

# **Advanced Strategies in HIPAA Security Risk Analysis**

---

**Margret Amatayakul, RHIA, CHPS,  
FHIMSS**

**Steven S. Lazarus, PhD, FHIMSS**

# Margret A

## Margret\A Consulting, LLC

*Strategies for the digital future of healthcare information*

- ❑ **Information management and systems consultant, focusing on electronic health records and their value proposition**
  - ❑ **Adjunct faculty, College of St. Scholastica; former positions with CPRI, AHIMA, Univ. of Ill., IEEI**
  - ❑ **Active participant in standards development**
  - ❑ **Speaker and author (Silver ASHPE Awards for "HIPAA on the Job" column in *Journal of AHIMA*)**
- ❑ Strategic IT planning
  - ❑ Compliance assessments
  - ❑ Work flow redesign
  - ❑ Project management and oversight
  - ❑ ROI/benefits realization
  - ❑ Training and education
  - ❑ Vendor selection
  - ❑ Product/market analysis

# Steve Lazarus

## Boundary Information Group

*Strategies for workflow, productivity, quality and patient satisfaction improvement through health care information*

- **Business process consultant focusing on electronic health records, and electronic transactions between organizations**
- **Former positions with MGMA, University of Denver, Dartmouth College; advisor to national associations**
- **Active leader in the Workgroup for Electronic Data Interchange (WEDI)**
- **Speaker and author (two books on HIPAA Security and one forthcoming on electronic health record)**

- Strategic IT business process planning
- ROI/benefits realization
- Project management and oversight
- Workflow redesign
- Education and training
- Vendor selection and enhanced use of vendor products
- Facilitate collaborations among organizations to share/exchange health care information

# Agenda

---

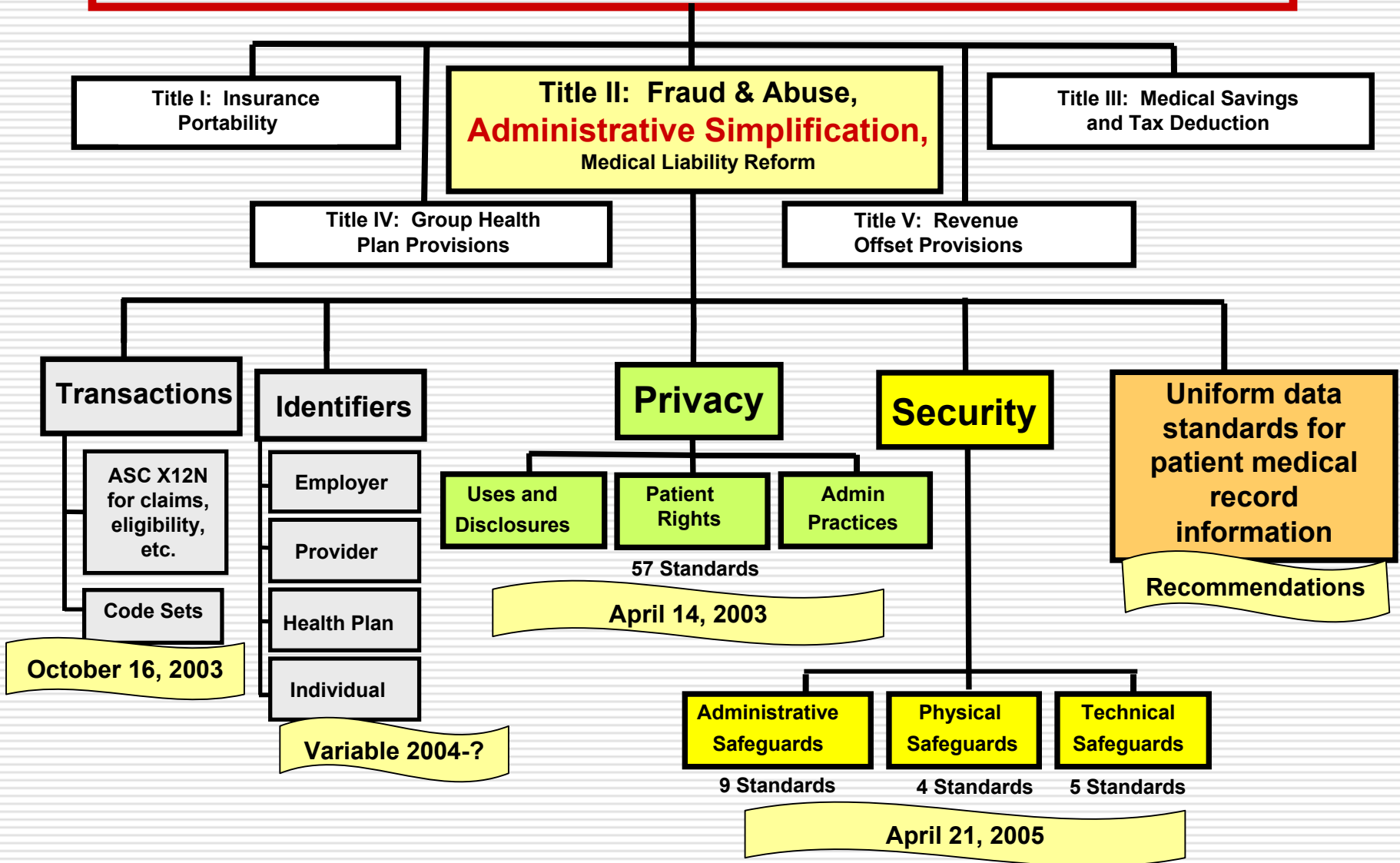
- ❑ **Security Rule in context of HIPAA**
- ❑ **Risk-based Approach to Information Security**
- ❑ **Executive Risk Mitigation Strategies**
- ❑ **Planning and Managing the Project**
- ❑ **Risk Management Approaches**
- ❑ **“Best Practices” for Ongoing Compliance**

# **Advanced Strategies in HIPAA Security Risk Analysis**

---

## **Security Rule in context of HIPAA**

# Health Insurance Portability & Accountability Act



# **“Mini-Security Rule”**

---

- “Mini-security rule” in Privacy Rule is not sufficient**
  - Does not address risk analysis**
  - Focuses on incidental disclosures**
  - Lacks specificity**
  - Efforts may be 2 – 4 years old**
- “Mini-security rule” does address the need to “secure” paper and oral forms of PHI**

# Fraud & Abuse Sets Precedence

<b>Fraud and Abuse</b>	<b>Privacy and Security</b>
1. Written standards of conduct & policies & procedures	1. Privacy & security policies & procedures
2. Designation of chief compliance officer; reports to CEO & governing body	2. Designation of information privacy official & information security official
3. Regular, effective education & training for all affected employees	3. Training & awareness building
4. Process to receive complaints & protect whistleblowers from retaliation	4. Privacy complaint & security incident reporting procedures
5. System to respond to allegations & the enforcement of disciplinary action	5. Complaint/incident handling & enforcement of sanction policy
6. Audits &/or other evaluation techniques to monitor compliance	6. Ensure uses & disclosures consistent with notice; information system activity review, risk management, evaluation
7. Investigation & remediation; policies addressing non-employment or retention of sanctioned individuals	7. Termination procedures for members of workforce & business associate contracts



# Security of TCS

---

- Promote adoption of electronic transactions**
- Achieve benefits of “direct connectivity”**
- Claims attachments coming**

# Uniform Data Standards for PMRI

---

- **Recommendations**
  - **Interoperability**
  - **Comparability**
- **EHR Initiatives**
  - **Uniform data sets**
  - **Pay-for-performance**
- **Heightened need for:**
  - **Contingency planning**
  - **Access controls**
  - **Authentication**

- **Interoperability**
  - HL7
  - DICOM
  - NCPDP SCRIPT
  - IEEE 1073
- **Comparability**
  - SNOMED CT®
  - LOINC
  - Federal Drug Terminologies

# **Advanced Strategies in HIPAA Security Risk Analysis**

---

**Using a Risk-based  
Approach to Information  
Security**

# YOU decide !

---

- Comprehensive**
  - Must address *all* aspects of security for electronic PHI
- Scalable**
  - Size, complexity, capabilities
  - Technical infrastructure
  - Costs
  - Probability & criticality of risks
- Technology-neutral**
  - Stable, but flexible
- Standards**
  - Require compliance
- Required & Addressable Implementation Specifications**
  - Implement or document alternative
- Very specific/very general, e.g.,**
  - Maintenance records
  - Encryption

# Benefits of Risk Analysis

---

- Comply with HIPAA**
- Build a business case**
- Help executives meet fiduciary duties**
- Build staff awareness & support**
- Uncover excellent new ideas**
- Reduce damages if you are sued**

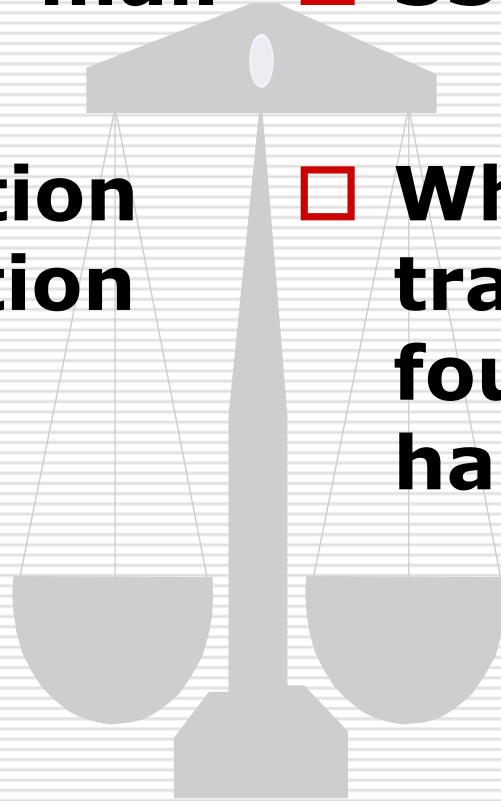
# Examples

---

Encrypted e-mail       SSL Web portal

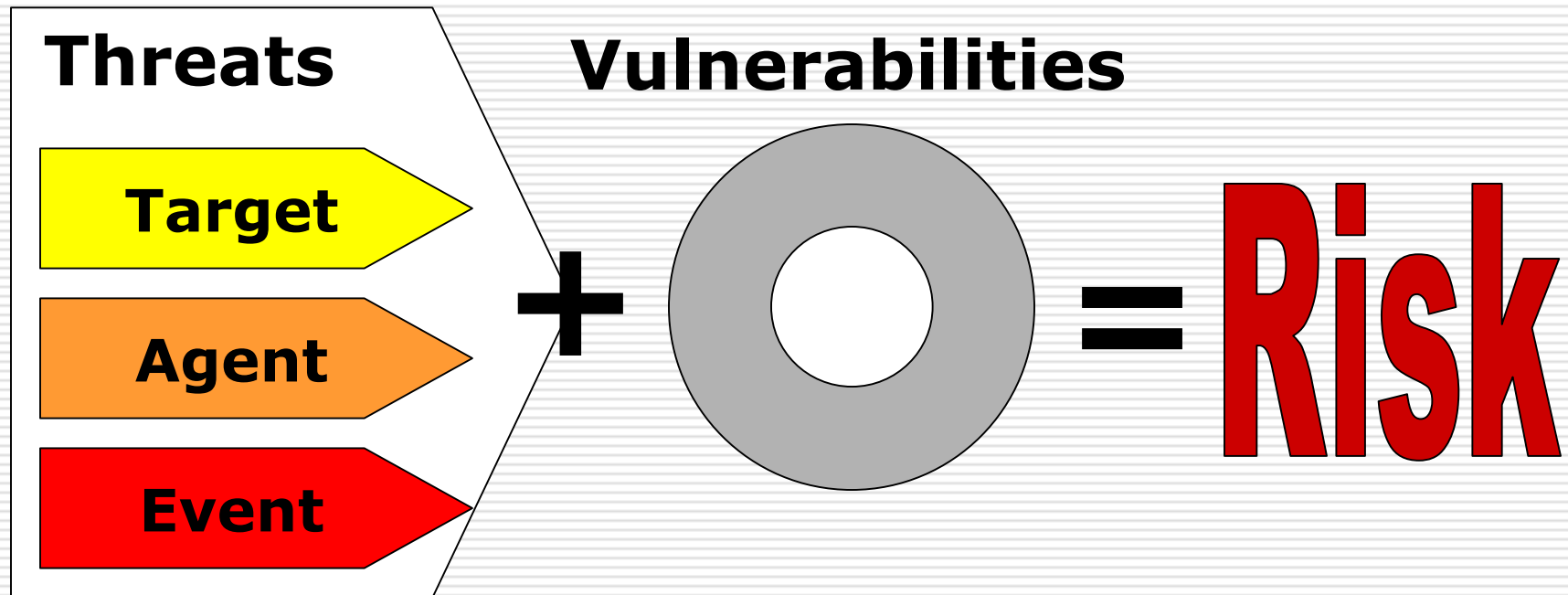
Reconstruction  
of examination  
rooms

White noise,  
tranquility  
fountains, wall  
hangings



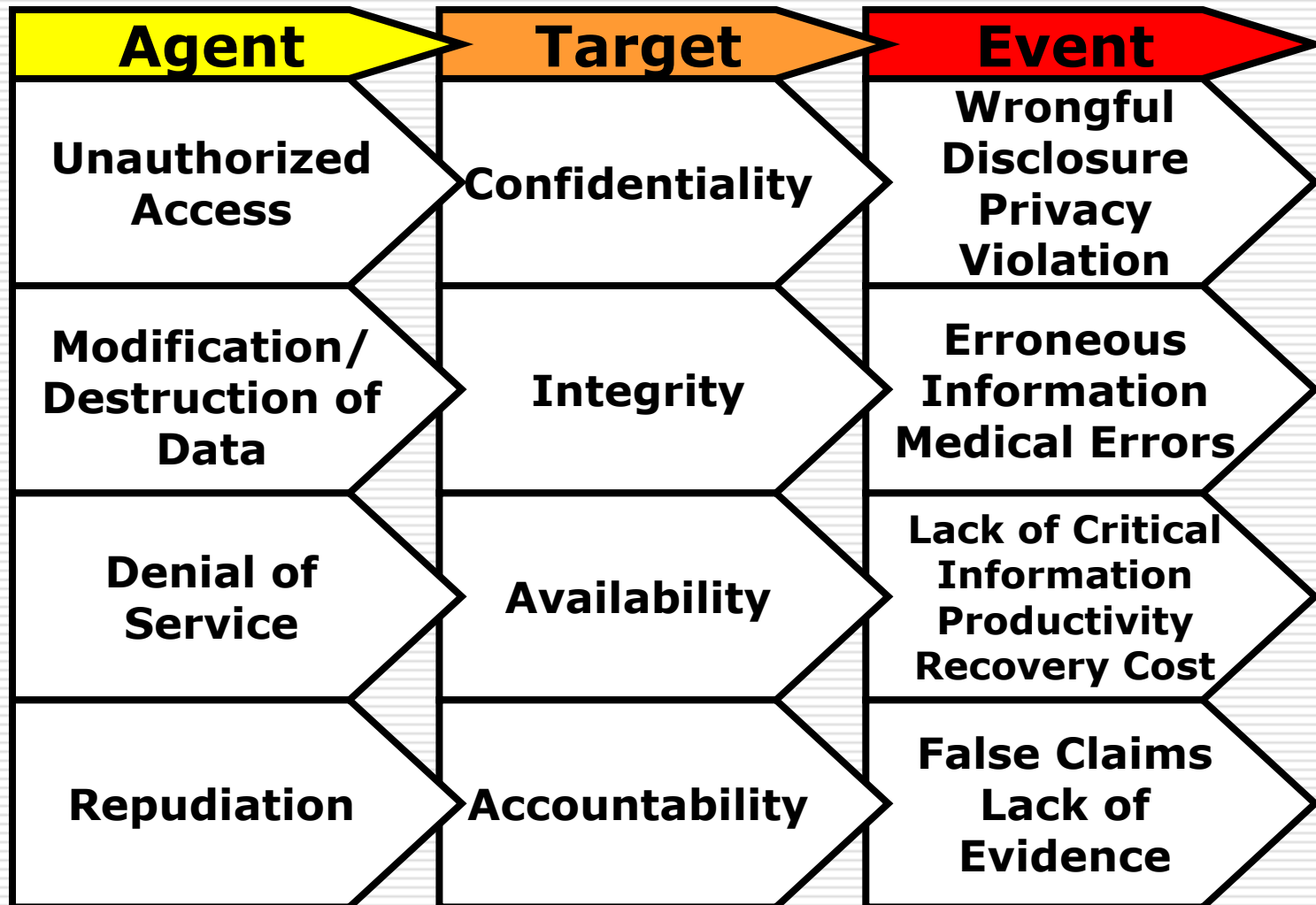
# Risk Analysis Process

---



# Targets – Agents - Events

---





# Threat Sources

---

## □ Accidental Acts

- Incidental disclosures
- Errors and omissions
- Proximity to risk areas
- Work stoppage
- Equipment malfunction

## □ Deliberate Acts

- Inattention/inaction
- Misuse/abuse of privileges
- Fraud
- Theft/embezzlement
- Extortion
- Vandalism
- Crime

## □ Environmental threats

- Contamination
- Fire
- Flood
- Weather
- Power
- HVAC

**What are YOUR concerns?**

# Surveys

## Internal Threats

Source: eWeek, January 21, 2002

**57% - Users accessing resources they are not entitled to**

**43% - Accounts left open after employee has left company**

**27% - Access to contractors not terminated upon project completion**

**21% - Attempted or successful break-in by angry employee**

# Primary Healthcare Concerns

.Adapted from: *Journal of Healthcare Information Management*, 17/1

## Tangible Losses

- Cost of data recovery
- Lost user productivity
- Investigate/prosecute offenders
- Insurance premium increases
- Fees for contract/regulatory defense
- Cost of fines

## Intangible Issues

- Harm to patient
- Lost patient & business partner confidence & loyalty
- Lost reputation, contributing to difficulty in recruitment
- Lower employee morale
- Career-threatening corporate officer liabilities

# Vulnerabilities

---

## Administrative

- Policy
- Accountability
- Management
- Resources
- Training
- Documentation

## Physical

- Entrance/exit controls
- Supervision/monitoring
- Locks, barriers, routes
- Hardware
- Property
- Disposal

## Technical

- New applications
- Major modifications
- Network reconfiguration
- New hardware
- Open ports
- Architecture
- Controls

# Security Vulnerability Tests

---

- Policy & procedure review
- Workforce perception survey
- Certification/accreditation
- Disaster recovery plan drills
- Social engineering
- Document grinding
- Facility security review
- Communications testing
- Wireless testing
- Backup, maintenance & change control log review
- Internet presence identification & testing

# Probability of Occurrence

- Has it happened before?
- How frequently?
- Does threat source have
  - Access, knowledge, motivation?
  - Predictability, forewarning?
  - Known speed of onset, spread, duration?
- Are controls available to
  - Prevent?
  - Deter?
  - Detect?
  - React?
  - Recover?

# Criticality of Impact

- Patient care
- Confidentiality
- Complaint/lawsuit
- Reduce productivity
- Loss of revenue
- Cost to remediate
- Licensure/ accreditation
- Consumer confidence
- Competitive advantage

# Risk Ranking

---

<b>Probability of Occurrence</b>	<b>Criticality of Impact</b>		
	<b>Low</b>	<b>Medium</b>	<b>High</b>
<b>High</b>	<b>3</b>	<b>6</b>	<b>9</b>
<b>Medium</b>	<b>2</b>	<b>4</b>	<b>6</b>
<b>Low</b>	<b>1</b>	<b>2</b>	<b>3</b>

# Example

---

Security Standard	Vulnerabilities	Threats	Probability	Criticality	Risk Score
Person or entity authentication	Weak password	Shoulder surfing	M	H	6

Probability	Criticality		
High	3	6	9
Medium	2	4	6
Low	1	2	3
	Low	Medium	High

# **Advanced Strategies in HIPAA Security Risk Analysis**

---

## **Executive Risk Mitigation Strategies**



# Has this happened to YOU?

- ❑ Foreign hacker stole 4,000 medical records from University of Washington, mid-2000
- ❑ Kaiser Permanente sent 858 patients' medical records to 19 before error in e-mail upgrade system was caught, Aug, 2000
- ❑ A 13-year-old daughter brought to work at University Medical Center, Jacksonville, stole patients' names and phone numbers and called them saying they either had AIDS or were pregnant, March, 1996
- ❑ A 17-year-old boy reconfigured physicians' central paging system at Inova Fairfax Hospital to forward pages to his own pager, & called in prescriptions which nurses administered to patients. Dec, 2000

**“It won't happen here”**

# Executive Engagement

---

- **Sarbanes-Oxley Act of 2002, PL 107-204, impact on private sector:**
  - **Management must establish and maintain an adequate **internal control structure** and procedures for financial reporting**
  
- **“A secure information infrastructure is central to many companies’ operational capabilities. Hence, the material condition of the business will be assessed, and certified by officers, in that light.”**
  - **Richard Marks, Davis Wright Tremaine, LLP**

# Risk Mitigation Options

---

<b>Option</b>	<b>NIST Definition</b>
<b>Risk Assumption</b>	<b>Accept risk &amp; continue operating or implement controls to lower risk to an acceptable level</b>
<b>Risk Avoidance</b>	<b>Avoid risk by eliminating cause and/or consequence</b>
<b>Risk Limitation</b>	<b>Limit risk with controls that minimize adverse impact of a threat's exercising a vulnerability</b>
<b>Risk Planning</b>	<b>Manage risk by developing a plan that prioritizes, implements, and maintains controls</b>
<b>Research &amp; Acknowledgement</b>	<b>Lower risk of loss by acknowledging vulnerability &amp; researching controls to correct</b>
<b>Risk Transference</b>	<b>Transfer risk by using other options to compensate for the loss, such as insurance</b>

Source: NIST, Special Publication 800-30, "Risk Management Guide for Information Technology Systems," U.S. Government Printing Office, Washington, DC, 2001.

# Wasn't this done before?

---

## Assessment

Identify **Vulnerabilities**

Prioritize by:  
■ Privacy Rule  
■ Importance

## Risk Analysis

Identify **Vulnerabilities**

+

Identify **Threats**

+

Measure

■ **Probability of Occurrence**

■ **Criticality of Impact**

=

Determine Risk



Select **Controls**

Identify **Residual Risk**

# Business Case Example

---

- ❑ **HIPAA doesn't require a hot site**
- ❑ **What form of DRP should you recommend for this environment?**



**Top ranking states  
in terms of number  
of killer tornadoes:**

**Texas  
Oklahoma  
Arkansas  
Alabama  
Mississippi  
Illinois  
Missouri  
Indiana  
Louisiana  
Tennessee**



# Residual Risk

---

- ❑ Level of risk remaining after controls have been implemented
- ❑ No such thing as 100% secure
- ❑ Estimate in same manner as original risk determination:
  - Probability of a threat exploiting a vulnerability
  - Criticality of impact
  - Probability plus criticality **with control** define residual risk

# **Advanced Strategies in HIPAA Security Risk Analysis**

---

## **Planning and Managing the Risk Analysis Project**

# Project vs. Process

---

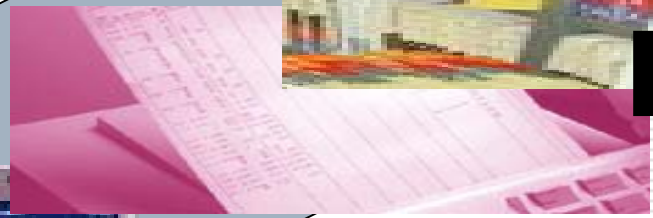
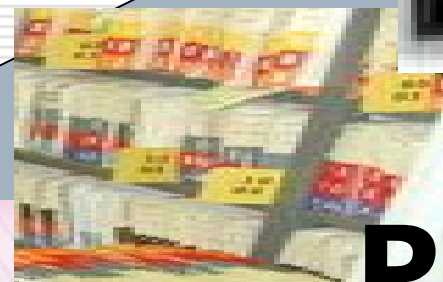
- Executive Support**
- Objectives**
- Scope**
- Staffing**
- Budget**
- Timeline**
- Reporting Results**
- Obtaining Approval for Controls**
- Identifying Residual Risk**

- Implementation**
  - Staffing**
  - External resources**
  - Vendor selection**
  - Licenses & capital**
  - Installation & testing**
  - Training**
  - Documentation**
  
- Ongoing monitoring for compliance**



# Objectives & Scope

---



**PHI**



**ePHI**

# Staffing the Project Team

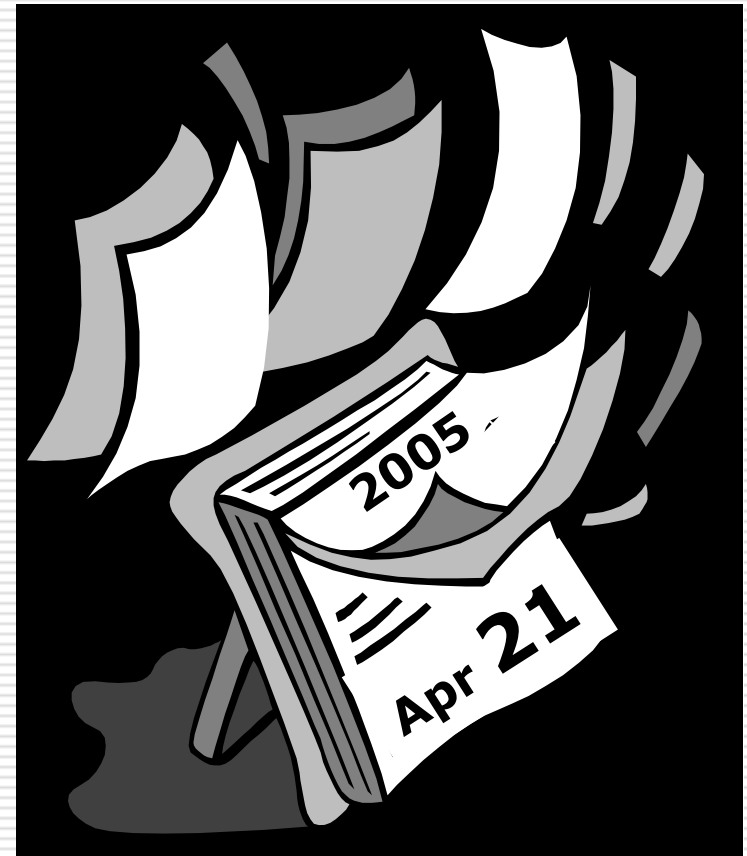
---

<b>Members</b>	<b>Purpose</b>
Information Security Official	Team Leader, Project Manager, Internal Consultant
User Representatives	Understand threats, evaluate functionality of controls, gain buy-in
I.T. Professionals	Identify vulnerabilities, evaluate technical capability, learn administrative controls
Representatives of Other Areas Monitoring Risk	Probability/criticality estimates, support implementation, represent customers
HR, Labor Relations, Legal, Contract Management	Represent user interests, assures controls meet other legal requirements
Trainers	Gain insight for training programs
Information Privacy Official	Coordinate with Privacy Rule compliance
Executive Sponsor	Interpret message for executives

# Budget & Timeline

---

<input type="checkbox"/> <b>Staff</b>	<b>\$</b>
<input type="checkbox"/> <b>External resources</b>	<b>\$</b>
<input type="checkbox"/> <b>Learning &amp; benchmarking resources</b>	<b>\$</b>
<input type="checkbox"/> <b>Software tools</b>	<b>\$</b>
<input type="checkbox"/> <b>Assessment tools &amp; services</b>	<b>\$</b>
<input type="checkbox"/> <b>Resource office</b>	<b>\$</b>



# Results & Approval

Microsoft Excel - Risk Analysis Tool

File Edit View Insert Format Tools Data Window Help

Type a question for help

113

HIPAA Security Risk Analysis and Risk Management Documentation Checklist														
Security Standard (\$ Citation) ■ Implementation Specification (Required/ Addressable)	Vulnerabilities			Threats		Risk Management								
	Policy, Procedure, Form	Process/Control Vulnerability	Criticality	Threats	Probability	Risk Score	Action	Residual Risk	Residual Risk Level	Resources	Approved	Responsible	Start/End Dates	Plan for Ongoing Monitoring
<b>ADMINISTRATIVE SAFEGUARDS</b> {} Corporate {} Site _____ {} Dept. _____														
1. Security Management Process §164.308(a)(1)														
1.1 Risk Analysis (R)														
1.2 Risk Management (R)														
1.3 Sanction Policy (R)														
1.4 Information System Activity Review (R)														
2. Assigned Security Responsibility §164.308(a)(2)														
3. Workforce Security §164.308(a)(3)														
3.1 Authorization and/or Supervision (A)														

# **Advanced Strategies in HIPAA Security Risk Analysis**

---

## **Risk Management Approaches**

# Risk Analysis Approaches

---

## □ Qualitative

- Scenario-based
  - Rating probability and criticality and ranking risk
- Integrates administrative, physical, and technical factors

## □ Quantitative

- Attempts to determine annualized loss expectancy from value of information assets
- Difficult to assign monetary value to health care information

# Quantitative Analysis

---

- **Annualized Loss Expectancy (ALE):**
  - **Asset value, times**
  - **% of asset loss caused by threat, times**
  - **Frequency of threat occurrence in a year**
- **Cost of Safeguard:**
  - **Purchase, development, and/or licensing costs**
  - **Physical installation costs; disruption to normal productivity during installation and testing**
  - **Normal operating costs, resource allocation, and maintenance/repair costs**
- **Cost of Safeguard vs. ALE:**
  - **Positive, recommend remediation**
  - **Negative, consider other alternatives**

# Steps to Conduct the Process

---

- 1. Executive management guidance on risk**
- 2. Inventory & characterize policies, procedures, processes, physical layout, systems**
- 3. Identify threats**
- 4. Identify vulnerabilities**
- 5. Determine likelihood risks may actually occur**
- 6. Analyze impact if risk actually occurs**
- 7. Determine & rate each risk**
- 8. Analyze appropriate types of controls**
- 9. Recommend controls & describe residual risk**
- 10. Document results**



# Practical Assessment

---

## Find Lowest Common Denominator

- Administrative
- Physical
- Technical
- Corporate
- Site/Department
- Application
- Data Center
- Network
- Platform

# Pair Threats & Vulnerabilities

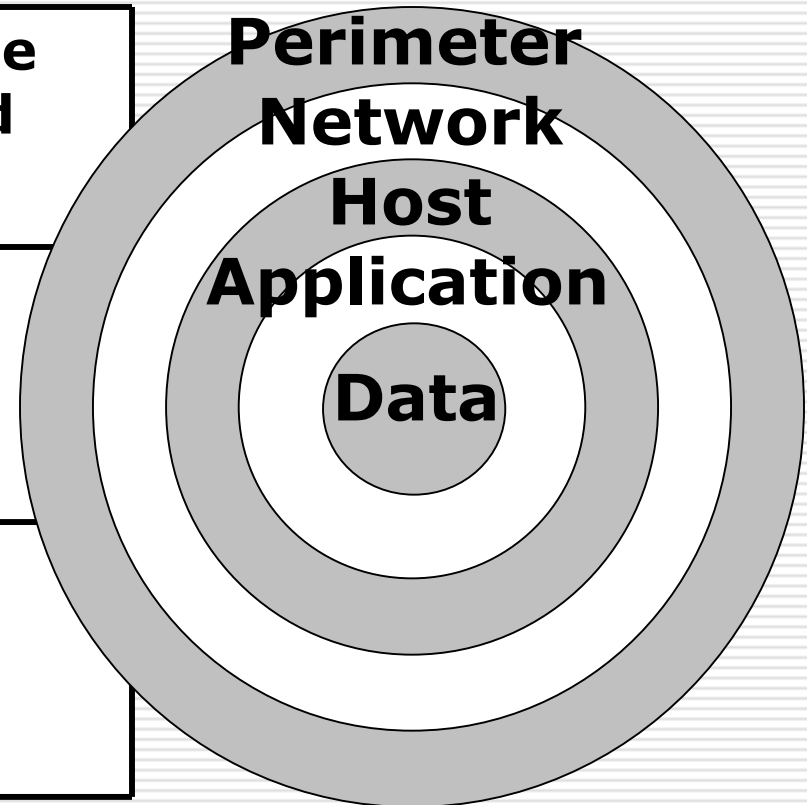
---

<b>Workstation</b>	<b>Location</b>	<b>Vulnerability/Threat Analysis</b>	<b>Control</b>
<i>Desktop</i>	<i>Nursing units</i>	<i>Staff only area, staffed continuously, all workstations turned away from public, high need for availability</i>	<i>Screen saver only</i>
<i>Desktop</i>	<i>Outpatient reception area</i>	<i>Public area, not staffed continuously</i>	<i>User log off on exit reminder &amp; automatic logoff set at 10 min.</i>
<i>Notebook</i>	<i>Exam room</i>	<i>Integrity issue, rotation of users need accountability</i>	<i>User log off on exit</i>

# Security Architecture

---

<b>Security service</b>	<b>Function to be accomplished</b>
<b>Security mechanism</b>	<b>Control that provides security function</b>
<b>Security architecture</b>	<b>Structure of controls to achieve functions</b>



# **Advanced Strategies in HIPAA Security Risk Analysis**

---

**“Best Practices” for  
Ongoing Compliance**

# “Best Practices”

---

- Most effective and efficient
- “Most appropriate”
- What a prudent person would do
- Whether or not specified in regulations

**Not...**

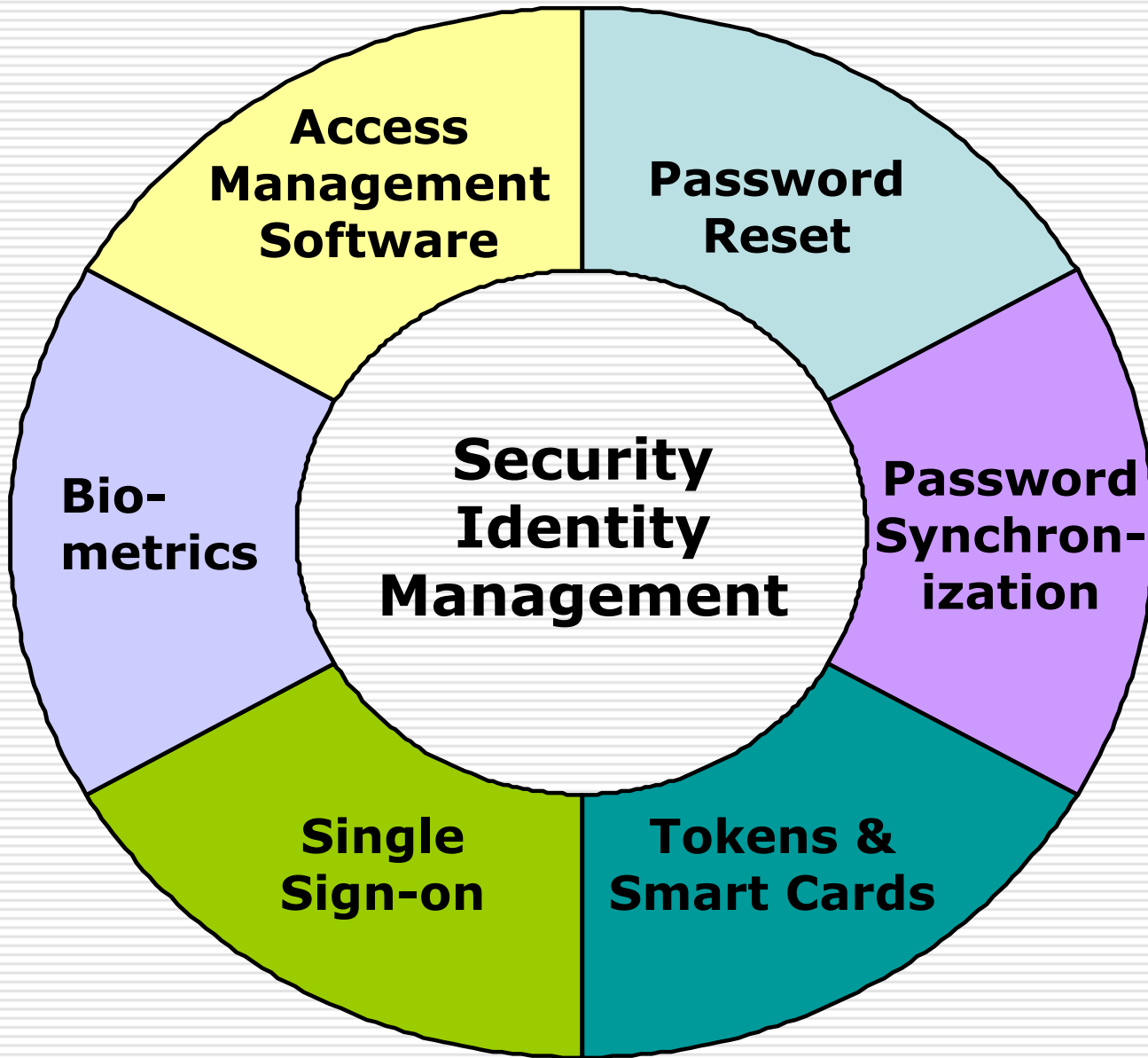
- Most expensive
- Expected to fill every gap
- Necessarily common in industry

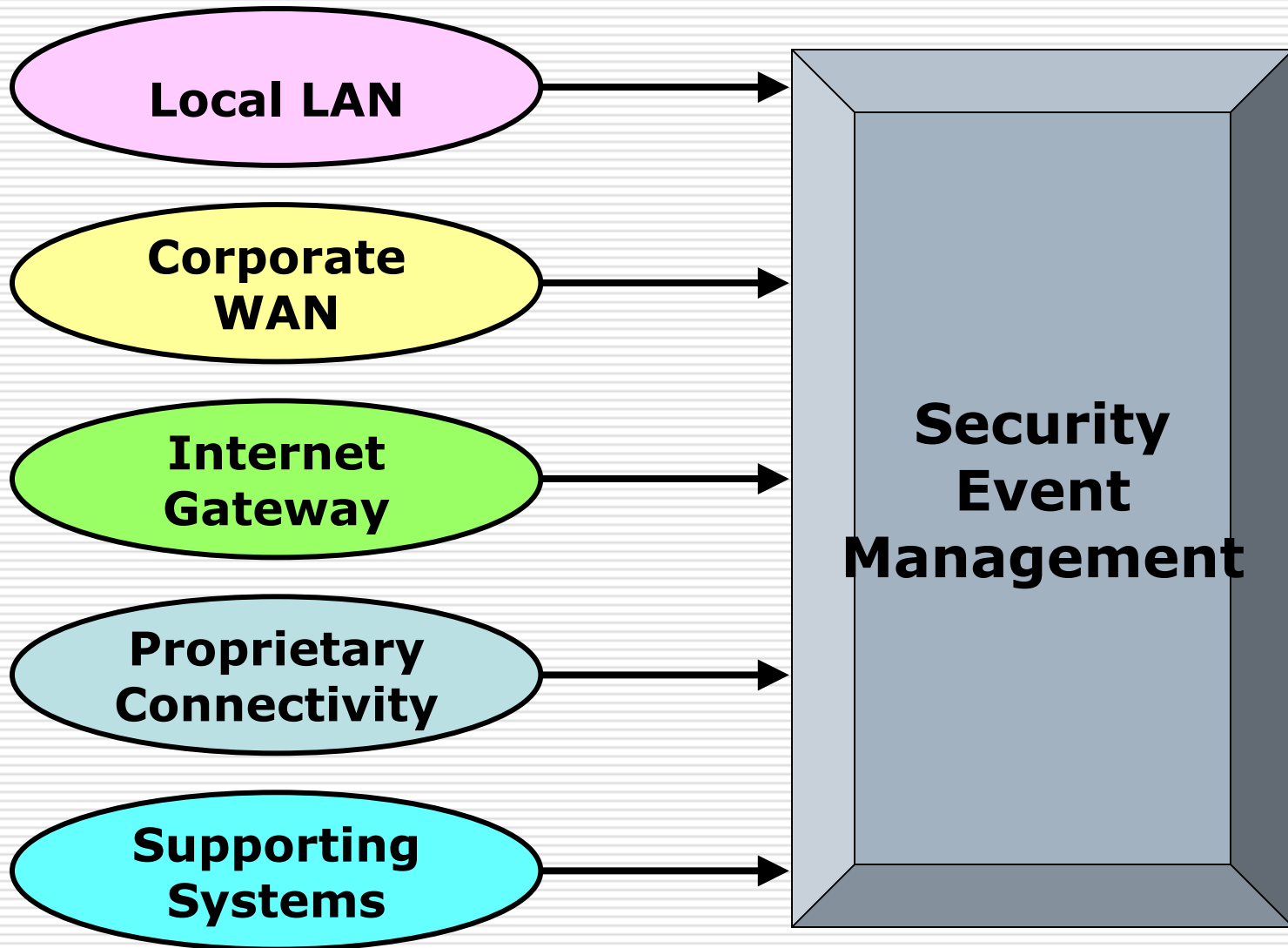
# Proposed Security Rule

---

- Access controls
- Alarms
- Audit trail
- Encryption
- Entity authentication
- Event reporting
- Integrity controls
- Message authentication

**Included in YOUR vendor offerings?**

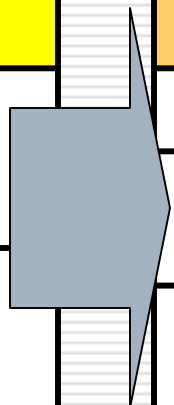






**"Does not apply to treatment..."**

<b>Minimum Necessary</b>	<b>Access Control</b>	<b>Assigns Privileges</b>
<b>Classes of Users</b>	<b>User-based</b>	<b>To each user</b>
<b>Categories of PHI</b>	<b>Role-based</b>	<b>To classes of users to categories of PHI</b>
<b>Conditions of Access</b>	<b>Context-based</b>	<b>Based on conditions</b>



**But, if there is no treatment relationship..."**



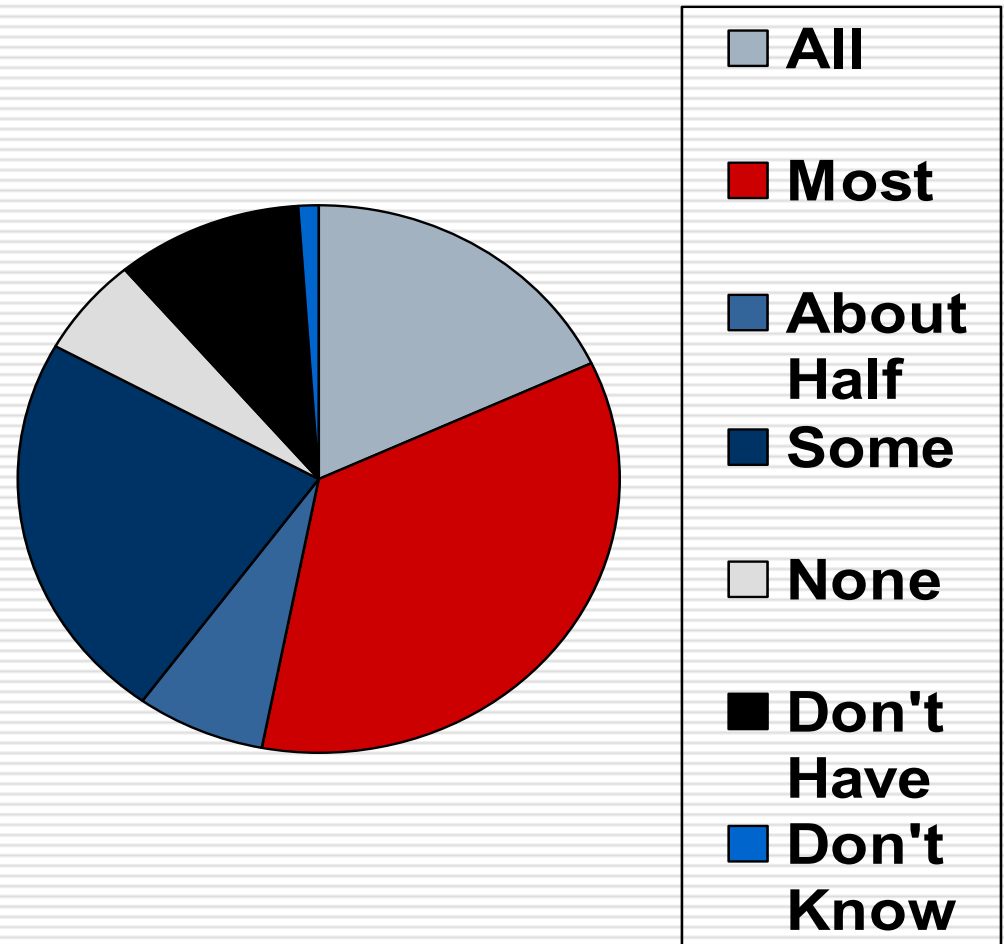
# Compliance

---

Extent to which  
IT security decisions  
were guided by policy

Source: *Information Security*, 9/2002

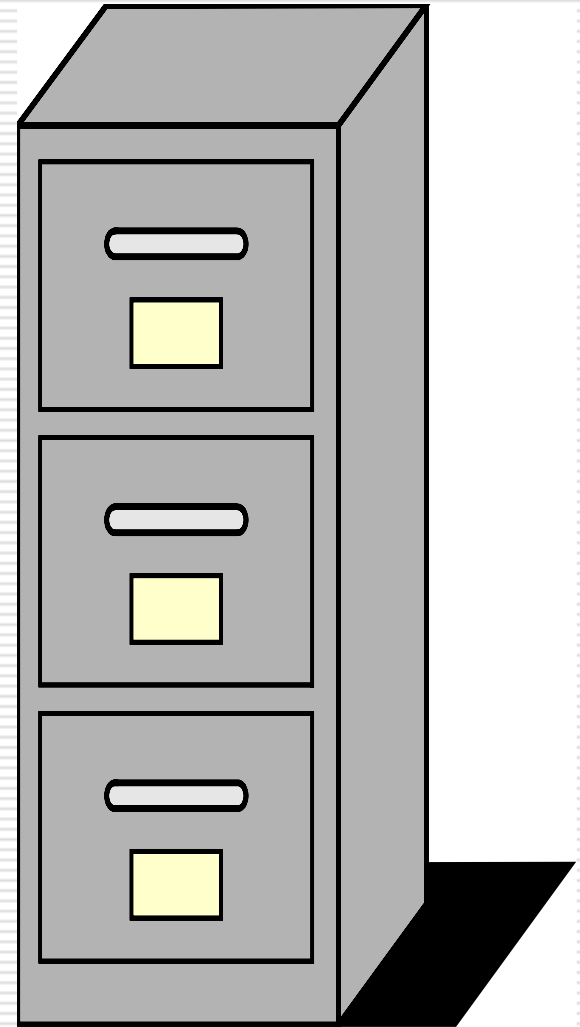
- Policies
- Standards
- Procedures
- Specifications
- Reports & logs



# Documentation

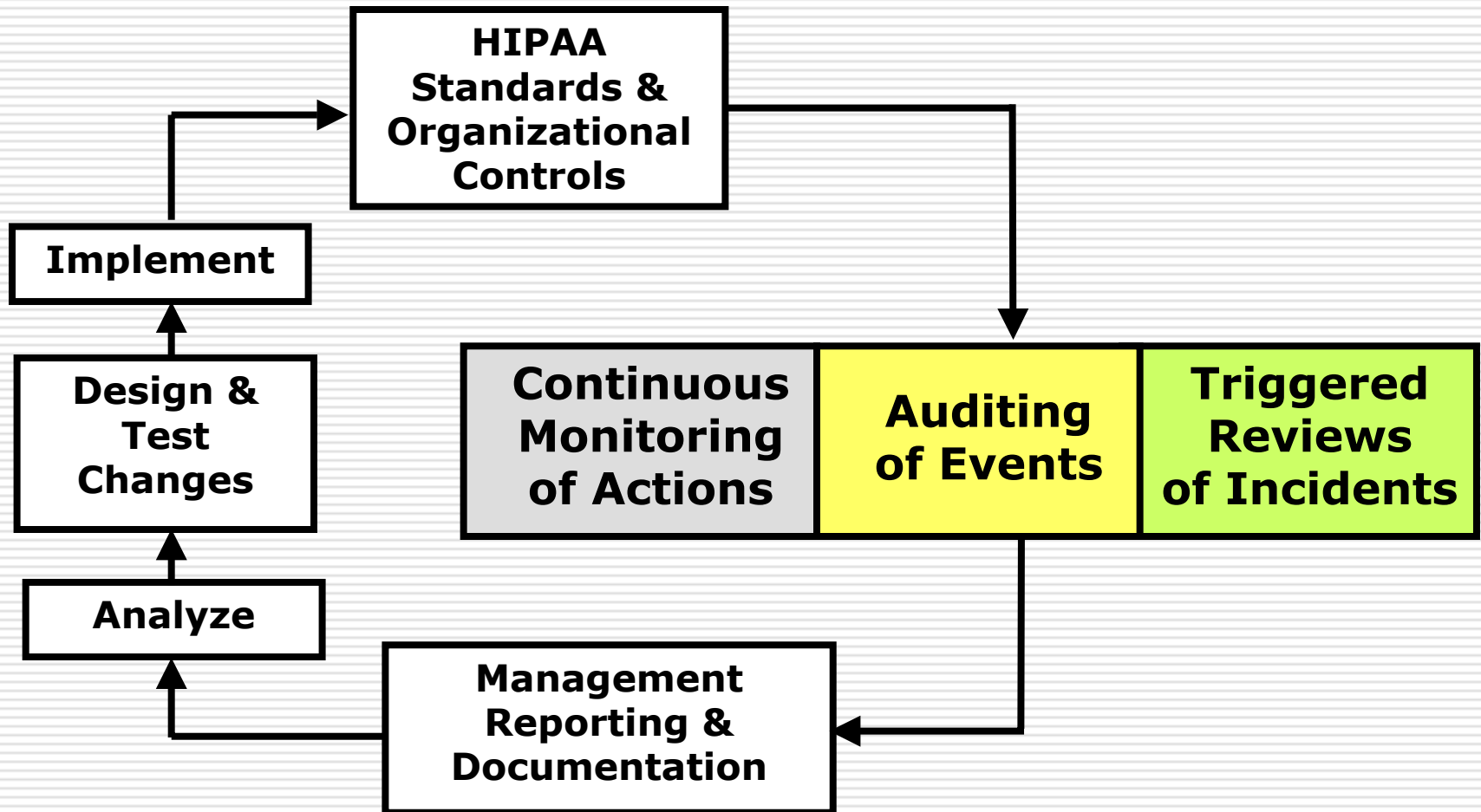
---

- 1. Rules & Regulations**  
**Policies & Procedures**  
**Training Materials**
- 2. Records: of Training**  
**Awareness Building**
- 3. Contracts**
- 4. Sensitive Findings**  
**Audit Trails**  
**Incident Reports**



# Compliance Assurance

---



# Compliance Assurance Plan

---

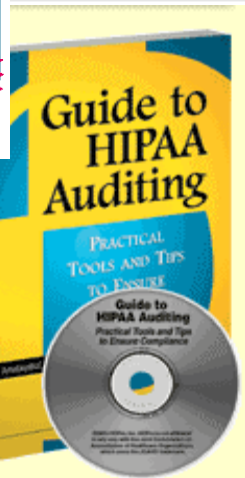
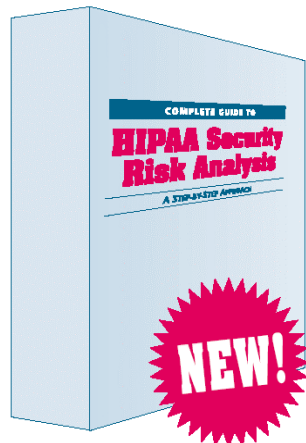
HIPAA Privacy and Security Compliance Assurance Plan	
Date of Plan:	Prepared by:
Compliance Goal:	
Standard(s):	
Owner(s):	
Risk:	
Current Control(s):	
Compliance Process(es):	
Schedule:	
Resources:	
Results:	
Recommendations:	
Follow up:	

# References & Resources

---

- **Required specifications and prioritization based on:**
  - **National Research Council, *For the Record: Protecting Electronic Health Information***
  - **[www.nap.edu](http://www.nap.edu)**
- **Significant reference to NIST Special Publications (SP) 800 Series documents:**
  - **<http://csrc.nist.gov/publications/nistpubs/>**
- **NIST certifying activities:**
  - **<http://www.niap.nist.gov>**
- **CMS IT Security – <http://cms.hhs.gov/it/security/References>**
- **WEDI – [www.wedi.org/snip](http://www.wedi.org/snip)**
- **SP 800-30, Risk Management Guide for Information Technology Systems, Chapters 3 and 4**
  - *Revision A DRAFT, Jan. 21, 2004*
- **SP 800-16, Information Technology Security Training Requirements, A role and performance based model**
- **SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems**
- **SP 800-33, Underlying Technical Models for Information Technology Security**
- **SP 800-26, Security Self-Assessment Guide for Information Technology Systems**
- **CMS Information Security Acceptable Risk Safeguards V1.1**

# References & Resources



[www.brownstone.com](http://www.brownstone.com)

- Amatayakul
- Lazarus

[www.hcpro.com](http://www.hcpro.com)

- Amatayakul

<https://catalog.ama-assn.org>

- Amatayakul
- Lazarus
- Walsh
- Hartley

# Contact Information

---

- **Margret Amatayakul, RHIA, CHPS, FHIMSS**  
Margret\A Consulting, LLC  
Schaumburg, IL  
[MargretCPR@aol.com](mailto:MargretCPR@aol.com)  
[www.margret-a.com](http://www.margret-a.com)
- **Steven S. Lazarus, PhD, FHIMSS**  
Boundary Information Group  
Denver, CO  
[SSLazarus@aol.com](mailto:SSLazarus@aol.com)  
[www.boundary.net](http://www.boundary.net)