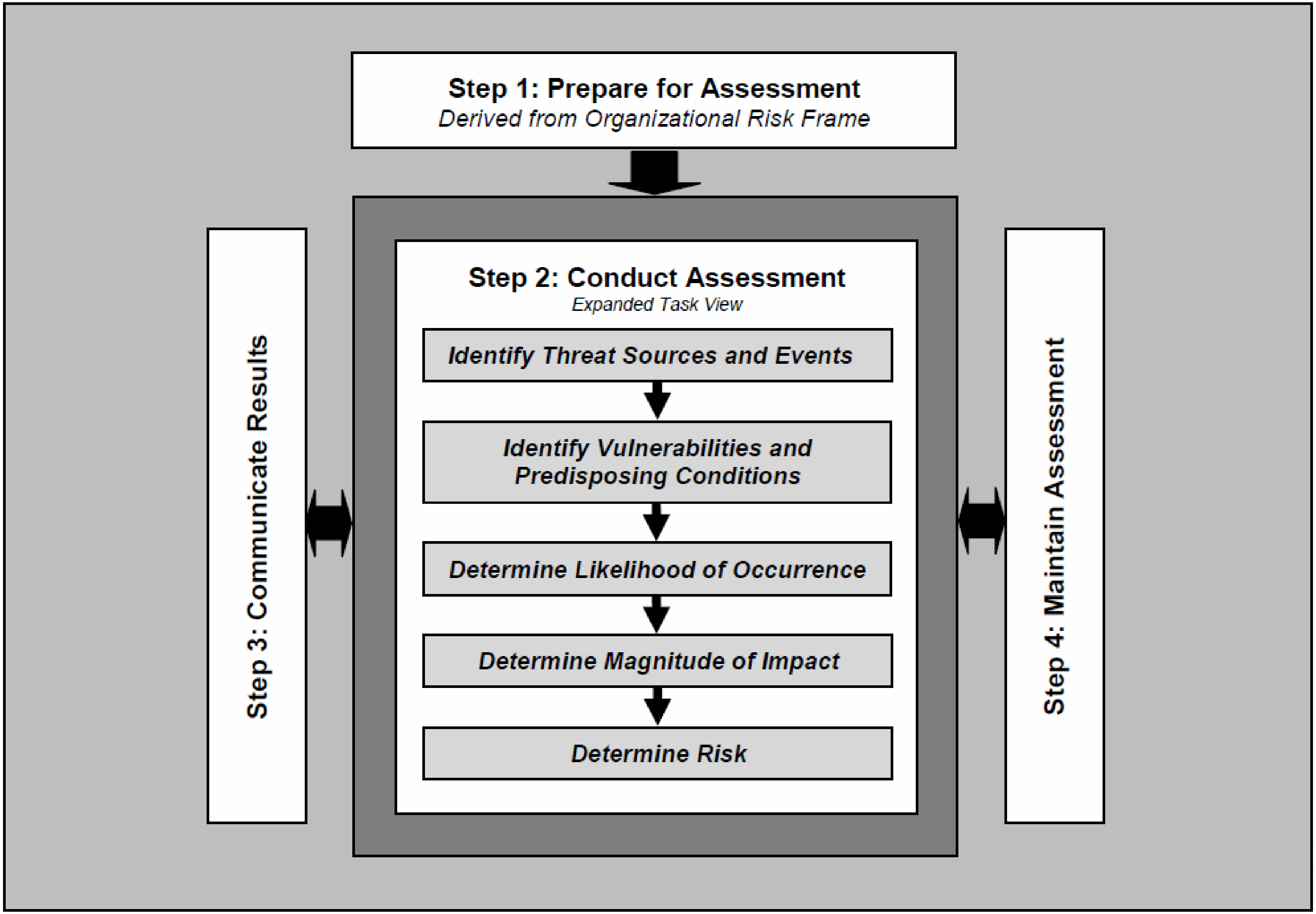
ORGANIZATIONAL RISK

To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.

Inputs from Risk Framing Step (Risk Management Strategy or Approach)

Influencing and Potentially Modifying Key Risk Factors

NIST Risk Assessment Process



Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment

Ongoing Risk Assessment

Risk analysis and risk management are ongoing, dynamic processes that must be periodically reviewed and updated in response to changes in the environment.

Risk assessments provide the baseline for risk management decisions on the health care organization's security controls.

- Risk analysis results inform and guide a more extensive organizational risk monitoring process.
- Organizations use risk assessment to make risk management decisions.
- The risk analysis identifies new risks or updates existing risk levels resulting from operational changes.
- The risk assessment becomes a basic input to an ongoing program of risk management.

Questions?

Christopher B. Sullivan, PhD
Image Research, LLC
cbsullivan@imageresearch.com
850-591-2821