HOLLAND&HART LLP


# HIPAA Security Rule: Risk Assessments

Matt Sorensen

# Disclaimer

This presentation is similar to any other legal education materials designed to provide general information on pertinent legal topics. The statements made as part of the presentation are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the speaker. This presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of law to your activities, you should seek the advice of your legal counsel.

# Source


1. Dept. of Health and Human Services, HIPAA Security Series, Volume 2, Paper 6: Basics of Risk Analysis and Risk Management, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf. Last accessed 12/19/2016.
2. https://www.healthit.gov/providers-professionals/security-risk-assessment. Last accessed 12/19/2016.

# HIPAA Security Rule

- 45 CFR 164.302-318
- 164.306 (General Requirements)
  - (a)(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
  - (a)(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
  - (a)(3) Protect against any reasonably anticipated uses or disclosures of such information

# HIPAA Security Rule

- 164.306 (General Requirements)
  - (b) Flexibility of Approach
    - Choose Security Measures That Are Reasonable & Appropriate
  - How do we know what is Reasonable & Appropriate?
    - size and complexity
    - technical infrastructure, hardware, and security capabilities
    - cost of security measures
    - probability and criticality of potential risks to ePHI
  - (c) Standards
  - (d) Implementation Specifications

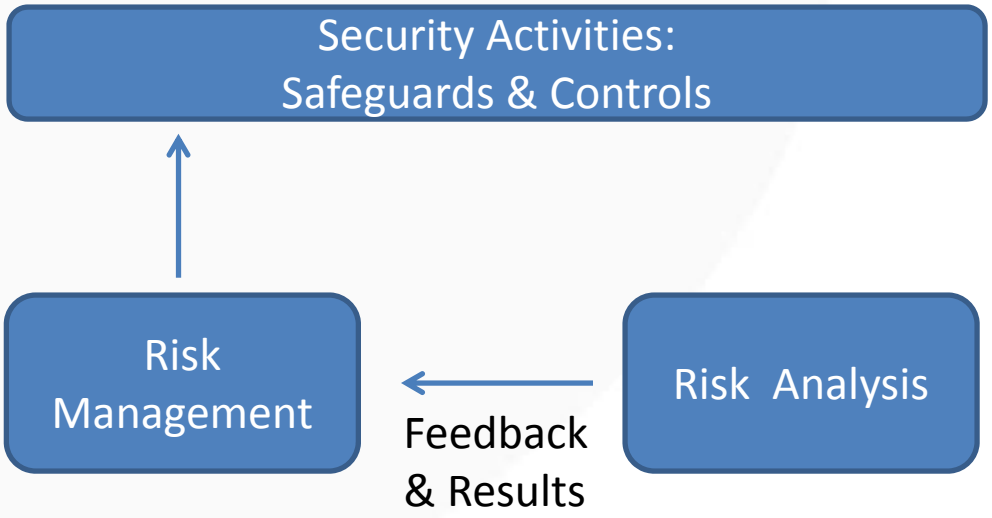
# HIPAA Security Rule

- 164.308 (Administrative Safeguards)
  - (a)(1)(i) Standard: Security Management Process
    - Implement policies and procedures to prevent, detect, contain, and correct security violations.
  - (a)(1)(ii) Implementation Specifications:
    - (ii)(A) Risk Analysis: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information.
    - (ii)(B) Risk Management: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

# HIPAA Security Rule - Documentation

- 164.316(B)(1)(ii): If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

# Risk Management & Analysis



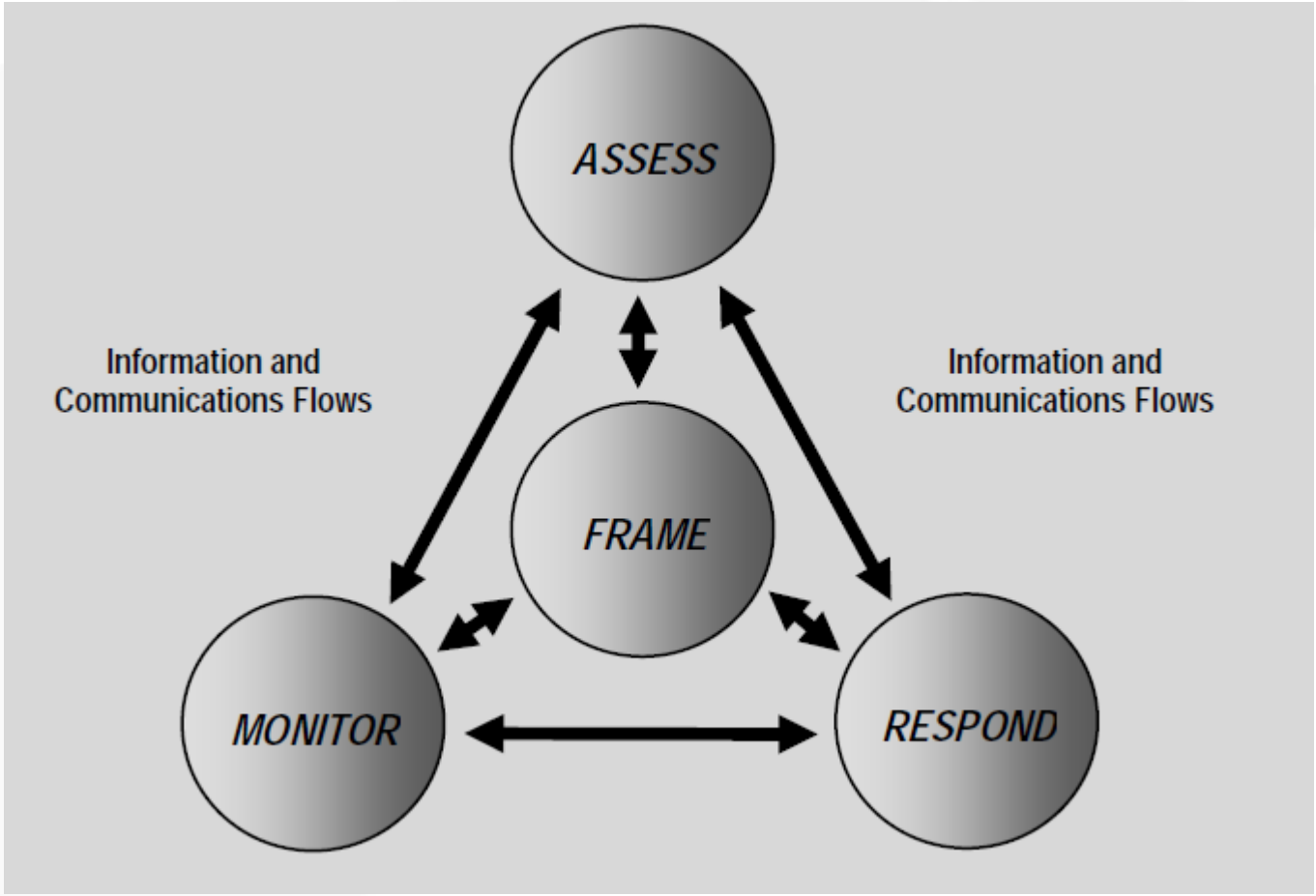
# NIST Standards

*"Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that organization's implementation activities. While NIST documents were referenced in the preamble to the Security Rule, this does not make them required. In fact, some of the documents may not be relevant to small organizations, as they were intended more for large, governmental organizations."* – Source: CMS FAQ on Security Rule.

# NIST Standards

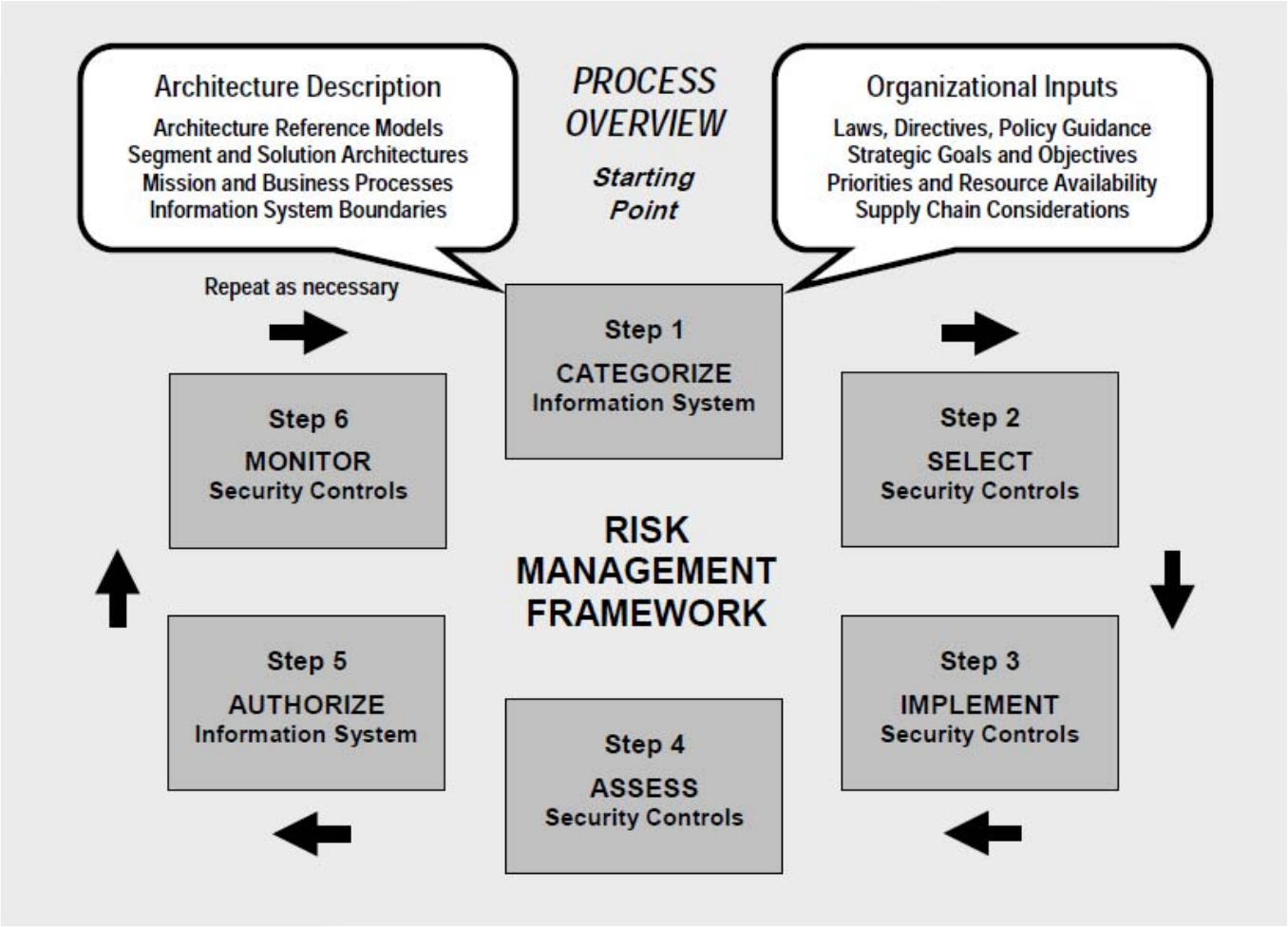
- 800-39: Managing Information Security Risk
- 800-37: Risk Management Framework
- 800-30: Risk Assessment

# NIST 800-39: Managing Information Security Risk




Source: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

# NIST 800-37: Risk Mgmt Framework




Source: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

# NIST 800-30: Risk Assessment

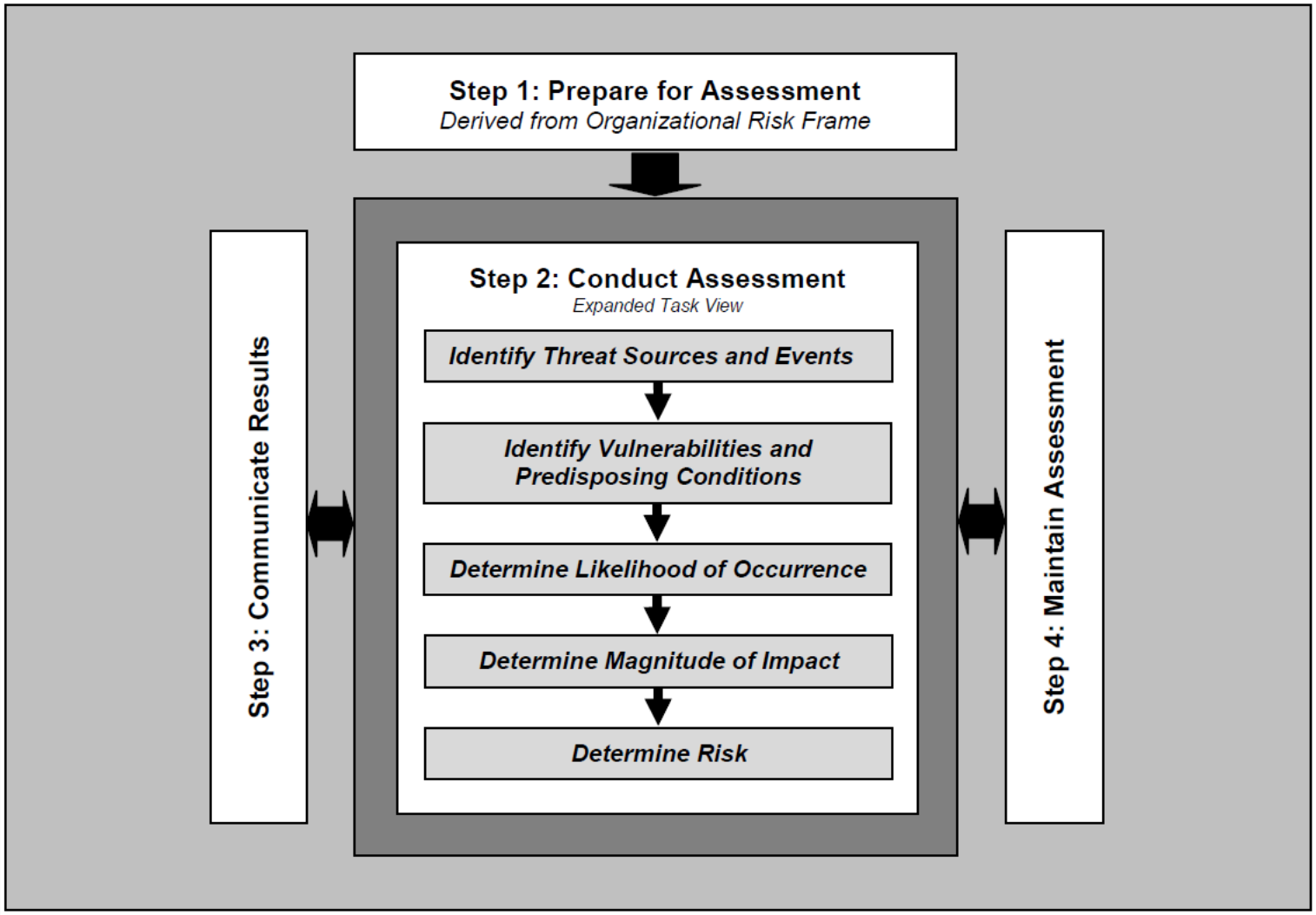
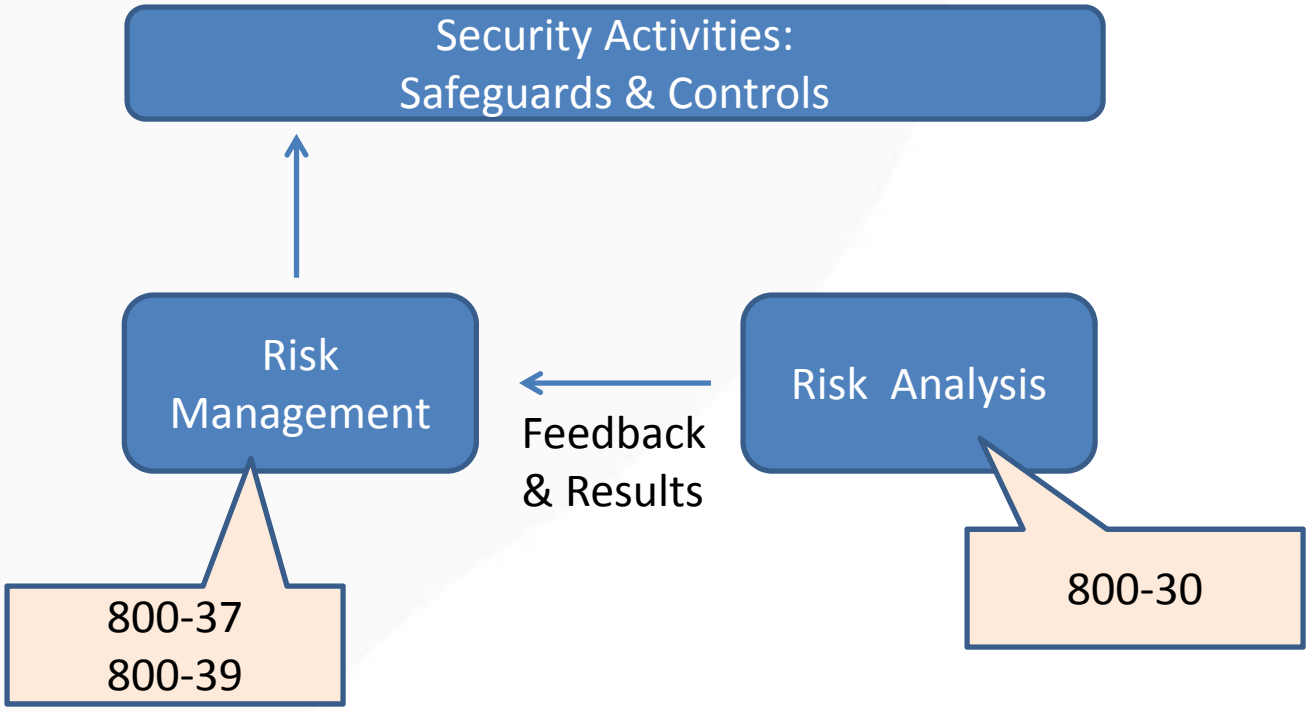



FIGURE 5: RISK ASSESSMENT PROCESS

Source: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

# Risk Management & Analysis



# Risk Definitions

- **Vulnerability:** *"[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised"*
- **Threat:** *"[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability."*
- **Risk:** *"The net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur.*

Source: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

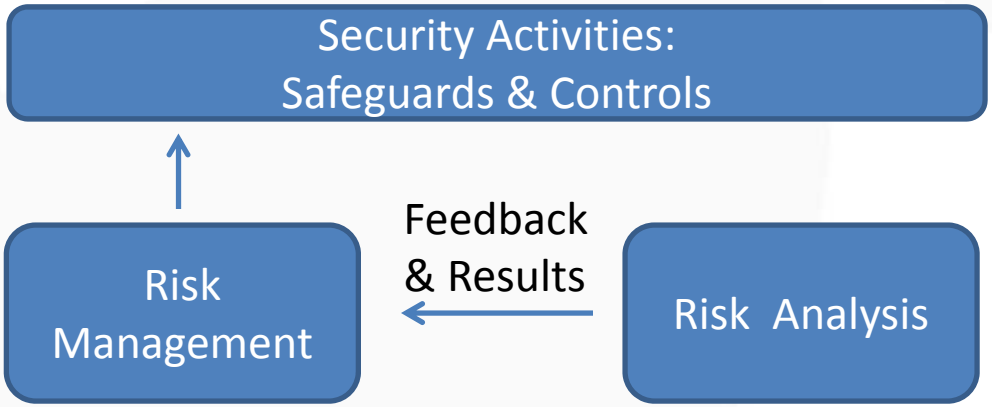
# Risk Definitions (Simplified)

- **Vulnerability:** a flaw or weakness.
- **Threat:** potential of a person or thing to exercise a vulnerability.
- **Risk:** The combination* of the likelihood and impact of a threat exploiting a vulnerability.
  - *Could also be:
    - function of
    - estimation of
    - cross-section of
    - calculation of
    - prognostication about
    - reasonable belief in, (based on experience, recent trends, and foreseeability)

# Risk Assessment Terms– Examples

- Threats -> Vulnerabilities = Risk
  - Threat Analysis
    - Human: intentional & unintentional
    - Natural: natural disaster
    - Environmental: power failures, chemical/pollutant
  - Vulnerabilities
    - in Technology: bugs, misconfiguration, inherent weakness
    - in People: social engineering, poor choices
    - in Process: defects, data handling

# Risk Management & Analysis




1. Administrative
2. Physical
3. Technical

1. Develop and implement a risk management plan.
2. Implement security measures.
3. Evaluate and maintain security measures.

1. Identify the scope of the analysis.
2. Gather data.
3. Identify and document potential threats and vulnerabilities.
4. Assess current security measures.
5. Determine the likelihood of threat occurrence.
6. Determine the potential impact of threat occurrence.
7. Determine the level of risk.
8. Identify security measures and finalize documentation

# Risk Analysis Steps

Risk Analysis

1. Identify the scope of the analysis
2. Gather data
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Identify security measures and finalize documentation

# Risk Analysis Steps

Risk Analysis

1. Identify the scope of the analysis
2. Gather data
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Identify security measures and finalize documentation

# Risk Assessment - Scope

- Includes potential risks and vulnerabilities to:
  - confidentiality,
  - availability, and
  - integrity of
- all ePHI that a covered entity creates, receives, maintains, or transmits.
- Includes ePHI in all forms of electronic media:
  - storage
  - network transmission

# Risk Analysis Steps

Risk Analysis

1. Identify the scope of the analysis
2. Gather data
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Identify security measures and finalize documentation

# Risk Assessment - Techniques

- Gather Data
  - Inventory of ePHI
  - Inventory of Systems
    - Workstations
    - Laptops
    - Mobile Devices
    - Servers and Databases
  - Interviews, Documentation, Past Projects

# Risk Analysis Steps

Risk Analysis

1. Identify the scope of the analysis
2. Gather data
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Identify security measures and finalize documentation

# Risk Assessment - Techniques

- Threats -> Vulnerabilities = Risk
  - Threat Analysis
    - Human: SKRAAMO
      - nation state
      - organized crime
      - hacktivist
      - opportunist
      - insider threats
    - Natural: regional occurrences
    - Environmental: proximity to industry

# Risk Assessment - Techniques

- Threats -> Vulnerabilities = Risk
  - Vulnerability Management: Find & Fix
    - in Technology: Scan, Review
    - in People: Assess Knowledge, Practices
    - in Process: Audit, Design, Effectiveness

# Risk Analysis Steps

Risk Analysis

1. Identify the scope of the analysis
2. Gather data
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Identify security measures and finalize documentation

# Risk Assessment – Assess Safeguards

- Safeguards (Controls)
- Preventive, Corrective, Detective
- Manual, Automated, Hybrid
- Test of Design
  - Is the safeguard designed properly to detect what it purports to detect?
- Test of Effectiveness
  - Inspect, Duplicate, Feed known bad events, Sample

# Risk Analysis Steps

Risk Analysis

1. Identify the scope of the analysis
2. Gather data
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Identify security measures and finalize documentation

# Risk Assessment

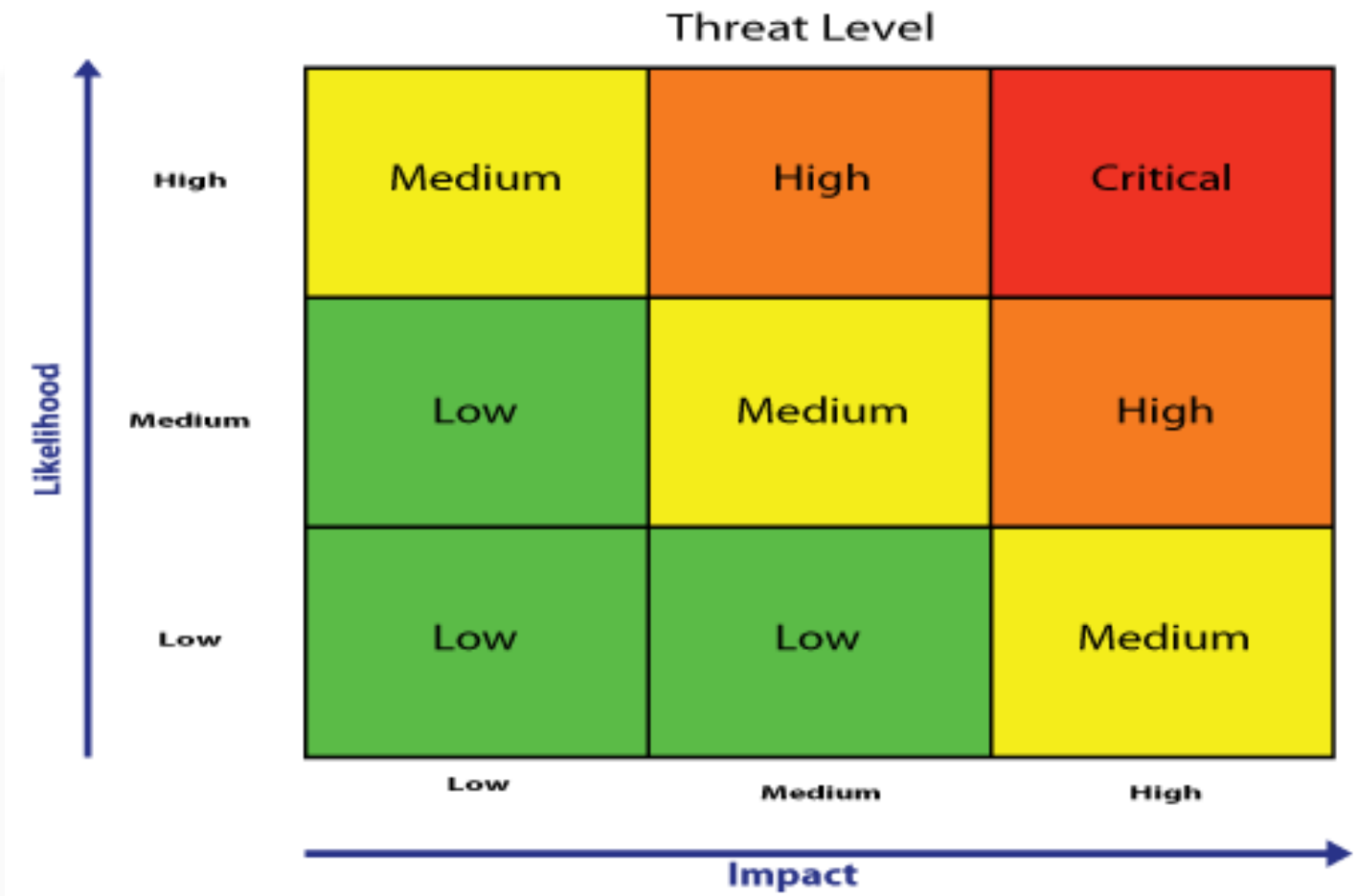
- Threats -> Vulnerabilities = Risk
  - Impact
    - L/M/H
    - Dollar Amount
      - Cost per breached record
      - Cost of breach, # of records
    - Score
  - Likelihood
    - L/M/H
    - Quantitative vs. Qualitative

# Risk Assessment – Probability

- Wall Street Quants
- Wired Magazine Cover 3/09
- Reminder:
  - we are tasked with foreseeing "reasonably anticipated" threats and hazards, uses and disclosures
  - addressing those with reasonable and appropriate safeguards


- https://www.wired.com/2009/02/wp-quant/
- http://archive.wired.com/wired/issue/17-03

# Risk Level




Source: http://the-outsourcing.com/subpage.php?pn=region&regid=1&aid=274

# Action Plans

- Critical
  - Item 1
    - Solution
    - Cost
    - Due Date
  - Item 1
    - etc.
- High
  - Item 3
    - Solution
    - Cost
    - Due Date
  - Item 4
- Medium
  - etc.
- Low
  - etc.

# Risk Assessment

- What is not considered a risk assessment:
  - Gap Assessment against the implementation specifications
  - A list of threats and corresponding safeguards
  - follow all the steps
  - show deliberation in:
    - identifying all ePHI
    - completing inventories
    - threat identification, likelihood and impact analysis

# Risk Assessment

- **Common Mistakes:**
  - **Failure to account for Third-Party Risk**
    - **SAAS, Cloud, Business Associates**
    - **Right to audit, over-reliance in absence of SOC 2**
    - **Misunderstanding of SOC 1 vs. SOC 2 reports**
  - **Failure to complete and inventory of ePHI and systems**
  - Not conducting a risk assessment as defined, opting for gap analysis
  - No risk assessment at all!
  - No minutes of board deliberations, management action

# Risk Assessment Tool

- Security Risk Assessment Tool
  - HealthIT.gov
  - Windows and iPad version
  - Paper versions
  - User guide
  - No guarantee of compliant results

Source: https://www.healthit.gov/providers-professionals/security-risk-assessment-tool

# Action Items: 30-90-180

- When you return to work
  - Identify when your next risk assessment is due
  - Review last risk assessment
  - Identify shortcomings, gaps
- 30 days:
  - Discuss noted shortcomings with management
  - Assign accountable party to plan for upcoming risk assessment to address observed weaknesses
- 90 days:
  - Complete inventory of: ePHI, storage media, transmission, and systems and endpoints
- 180 days:
  - Conduct an improved risk assessment

HOLLAND&HART LLP


# Thanks for Participating

**Kim Stanger**
kcstanger@hollandhart.com

**Matt Sorensen**
cmsorensen@hollandhart.com