Building a Risk Management Framework for HIPAA & FISMA Compliance

Anurag Shankar
Center for Applied Cybersecurity Research
Indiana University

2015 Technology Exchange
October 6, 2015
Outline

1. Introduction
2. HIPAA & FISMA Demystified
3. Cyber Compliance: The IU Approach
4. Building & Leveraging a Risk Management Framework
5. Conclusion
1. Introduction
Why a talk on compliance?

• We have a new user community - clinical researchers.
  • Their research IT are growing to HPC, HPN, and HPS* scales.
  • Medical school IT cannot keep up.
  • Their data is laced with regulations (HIPAA, FISMA).

• Compliance is a foreign language (to most of us).
  • We deal with the usual suspects – physical scientists and engineers.
  • Regulations are not our forte.

* High performance computing, networking and storage
Compliance challenges

• Fear, uncertainty, doubt.
• Language barrier.
• Lack of resources.
• Local risk tolerance.
• Risk ownership.
• Policy.
The goals this morning

• Learn to speak compliance.
• Bring regulations to a practical, actionable plane.
2. Regulations - HIPAA and FISMA
HIPAA
What is HIPAA?

• **Health Insurance Portability & Accountability Act.**

• Provides the ability to transfer and continue health insurance coverage for American workers and their families when they change or lose their jobs.

• Enforced by the Office for Civil Rights (OCR) in the U.S. Department of Health & Human Services (HHS).
HIPAA Timeline


• The Health Information Technology for Economic & Clinical Health (HITECH) Act of 2006.

• The HIPAA Omnibus Final Rule of 2013 included provisions from HITECH & the 2008 Genetic Information Nondiscrimination Act (GINA).
Is HIPAA all about patient privacy?

• No. There are many other components.
• Privacy is addressed through the HIPAA Privacy Rule, the HIPAA Security Rule, and breach notification requirement.
  • The Privacy Rule defines who HIPAA applies to (a covered entity), what is protected (protected health information or PHI), and covers disclosures of PHI.
  • The Security Rule focuses exclusively on protecting electronic PHI (ePHI) in any form – at rest, in transit, under analysis, etc.
What constitutes PHI*?

Patient information in any form (paper, verbal, electronic) containing any of the following 18 identifiers:

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web universal resource locators (URLs)
15. Internet protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic or code

PHI, when properly de-identified, is no longer subject to HIPAA

* You may also hear the terms personally identifiable information (PII), individually identifiable health information (IIHI), health information, etc., but they are not created equal.
Is all identifiable health information PHI?

• No, only when it is within the healthcare context.

• For instance,
  • identifiable health information (yours or someone else’s) you share publicly on Facebook is not PHI (it is not subject to HIPAA).
  • However, if a medical professional (doctor, nurse, etc.) shares it publicly on Facebook, it is PHI and thus subject to HIPAA. Such a disclosure would be considered a breach under HIPAA.
Who does HIPAA apply to?

- A HIPAA covered entity (CE).
- Only healthcare providers, health plans, and health clearinghouses are considered covered entities.
- Universities are often hybrid covered entities, meaning they have both non-covered (e.g. the English dept.) and covered components (e.g. the Student Health Center, School of Medicine).
- HIPAA applies to the entire CE (the legal entity). It is the CE that faces penalties when a HIPAA violation occurs, not its employees or subunits.
Does HIPAA apply to me?

• Yes, if you serve a covered entity,
  • either as a unit of your covered entity or
  • as a Business Associate, AND
  • you create, receive, transmit, or maintain PHI.

• You cannot say “I didn’t know we had PHI”. Plausible denyability can be quite expensive under HIPAA.

• Your organization is not a covered entity if it is not involved in healthcare operations directly.

Check with your compliance folks or counsel
What is a Business Associate (BA)?

• A “a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.”

• However, there is a “conduit exception” which excludes ”... those entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers (ISPs) providing mere data transmission services.”
Business Associate Agreements

• HIPAA mandates you to have a Business Associate Agreement (BAA) with BAs (since it’s a disclosure of PHI). The BAs must have BAAs with their BAs, and so on.

• The BAA must include language stating that the BA will protect your PHI and abide by HIPAA. (Sample BAAs are at HHS site.)

• You are expected to do due diligence to ensure that the BA can protect your PHI as per HIPAA.

• The BAs are subject to HIPAA independently if they have PHI. So are their BAs, all the way down the chain.
Breach Notification

• HIPAA mandates a breach of PHI to be reported to the OCR & those affected within 60 days.
• For breaches involving > 500 individuals, local media outlets must also be notified.
• It is for you to decide whether a security incident rises to the level of a breach.
Enforcement

• HIPAA violations can result in civil monetary penalties against a covered entity and/or criminal penalties against individuals, with imprisonment up to 10 years.

• An audit may occur if there is a breach. However, a breach is not automatically a HIPAA violation.

• Audits used to occur only in response to a breach or a complaint. The OCR has received funding to institute a random audit program now. They are getting ready for the first round of such audits.
When is a breach a HIPAA violation?

Violations occur when the CE is not doing due diligence required under HIPAA or ignoring HIPAA altogether:

- Not responding to the OCR despite repeated requests.
- Having no information security process whatsoever.
- No risk assessment and mitigation.
- No incident response.
- No documentation.
- Not following documented policies and procedures.

The OCR expects breaches; that is not the point
## Civil Monetary Penalties

A breach of 100 patient records = 100 violations

A maximum “Did Not Know” cost of a breach of 100 patient records = $50K x 100 = $5 million!

### Table: Civil Monetary Penalties

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation For violations occurring before 2/18/2009</th>
<th>Each Violation For violations occurring on or after 2/18/2009</th>
<th>All Identical Violations Per Calendar Violations Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>Up to $100</td>
<td>$100 - $50,000</td>
<td></td>
</tr>
<tr>
<td>Reasonable Cause*</td>
<td>Up to $100</td>
<td>$1000 - $50,000</td>
<td></td>
</tr>
<tr>
<td>Willful Neglect - Corrected</td>
<td>Up to $100</td>
<td>$10,000 - $50,000</td>
<td>$25,000</td>
</tr>
<tr>
<td>Willful Neglect - Not Corrected</td>
<td>Up to $100</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

* = An act of omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification (HIPAA) provision, but in which the covered entity or business associate did not act with willful neglect.

The cost of “I didn’t know we had PHI”.

---

- **Civil Monetary Penalties**
- **Violation Category**
- **Each Violation**
- **All Identical Violations Per Calendar Violations Year**
- **Did Not Know**
  - For violations occurring before 2/18/2009: Up to $100
  - For violations occurring on or after 2/18/2009: $100 - $50,000
- **Reasonable Cause**
  - For violations occurring before 2/18/2009: Up to $100
  - For violations occurring on or after 2/18/2009: $1000 - $50,000
- **Willful Neglect - Corrected**
  - For violations occurring before 2/18/2009: Up to $100
  - For violations occurring on or after 2/18/2009: $10,000 - $50,000
- **Willful Neglect - Not Corrected**
  - For violations occurring before 2/18/2009: Up to $100
  - For violations occurring on or after 2/18/2009: $50,000

---

**Maximum “Did Not Know” cost of a breach of 100 patient records = $50K x 100 = $5 million!**

**Civil Monetary Penalties**

- **Did Not Know**
  - For violations occurring before 2/18/2009: Up to $100
  - For violations occurring on or after 2/18/2009: $100 - $50,000

---

**Reasonable Cause**

- For violations occurring before 2/18/2009: Up to $100
- For violations occurring on or after 2/18/2009: $1000 - $50,000

---

**Willful Neglect**

- Corrected
  - For violations occurring before 2/18/2009: Up to $100
  - For violations occurring on or after 2/18/2009: $10,000 - $50,000

- Not Corrected
  - For violations occurring before 2/18/2009: Up to $100
  - For violations occurring on or after 2/18/2009: $50,000
Enforcement in Action

- **Group slapped with $6 penalty**

- **WellPoint to pay $1.7 million HIPAA**

- **$400,000 Penalty in HIPAA Case**
  - Idaho State University Cited After Breach Investigation

- **Another Big Fine After a Small Breach**
  - HIPAA Investigation Leads to Sanctions

- **Stanford reports fifth big HIPAA breach**
  - Stolen laptop at children's hospital compromises PHI of 13,000

- **On further review, $4.3 million Cignet HIPAA fine not a big surprise**

- **Alaska settles HIPAA security case for $1,700,000**

- **Walgreens must pay woman $1.44 million over HIPAA violation**

- **New York-Presbyterian, Columbia to pay largest HIPAA settlement: $4.8 million**

- **HIPAA Breaches in the Cloud**

- **$4.8M HIPAA Fine Part Of Wider HHS Crackdown**
  - HHS attorney predicts big year for HIPAA fines

- **Tenet employee charged with theft, HIPAA violations**

- **HIPAA Violation Indictments for 2 Medical Office Assistants**
  - United States Attorney and U.S. Secret Service announced indictment of twelve individuals in a
    - United States Attorney and U.S. Secret Service announced indictment of twelve individuals in a
Breaches reported by universities

The penalties are bad; reputational damage is worse
What does HIPAA mean for an IT provider?

• To protect ePHI as per the HIPAA Security Rule.
The HIPAA Security Rule

• The Security Rule requires 1. Administrative, 2. Physical, and 3. Technical safeguards to
  • Ensure the confidentiality, integrity, and availability of all ePHI created, received, maintained or transmitted;
  • Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  • Protect against reasonably anticipated, impermissible uses or disclosures;
  • Ensure compliance by the workforce; and
  • Provide a means for managing risk in an ongoing fashion.
Security Rule Safeguards

• **Administrative** – security management/officer, workforce security, incident response, disaster planning, evaluations, etc.

• **Physical** – facilities access, workstation use/security, device/media controls, etc.

• **Technical** – access/audit control, integrity, authentication, transmission security, etc.

+ organizational/policies/documentation requirements
Required and Addressable

• The Security Rule safeguards are either required or addressable.
• Required = what it says.
• Addressable = must be in place, but ok if you explain why you don’t have it in place and/or how you will otherwise address the risk.
HIPAA Safe Harbor

• If the data is encrypted at rest and the encryption key is stored separately from the data and secured, a breach need not be reported to the OCR.

• This is called HIPAA safe harbor.
Can I be certified HIPAA compliant?

• No, HIPAA doesn’t define a threshold where you are suddenly compliant.
• The OCR has not authorized anyone to certify compliance.
• You can get third party certification but the OCR does not recognize them. They may still find you lacking.
• All you can do is exercise due diligence - continuously assess and mitigate risk. HIPAA compliance is either self asserted or blessed by local authorities.
How do I handle HIPAA then?

• Based on your environment, budget, and risk tolerance.
• Check if your local HIPAA Compliance or Information Security folks already have a process in place or have recommendations. Use their expertise.
• Securing the ePHI and documentation is still your task.
What is FISMA?


“Each federal agency shall develop, document, and implement an agency wide information security program to provide information security for the information and information systems that support the operations and assets of the agency ...”
Who does FISMA apply to?

• Government agencies, their subcontractors, or other sources that serve the agencies.
When does FISMA apply?

• When you use agency systems to manage information on behalf of an agency.
• When you use or operate information systems on behalf of an agency.
• If your contract says it does.
HHS guidance

“FISMA's requirements follow agency information into any system which uses it or processes it on behalf of the agency. That is, when the ultimate responsibility and accountability for control of the information continues to reside with the agency, FISMA applies.”

• The term "on behalf of" indicates that only those entities that are acting, under agency principles, as agents, where HHS (or a component) is the principal, are covered by FISMA.
Does FISMA apply to me?

- Probably, if you have a contract with a govt. agency, e.g. NIH.
- Check the contract; it will explicitly state FISMA requirements.
- Check if FISMA language has been added to existing contracts when they are renewed.
- It is sometimes possible to negotiate FISMA out.
What does FISMA require?

• Adopting the NIST Risk Management Framework (RMF).
• Accreditation.
• Regular reporting and reviews.
The FISMA Workflow

Define system boundaries

Assess Risk (NIST 800-30, 37, 39)

Apply Controls (NIST 800-53)

Evaluate Controls (NIST 800-53A)

Authority to Operate (ATO)
Define System Boundaries

• Also known as the accreditation boundaries.
• Defines where the “system” begins and ends.
• A system can be a part of a network, an application, a logical collection of disparate components, etc.
• A conceptual boundary extends to all direct and indirect users of the system that receive output.
• Requires IT professionals.
Assess Risk

- Guidance from NIST documents NIST 800-30, 37, and 39 is used to conduct a risk assessment.
- Individual risks and severity are identified.
- A prioritized list of risks is created.
Select Controls

• The results of the risk assessment and the NIST control catalog NIST 800-53 are used to select controls that mitigate risk.

• Existing controls will mitigate some of the risk. Residual risk is addressed by adding missing controls.

• The FISMA contract will specify the required security control baseline (High, Medium, or Low).
Evaluate Controls

• Requires regular assessments.
• Involves testing the controls in place to gauge their effectiveness in mitigating risk.
• Evaluations can be internal or external.
• The NIST 800-53A document covers evaluating NIST 800-53 controls.
Authority to Operate (ATO)

• The compliance paperwork is submitted to the agency.
• An ATO letter is issued by the agency authorizing the operation of the system.
• If remediation is required, the agency may issue an Interim Authority To Operate (IATO) with a defined end date.

+ continuous monitoring and regular reporting requirements.
What does it take to do FISMA?

- A significant amount of effort and $$.  
- Duke Medicine, one academic FISMA implementation, estimates that, for each PI contract, it takes them ~25 hours to review all the documentation, make suggested contractual changes for agency negotiation, and create a FISMA management plan. 
- A separate budget line item has to be included in the contract to cover FISMA costs. 
- Many use a completely walled garden.
3. Cyber Compliance: The IU Approach
History

• IU has a mature research cyberinfrastructure (CI), serving both local and national users.

• It is provisioned through IU’s central IT organization.

• It delivers supercomputing, data storage/archival, visualization, application development & optimization, data management, etc.

• Prior to 2000, it was used almost exclusively by the usual suspects - physical scientists and engineers.
HIPAA intervenes

• A Lilly Endowment grant in 2000 to accelerate genomics research at IU included using the existing CI for IU School of Medicine researchers.
• HIPAA compliance for research systems became a requirement.
• Forced us to learn HIPAA and how it affects the research workflow.
The most important compliance step

• We created an oversight committee to oversee our HIPAA effort and put every stakeholder on it – the Compliance Officers, Counsel, CISO, School of Medicine faculty/IT staff/CIO, Central IT senior management, etc.

• They became our ambassadors and started sending clinical researchers, NIH grant money, reflected glory our way.
Research workflow & compliance

It was useful to follow the research data end to end, through its entire lifecycle to understand where compliance touches it.

Steps in red involve compliance.

Pre-Grant
- Prelim. Investigation
- IRB
- CI Design

Proposal
- Proposal Preparation
- Budget Preparation
- Proposal Funding

Execution
- Data Acquisition
- Data Analysis
- Simulation
- Data Management
- Data Sharing
- Data Visualization
- Data Publishing

Post-Grant
- Data Archival
- Data Disposal
Evolution

• We initiated a HIPAA specific, homegrown compliance process in 2008.
• It worked well initially, but was too rigid to accommodate other rules and regulations appearing on the horizon (e.g. FISMA).
• This motivated search for a standards based, regulation neutral process.
• The obvious choice was the widely used, highly flexible NIST standard.
• Resulted in the creation of a single, reusable framework for cyber compliance in general.
How does it work?

1. Establish the base NIST Risk Management Framework (RMF)
2. Align with the NIST standard (not individual regulation)
3. Map the regulation to NIST
4. Add missing* regulatory controls

This allows scaling laterally to cover any regulation or potential regulation changes; all that changes are steps 2 and 3

* Regulatory controls missing from NIST
Handling HIPAA

1. Align with the NIST low security baseline
2. Map HIPAA to NIST using NIST 800-66
3. Add HIPAA safeguards missing from NIST
## HIPAA to NIST Mapping (from NIST 800-66)

|-------------------------------|------------------------------|------------------------------|------------------------------------------|-----------------------------|
| 164.308(a)(1)(i)              | Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations. | Risk Analysis (R): 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. | RA-1 | FIPS 199  
NIST SP 800-14  
NIST SP 800-18  
NIST SP 800-30  
NIST SP 800-37  
NIST Draft SP 800-39  
NIST SP 800-42  
NIST SP 800-53  
NIST SP 800-55  
NIST SP 800-60  
NIST SP 800-84  
NIST SP 800-92  
NIST SP 800-100 |
| 164.308(a)(1)(ii)(A)          |                              | Risk Management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | RA-2, RA-3, RA-4, PL-6 | |
| 164.308(a)(1)(ii)(B)          |                              | Sanction Policy (R): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. | PS-8 | |
| 164.308(a)(1)(ii)(C)          |                              | Information System Activity Review (R): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | AU-6, AU-7, CA-7, IR-5, IR-6, SI-4 | |
| 164.308(a)(1)(ii)(D)          |                              |                              | CA-4, CA-6 | |
| 164.308(a)(2)                 | Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. |                              | CA-4, CA-6 | |
4. Building and Leveraging the NIST Risk Management Framework
What is managing cyber risk?

• Identify, assess, prioritize, and mitigate risk to assets on an ongoing basis.
• Focuses on risk, calculated as follows.
  \[
  \text{Risk} = \frac{\text{Threat/Vulnerability} \times \text{Likelihood}}{\text{Impact}}
  \]
• So a big threat from an existing vulnerability that is highly unlikely to be exploited/has little impact is low risk. You don’t kill yourself over it.
• Risk assessment sharply focuses attention and optimizes resources.
Aren’t firewalls, encryption, etc. enough?

• No. Technical controls are only one component of cyber risk management. It requires a more holistic approach.

• Why not encrypt it all at rest and have HIPAA safe harbor? Because it’s not always possible, and you still have to protect the key server.

• The NIST risk management framework gives us precisely that.
The NIST RMF

• Comprises of the following:

  • **Good governance** = institutional security organization, policies, sanctions, enforcement
  • **Risk management** = assessment, mitigation through appropriate physical, administrative, technical controls
  • **Review** = regular monitoring, reviews, assessment, and mitigation
  • **Awareness and training**
  • **Documentation**
NIST Security Lifecycle

RISK MANAGEMENT FRAMEWORK
Security Life Cycle

Starting Point
FIPS 199 / SP 800-60

SP 800-37 / SP 800-53A

MONITOR
Security Controls

SP 800-37

AUTHORIZE
Information System

SP 800-53A

ASSESS
Security Controls

SP 800-70

IMPLEMENT
Security Controls

FIPS 200 / SP 800-53

SELECT
Security Controls

SP 800-53 / SP 800-30

SUPPLEMENT
Security Controls

SP 800-18

DOCUMENT
Security Controls
But I don’t have resources to do all that

• You likely have some or all of these:
  • An information security office
  • Institutional IT policies
  • Many security controls already in place
  • Documentation

• This is plenty to start with. It means that you have the basic elements of the NIST RMF in place already.

• The rest is a one-time effort to establish the RMF. Much of it is documentation.

• A risk assessment enables further economies.
Risk Assessment

• The beginning of the road in cyber risk management. You cannot manage risk unless you know what risk you have.

• There are many ways to assess risk, ranging all the way from pedestrian (& cheap) to highly complex (& expensive).

• Your effort should be commensurate with budget, risk tolerance, and organizational complexity.
Implementation Steps

1. Assign Resources
2. Develop tools
3. Develop process
4. Apply process to new systems
5. Migrate existing systems to new process
Develop process

1. Inventory
2. Documentation of System & Controls
3. Risk Assessment
4. Risk Response
5. Awareness & Training
6. Oversight & Approval
7. Authority to Operate
8. Ongoing Risk Management
Inventory what you have

• System details, ePHI location, security settings, BAAs, scan info, access methods, disposal information, etc.
• Software, version, patch level, BAAs, scan info, etc.
• Privileged access inventory - names, roles, dates authorized, etc.
• Incident log – incident summary, response.
### System Inventory

<table>
<thead>
<tr>
<th>System</th>
<th>Location</th>
<th>Prod/Test</th>
<th>HW</th>
<th>PII Location</th>
<th>HW Maint/Contract?</th>
<th>HIPAA BAA/137?</th>
<th>OS</th>
<th>Version</th>
<th>Highest Data Classification</th>
<th>Critical Data Category</th>
<th>HIPAA Aligned?</th>
<th>Access Method</th>
<th>Directly by End Users?</th>
<th>End User Facing Applications</th>
<th>Authen. Methods</th>
<th>Open Host Ports</th>
<th>Data Center Firewall Allows Ports</th>
<th>Host Firewall Allows Ports</th>
<th>Last Host Scan &amp; Result</th>
<th>Retire Date &amp; How Disposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>system1</td>
<td>site-1.edu</td>
<td>P</td>
<td>Dell PowerEdge 3000X</td>
<td>Avantel NetworkInc</td>
<td>Yes</td>
<td>No</td>
<td>RHEL</td>
<td>8.4</td>
<td>Critical</td>
<td>ePHI</td>
<td>No</td>
<td>Active Directory</td>
<td>Not identified</td>
<td>Active Directory</td>
<td>80, 22-443</td>
<td>80, 443</td>
<td>22, 80, 443</td>
<td>1/10/2014, Clean</td>
<td>1/2/03, Storage media removed and destroyed</td>
<td></td>
</tr>
<tr>
<td>system2</td>
<td>site-2.edu</td>
<td>II</td>
<td>Dell PowerEdge 3000X</td>
<td>Avantel NetworkInc</td>
<td>Yes</td>
<td>No</td>
<td>RHEL</td>
<td>8.4</td>
<td>Critical</td>
<td>ePHI</td>
<td>No</td>
<td>Active Directory</td>
<td>Not identified</td>
<td>Active Directory</td>
<td>80, 22-443</td>
<td>80, 443</td>
<td>22, 80, 443</td>
<td>1/10/2014, Clean</td>
<td>1/2/03, Storage media removed and destroyed</td>
<td></td>
</tr>
</tbody>
</table>

### Software Inventory

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>system1</td>
<td>Apache</td>
<td>2.4</td>
<td>N</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>AD</td>
<td></td>
</tr>
<tr>
<td>system1</td>
<td>MySQL</td>
<td>5.6</td>
<td>N</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>system1</td>
<td>Java</td>
<td>7.1</td>
<td>N</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

### Incident Log

<table>
<thead>
<tr>
<th>Name</th>
<th>Incident Date</th>
<th>Software Exploited</th>
<th>Vulnerabilities</th>
<th>Incident Details</th>
<th>How Detected?</th>
<th>Date ISO Notified</th>
<th>How Responded?</th>
<th>ISO ATO Issued on</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1/2/14</td>
<td></td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>ISO ATO issued</td>
<td>Patch XXXX applied</td>
<td>1/10/14</td>
</tr>
</tbody>
</table>

### Privileged Access Inventory

<table>
<thead>
<tr>
<th>System</th>
<th>Name</th>
<th>Access Authorized</th>
<th>Type of Access</th>
<th>Access Terminated</th>
</tr>
</thead>
<tbody>
<tr>
<td>site-1</td>
<td>Name1</td>
<td>1/10/2010</td>
<td>System Administrator</td>
<td></td>
</tr>
<tr>
<td>site-1</td>
<td>Name2</td>
<td>1/10/2010</td>
<td>System Administrator</td>
<td></td>
</tr>
<tr>
<td>site-1</td>
<td>Name3</td>
<td>1/1/12</td>
<td>System Administrator</td>
<td></td>
</tr>
<tr>
<td>site-1</td>
<td>Name4</td>
<td>1/1/12</td>
<td>System Administrator</td>
<td></td>
</tr>
<tr>
<td>site-1</td>
<td>Name5</td>
<td>1/1/12</td>
<td>System Administrator</td>
<td></td>
</tr>
</tbody>
</table>

The inventory template
Document the system and controls

• Controls are documented in the System Security Plan or SSP.
• IU template based on what DHHS, NASA, etc. use to satisfy FISMA.
• Describes system name, categorization, contacts, purpose, components, interconnections, boundaries, dependencies, and all NIST 800-53 security & privacy controls in place.
1 SYSTEM CHARACTERIZATION

1.1 System Name

The system name is "SSP" or "System Name" is a unique identifier for the system that is required to be documented in the SSP template.

1.2 System Type

The system type is "SSP" or "System Type" is a description of the type of system, such as "Data Center" or "Network Infrastructure".

1.3 System Categorization

The system categorization is "SSP" or "System Categorization" is a description of the level of sensitivity or criticality of the system, such as "Low," "Medium," or "High."

1.4 System Environment

The system environment is "SSP" or "System Environment" is a description of the operating environment, such as "Data Center" or "Remote Access." The SSP template should include the environment in which the system is housed.

1.5 System Status

The system status is "SSP" or "System Status" is a description of the current status of the system, such as "Operational," "Under Development," or "Discontinued." The SSP template should include the status of the system.

1.6 Information Contacts

The information contacts are "SSP" or "Information Contacts" are the individuals responsible for providing information about the system, typically including the system owner, system administrator, and contact information.

1.7 General Description / Purpose

The general description or purpose is "SSP" or "General Description / Purpose" is a brief description of the system's function, such as "Manage access to sensitive data" or "Support customer service requests." The SSP template should include a brief description of the system's purpose.

1.8 System Environment

The system environment is "SSP" or "System Environment" is a description of the environment in which the system operates, such as "Network Infrastructure" or "Cloud." The SSP template should include the environment in which the system is housed.

1.9 System Status

The system status is "SSP" or "System Status" is a description of the current status of the system, such as "Operational," "Under Development," or "Discontinued." The SSP template should include the status of the system.

1.10 Information Contacts

The information contacts are "SSP" or "Information Contacts" are the individuals responsible for providing information about the system, typically including the system owner, system administrator, and contact information.

1.11 General Description / Purpose

The general description or purpose is "SSP" or "General Description / Purpose" is a brief description of the system's function, such as "Manage access to sensitive data" or "Support customer service requests." The SSP template should include a brief description of the system's purpose.

1.12 System Environment

The system environment is "SSP" or "System Environment" is a description of the environment in which the system operates, such as "Network Infrastructure" or "Cloud." The SSP template should include the environment in which the system is housed.

1.13 System Status

The system status is "SSP" or "System Status" is a description of the current status of the system, such as "Operational," "Under Development," or "Discontinued." The SSP template should include the status of the system.

1.14 Information Contacts

The information contacts are "SSP" or "Information Contacts" are the individuals responsible for providing information about the system, typically including the system owner, system administrator, and contact information.

1.15 General Description / Purpose

The general description or purpose is "SSP" or "General Description / Purpose" is a brief description of the system's function, such as "Manage access to sensitive data" or "Support customer service requests." The SSP template should include a brief description of the system's purpose.

1.16 System Environment

The system environment is "SSP" or "System Environment" is a description of the environment in which the system operates, such as "Network Infrastructure" or "Cloud." The SSP template should include the environment in which the system is housed.

1.17 System Status

The system status is "SSP" or "System Status" is a description of the current status of the system, such as "Operational," "Under Development," or "Discontinued." The SSP template should include the status of the system.

1.18 Information Contacts

The information contacts are "SSP" or "Information Contacts" are the individuals responsible for providing information about the system, typically including the system owner, system administrator, and contact information.

2 NIST 800-33 SECURITY CONTROLS

2.1 (AC-1) Access Control

AC-1 (a) Develop, Document, and Disseminate Policy.

AC-1 (c) Review and Update Policy.

AC-1 (d) IT policy & Procedures are reviewed regularly. The policy administration process is described in detail at http://policies.indiana.edu/security/policies/proc

AC-1 (e) Access Control Management (a) NIST 800-33 (b) NIST 800-33 (c) NIST 800-33 (d) NIST 800-33 (e) NIST 800-33 (f) NIST 800-33 (g) NIST 800-33 (h) NIST 800-33 (i) NIST 800-33 (j) NIST 800-33 (k) NIST 800-33 (l) NIST 800-33 (m) NIST 800-33 (n) NIST 800-33 (o) NIST 800-33 (p) NIST 800-33 (q) NIST 800-33 (r) NIST 800-33 (s) NIST 800-33 (t) NIST 800-33 (u) NIST 800-33 (v) NIST 800-33 (w) NIST 800-33 (x) NIST 800-33 (y) NIST 800-33 (z) NIST 800-33

Each account is unique. It is a system account for an identifier.

Institutional Accounts

"<SystemName>" uses <IoT> for authentication for both the server OS and the application. <IoT> account management policies are described in the following documents: "<IoT> account management policies" describe <IoT> for the following:

Institutional Accounts

"<SystemName>" uses <IoT> for authentication for both the server OS and the application. <IoT> account management policies are described in the following documents: "<IoT> account management policies" describe <IoT> for the following:

Institutional Accounts

"<SystemName>" uses <IoT> for authentication for both the server OS and the application. <IoT> account management policies are described in the following documents: "<IoT> account management policies" describe <IoT> for the following:

Institutional Accounts

"<SystemName>" uses <IoT> for authentication for both the server OS and the application. <IoT> account management policies are described in the following documents: "<IoT> account management policies" describe <IoT> for the following:

Institutional Accounts

"<SystemName>" uses <IoT> for authentication for both the server OS and the application. <IoT> account management policies are described in the following documents: "<IoT> account management policies" describe <IoT> for the following:

Institutional Accounts

"<SystemName>" uses <IoT> for authentication for both the server OS and the application. <IoT> account management policies are described in the following documents: "<IoT> account management policies" describe <IoT> for the following:

Institutional Accounts

"<SystemName>" uses <IoT> for authentication for both the server OS and the application. <IoT> account management policies are described in the following documents: "<IoT> account management policies" describe <IoT> for the following:

Institutional Accounts

"<SystemName>" uses <IoT> for authentication for both the server OS and the application. <IoT> account management policies are described in the following documents: "<IoT> account management policies" describe <IoT> for the following:

Institutional Accounts

"<SystemName>" uses <IoT> for authentication for both the server OS and the application. <IoT> account management policies are described in the following documents: "<IoT> account management policies" describe <IoT> for the following:

Institutional Accounts

"<SystemName>" uses <IoT> for authentication for both the server OS and the application. <IoT> account management policies are described in the following documents: "<IoT> account management policies" describe <IoT> for the following:

Institutional Accounts

"<SystemName>" uses <IoT> for authentication for both the server OS and the application. <IoT> account management policies are described in the following documents: "<IoT> account management policies" describe <IoT> for the following:

Institutional Accounts

"<SystemName>" uses <IoT> for authentication for both the server OS and the application. <IoT> account management policies are described in the following documents: "<IoT> account management policies" describe <IoT> for the following:

Institutional Accounts

"<SystemName>" uses <IoT> for authentication for both the server OS and the application. <IoT> account management policies are described in the following documents: "<IoT> account management policies" describe <IoT> for the following:

Institutional Accounts

"<SystemName>" uses <IoT> for authentication for both the server OS and the application. <IoT> account management policies are described in the following documents: "<IoT> account management policies" describe <IoT> for the following:

Institutional Accounts

"<SystemName>" uses <IoT> for authentication for both the server OS and the application. <IoT> account management policies are described in the following documents: "<IoT> account management policies" describe <IoT> for the following:

Institutional Accounts

"<SystemName>" uses <IoT> for authentication for both the server OS and the application. <IoT> account management policies are described in the following documents: "<IoT> account management policies" describe <IoT> for the following:
Document enterprise common controls

- Individual SSPs describe NIST 800-53 controls you have in place.
- Many of these will be inherited from your organization. They will apply to all systems. We call them enterprise common controls (ECC).
- It is wasteful to include them every time in each SSP.
- So document ECCs separately and have individual SSPs simply point to the ECC docs.
The ECC document is literally NIST 800-53 with responses.
Assess risk

• Do risk self-assessments; they are cheap
• Have managers & system administrators sit down and brainstorm.
• Identify areas of vulnerabilities and risk for the system.
• Document risk areas, controls that address those risks, residual risks, and risk severity.
• Have external, third party assessments every once in a while if you can afford them.
The Risk Assessment Report Template

<table>
<thead>
<tr>
<th>Threat/Val. Pair #</th>
<th>Threat Event</th>
<th>Area of Exploitable Vulnerability</th>
<th>Risk Category</th>
<th>Risk Details</th>
<th>Mitigating NIST Controls</th>
<th>Mitigating NIST Controls/Factors Summary</th>
<th>Residual Vulnerability</th>
<th>Residual Risk Level</th>
<th>Risk Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Attack</td>
<td>Account management</td>
<td>Compromise of confidentiality and integrity</td>
<td>Data exposure due to weak account management practices (account provisioning, testing, deprovisioning)</td>
<td>AC-2</td>
<td>Use of institutional accounts and mature account management practices.</td>
<td>Low</td>
<td>Mitigated by existing controls</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Attack</td>
<td>Password management</td>
<td>Compromise of confidentiality and integrity</td>
<td>Data exposure due to weak password management practices (password strength, expiration, password changes without validation, passwords in scripts)</td>
<td>IA-2, IA-4, IA-5, IA-6, IA-7</td>
<td>Use of institutional accounts and mature password management practices. No passwords in scripts.</td>
<td>Low</td>
<td>Mitigated by existing controls</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Attack, recon</td>
<td>Logical access controls</td>
<td>Compromise of confidentiality and integrity</td>
<td>Data exposure due to unauthorized access (trivial ports, generic accounts, accounts with no passwords, uncontrolled remote access)</td>
<td>AC-3, AC-5, AC-6, AC-8, AC-13, SC-7</td>
<td>Most system components behind Data Center firewall. Generic accounts/accounts with blank passwords deleted.</td>
<td>Moderate</td>
<td>See POA&amp;M</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Attack</td>
<td>Privilege management</td>
<td>Compromise of confidentiality and integrity</td>
<td>Data exposure due to unauthorized access resulting from weak privilege management (deliberate administrative accounts, no explicit privilege authorization)</td>
<td>AC-1, AC-2, AC-3, AC-4, AC-13</td>
<td>No individual accountability due to administrative account.</td>
<td>Moderate</td>
<td>See POA&amp;M</td>
<td></td>
</tr>
</tbody>
</table>
Document risk response

• Document how you will respond to residual risk in a Plan of Action & Milestones or POA&M document.

• It states whether the risk was accepted, transferred, addressed, or to be mitigated, and reasons, timelines and planned mitigation activities/controls.

• Valid reasons for accepting a risk is budget, resource constraints, etc. You can often still address them through training.
<table>
<thead>
<tr>
<th>Risk</th>
<th>Risk Level</th>
<th>Action</th>
<th>Milestone</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application access to external data sources</td>
<td>Moderate</td>
<td>Risk accepted pending evaluation. Risk will be calculated for each specific application installed and the nature of connection and addressed accordingly.</td>
<td>Each application connecting to an external source will be analyzed independently to evaluate and mitigate risk.</td>
<td></td>
</tr>
<tr>
<td>&lt;device&gt; located outside Data Center firewall</td>
<td>Moderate</td>
<td>Risk addressed. The volume of data has an adverse effect on the Data Center firewall and the end user experience. The risk is minimized through existing security controls that address the device specifically.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No individual accountability due to shared administrative accounts</td>
<td>Moderate</td>
<td>Risk addressed in the next column. The Citrix application requires the use of administrative accounts.</td>
<td>The risk will be mitigated via an access inventory of privileged access.</td>
<td>6/1/14</td>
</tr>
</tbody>
</table>
Train staff

• Mandate annual training for both management and staff responsible for the system.

• At IU three e-training modules must be completed:
  1. The standard IU HIPAA training (covering the law and IU policies & procedures)
  2. IU Human Subjects training
  3. UITS specific information on how HIPAA applies to the IT organization specifically, our policies & NIST procedures

• Document all security related training in a training log.
Train users and raise awareness

• Provide online training and awareness via a knowledge base, YouTube videos or other media, in person classes, and email alerts.
• Can do things like launching your own phishing attack.
• Work individually with users, train them as you help them.
• Help them create their own (HIPAA) documentation describing how they are protecting their end.
Institute oversight/approval

• Have your authorities provide oversight (which may be required at your institution) and approval or assign someone within your organization.

• At IU the completed compliance documentation package is sent to the IU HIPAA Compliance Office, the University Information Security Office, and Internal Audit.
Institute ongoing risk management

• Institute regular, ongoing risk management through:
  • Regular reviews, risk re-assessments, and documentation updates.
  • Continuous, automatic monitoring of systems.
  • Annual training & awareness.
  • Oversight.
  • External assessments.
  • Penetration testing.
  • Campaigns (phishing, etc.)
4. Conclusion
Compliance is doable

• The government does not expect you to undertake herculean measures or build walled gardens.

• Cyber compliance requirements are all about best practices, something we should be doing anyway (and are, mostly).

• You likely have sufficiently good information security in place already. It doesn’t take a gargantuan effort to go all the way.
Benefits

• A standards based RMF implementation makes you rule/regulation proof.

• Customers with sensitive data will trust your shop, bringing in new business and funding.

• Your compliance folks will send people your way (ours do).

• You will better serve researchers/your mission.
The evolution of cybersecurity

• No one thinks cybersecurity is a solvable problem; The fixes aren’t working despite huge cybersecurity budgets.

• A new approach called “resilience” is emerging.

• It treats the situation just like the medical establishment does human disease. You will be sick. You will be hacked. Period.

• The goal is to survive being hacked, be resilient.

• How? Prevent (defend, detect, remediate - baseline risk management), Respond (incident response), Recover (DR), and Refine (learn, adapt).
Links

• The HIPAA Security Rule
  • http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

• NIST 800-66: Guide to Implementing the HIPAA Security Rule

• NIST 800-53: Recommended Security Controls

• NIST 800-53A: Guide for Assessing Security Controls

• NIST HIPAA Security Rule Toolkit
  • http://scap.nist.gov/hipaa/

• NIST Templates (email me)
Contact

Anurag Shankar
ashankar@iu.edu