Aligning Your Research Cyberinfrastructure with HIPAA and FISMA

Anurag Shankar
Center for Applied Cybersecurity Research
Indiana University

2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure
August 17, 2015

INDIANA UNIVERSITY

UNIVERSITY INFORMATION TECHNOLOGY SERVICES

Schedule

1. Introduction	1:00 – 1:05
2. Research Cyberinfrastructure & Compliance	1:05 – 1:15
3. A Gentle HIPAA Primer	1:15 – 1:45
4. A Gentler FISMA Primer	1:45 – 2:15
5. A Risk Management Primer	2:15 – 2:30
6. The NIST Risk Management Framework	2:30 – 3:00
Break	3:00 – 3:30
7. Building a Risk Management Framework	3:30 – 4:00
8. Using it to Address HIPAA & FISMA	4:00 – 4:20
9. The Future	4:20 – 4:30
10. Conclusion, Q & A / Discussion	4:30 – 5:00

1. Introduction

Quiz

- Do you know what kinds of data you have on your systems?
- Do you allow biomedical researchers on your systems?
- Have you a mechanism to stop sensitive data on the system?

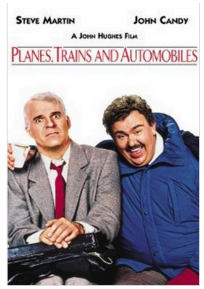
Data Inventory

- A recent DLP exercise at IU showed that all 120 or so cloud storage systems are being used.
- Data flows showed plenty of personally identifiable health information.
- An Identity Finder run following a security incident on a user PC showed SSNs, etc.

* Big Data to Knowledge

Cybersecurity State of the Union

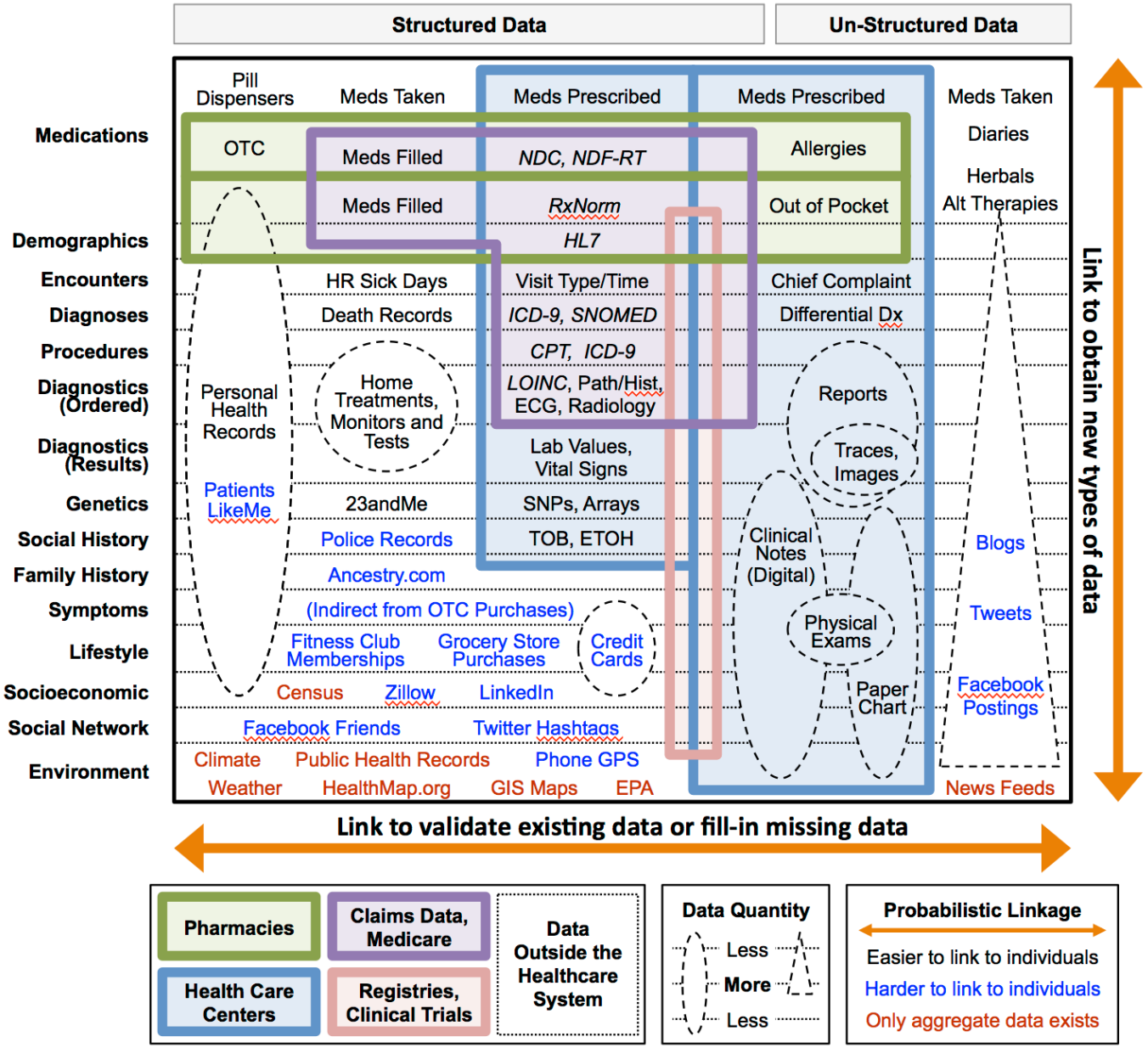
- Massive breaches this past year.
- On average half a million web attacks per day*. The network itself is being targeted now.
- Data exfiltration is most common, but new threats are emerging, in particular crypto-ransomware.
- Scary new targets (transportation, medical devices, etc.), IoT.



2015 Internet Security Threat Report, Symantec

Healthcare Cybercrime

- Healthcare is the most heavily targeted sector, breaches up 25%.
- Exfiltrated patient information being used for identity & insurance fraud, blackmail & extortion, celebrity snooping, etc.
- Patient records yield the highest price on the cybercrime market today.
- Problem as big as the data.



Healthcare "Big Data" Zoo

Weber, Mandl, and Kohane "Finding the Missing Link for Big Biomedical Data" JAMA 2014.4228

Where are we headed?

- Big Data spurring new areas of research, for instance electronic medical record (EMR) analytics, data repurposing, metadata harvesting, healthcare AI, etc.
- NIH calls this BD2K*.
- Coming to a … facility near you (campus, lab, NSF center??).

* Big Data to Knowledge

2. Research CI & Compliance

Major Cybersecurity Regulations Affecting Research

- Health Insurance Portability & Accountability Act (HIPAA) - 1996
- FDA CFR 21 Part 1 – 1997
- Federal Information Security Management Act (FISMA) – 2002

NIH

- Identifiable health data may be* subject to HIPAA Privacy.
- NIH funded researchers use a well established structure that handles HIPAA and FDA compliance (IRBs, Office of Research Administration, HIPAA Compliance Office, etc.)
- NIH is requiring FISMA compliance for contracts.

* HIPAA doesn't apply to all health data

NSF

- NSF doesn't directly fund health research. However, it does fund social sciences and uses IRBs for human subjects research.
- Human subjects research must comply with the Common Rule*.
- FISMA may be coming to NSF contracts/grants.

* http://www.nsf.gov/bfa/dias/policy/docs/45cfr690.pdf

Ready or Not …

- Analysis, storage, and management needs of health sciences research data reaching scales typical of physical sciences and engineering.
- Medical Center IT cannot keep pace.
- Existing local or national research CI often the only refuge.
- Health data ends up on our systems, often identifiable, without our knowledge or choice.


COMPLIANCE

Challenges

- Researchers/CI providers are not regulatory experts.
- Cyber risk still a new concept for many.
- Lack of resources.
- Increasing HIPAA fines/audits.
- Potential loss of funding/face.

HIPAA & Research CI at Indiana University

Research CI at IU

- IU has had a mature, central research CI (local and national) for a couple decades now.
- CI provisioned through the Research Technologies (RT) division of the University Information Technology Services (UITS), IU's central IT organization.
- RT delivers supercomputing, data storage/archival, visualization, application development & optimization, data management, etc.

HIPAA Intervenes

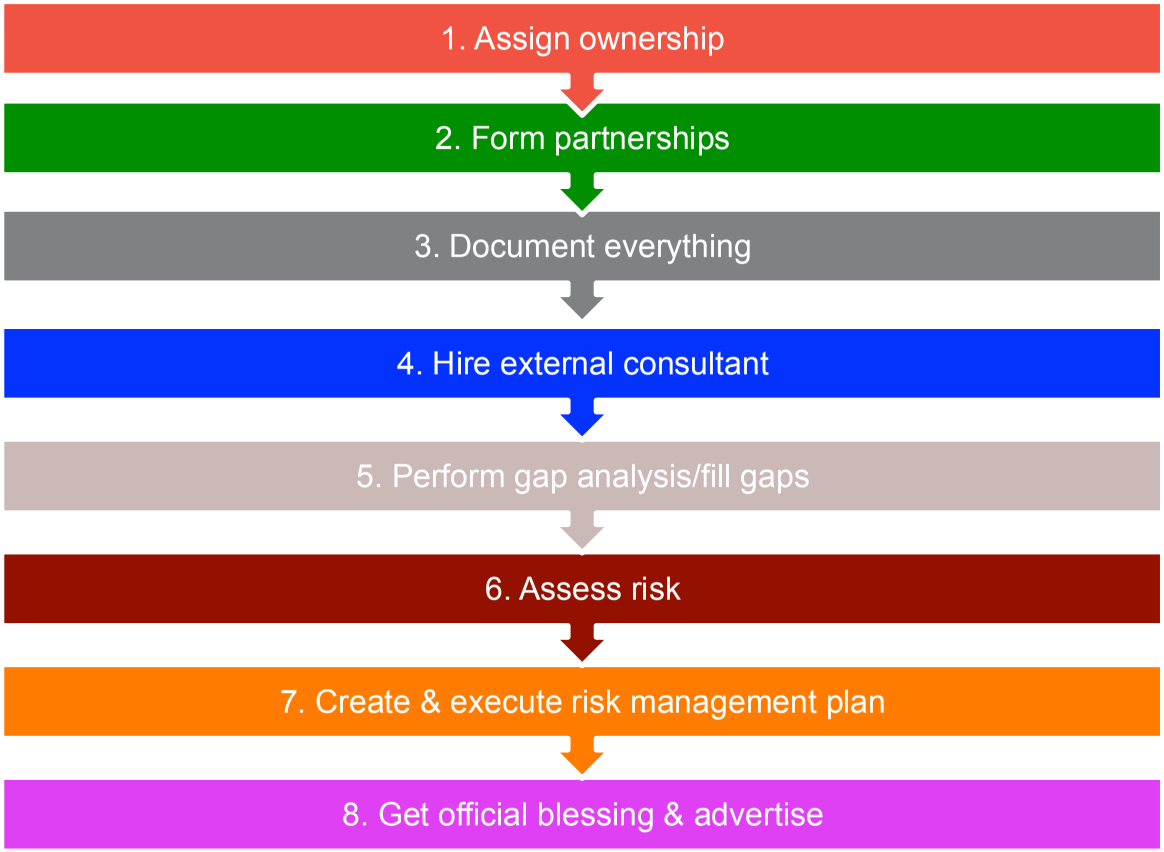
- Prior to 2000, IU's central research CI used almost exclusively by the usual suspects - physical scientists and engineers.
- A Lilly Endowment grant to accelerate genomics research proposed using the existing CI for IU School of Medicine researchers.
- HIPAA compliance became a requirement.

Timeline

It wasn't until 2007 when HIPAA efforts to align our entire research CI began in earnest. The project took two years and required:

- Dedicated resources (1 FTE).
- Education (regulatory/security).
- An institution-wide committee for oversight and advocacy.
- An external gap and risk assessment.

HIPAA Implementation Steps



HIPAA Steps

① Assign ownership: One RT director and one staff (about 1 FTE)

② Form partnerships: Put all stakeholders on an oversight committee.

③ Document everything: Policies & procedures, responsibilities

④ Hire external consultant: Recommended by IU Compliance

⑤ Perform gap analysis: Measured how far controls are from HIPAA

⑥ Fill gaps: Plugged as many holes as we could

⑦ Assess risk: Output from 3&5 informed the assessment

⑧ Create & execute risk management plan: Guided by consultant

⑨ Get official blessing & advertise: Focus on biomedical researchers

Results

We received a blessing from the IU Compliance in 2009 of our "ability to handle ePHI".

- … and starting from zero in 2009, we grew to:

1. Number of biomedical user accounts	3,000
2. Volume of biomedical data stored	~1PB
3. Use of computing cycles	1 MSUs
4. Number of databases	~ 1000
5. New services for biomedical users	>10
6. Number of NIH grants that fund us	5
7. Number of FTEs funded by these grants	~ 10

Evolution

- Initial process and resources developed were largely homegrown & ad-hoc (much fumbling).
- Other rules/regulations such as FISMA, PCI-DSS, new IU IT risk policy, etc. were appearing on the horizon.
- By 2013 the structure was showing its age. It was also too HIPAA specific.
- A unified approach to compliance became apparent. (Most rules and regulations require risk management strategy and nearly the same controls.)

Compliance 2.0

- Needed a widely accepted standard.
- NIST chosen because it is a federal standard & addresses both HIPAA & FISMA compliance.
- It provides a persistent and evolving risk management framework, not just security controls.
- Strategy is to align with NIST first, then use mappings to specific regulations/requirements.
- Addresses departures from NIST explicitly.

Compliance 2.0 …

- The essential elements were there already.
- In 2013 added missing components - risk self assessment & mitigation, inventory, training, and more detailed documentation of controls.
- Documentation uses IU customized FISMA templates borrowed from DHHS/NASA.
- Transitioned to the new process over time, all new systems using it, old systems being migrated.

3. A Gentle HIPAA Primer

What is HIPAA?

"No, it's not a female Hippopotamus, anyone else know?

HIPAA
Health Insurance Portability & Accountability Act

HIPAA

- Health Insurance Portability & Accountability Act.
- Passed in 1996, became law in 2001.
- Enforced by the Office for Civil Rights (OCR) in the US Dept. of Health & Human Services (DHHS).
- The HIPAA Omnibus Final Rule of 2013 includes provisions from the 2006 Health Information Technology for Economic & Clinical Health (HITECH) Act & the 2008 Genetic Information Nondiscrimination Act (GINA).

Patient Privacy Protection

- Addressed via the HIPAA Privacy Rule and the HIPAA Security Rule.
- The Privacy Rule defines who HIPAA applies to (covered entities), what is protected (protected health information or PHI), and covers disclosure.
- The Security Rule focuses exclusively on how to protect electronic PHI (ePHI) in any form – at rest, in transit, under analysis, etc.

  → ePHI = identifiable patient data with any of 18 identifiers

Identifiers that Make Data PHI

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 protected

Relationship to State Laws

- Many states have their own privacy laws.
- If HIPAA is incompatible with state laws, HIPAA preempts state.
- Except when the state law provides greater privacy protections than HIPAA.
- DHHS makes the determination upon request.
- HIPAA is a floor, not a ceiling.

Covered Entity

- HIPAA only applies to a covered entity (CE).
- Covered entities are healthcare providers, health plans, and health clearinghouses.
- Universities often choose to be hybrid covered entities, with both covered (healthcare) and non-covered components.
- HIPAA affects the whole CE. (For instance, the CE faces fines when a HIPAA violation occurs, not an individual department or employee.)

Am I covered?

- Your organization is not a covered entity if it is not involved in healthcare operations directly.
- You may still be subject to HIPAA if you serve a covered entity as a member of your covered entity's workforce or as a Business Associate* and handle PHI for them in any way, shape, or form.
- You cannot say "I didn't know we had PHI".

* To be discussed

Business Associate

A HIPAA Business Associate* (BA) is defined as “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.”

* BA is a HIPAA specific term

Business Associate Agreement

- HIPAA may require a Business Associate Agreement (BAA) with vendors that can touch ePHI on your system (since it's a disclosure).
- The BAA must include language that the BA will protect your PHI and abide by HIPAA. (Sample BAAs at DHHS site.)
- It mandates due diligence (an assessment) to ensure that the BA can protect your PHI as per HIPAA.

Am I a Business Associate?

- You are not a BA if you are part of (say) a university providing services to its medical school.
- You are if you are (a) providing services to a CE completely separate from yours, and (b) store or process PHI for them.
- If the latter, the external CE must have a BAA with you (since your sys admins have access to user data).
- They are in violation of HIPAA if they do not.

What is a HIPAA Breach?

- An incident where an unauthorized disclosure of PHI has occurred.
- For instance a successful attack against a server which allows a hacker access to PHI, theft of an unencrypted device with PHI, loss of paper PHI, verbal disclosure, etc.
- Despite these situations, it may not be a breach if by forensics or other means you can show a high likelihood that that no PHI was accessed.

A HIPAA Breach?

"Mrs. Cranley! You need to sign this HIPAA privacy form before the doctor can look at those warts on your stomach!"

Breach Notification

- HIPAA requires a breach of PHI to be reported to the OCR & patients whose data has been lost within 60 days.
- For breaches involving > 500 individuals, local media outlets must also be notified.
- Breaches are highly damaging.
- Not reporting a breach is a serious HIPAA violation that is liable for big penalties.

Enforcement

- HIPAA is enforced by the Office for Civil Rights (OCR) in the Dept. of Health & Human Services (DHHS).
- Violations can result in civil monetary penalties (up to $1.5 million) against a covered entity and/or individual criminal penalties (imprisonment up to 10 years).
- The OCR was funded via ARRA/HITECH to institute an audit program. They have done 150 audits already and getting ready for more.

Civil Monetary Penalties

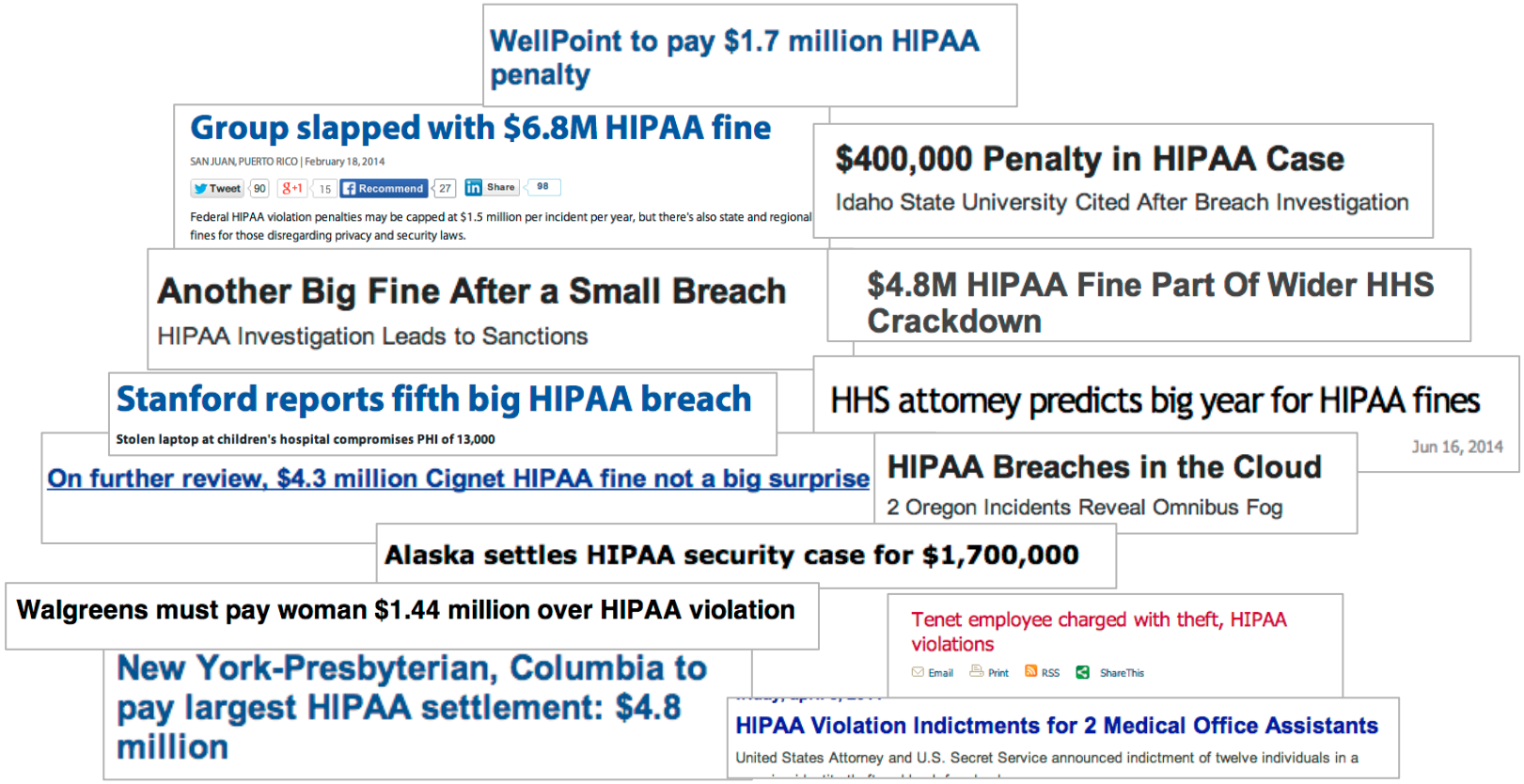
Violation Category	Each Violation		All Identical Violations Per Calendar Year	
	For violations occurring before 2/18/2009	For violations occurring on or after 2/18/2009	For violations occurring before 2/18/2009	For violations occurring on or after 2/18/2009
Did Not Know (that a violation occurred)	Up to $100	$100 - $50,000	$25,000	$1,500,000
Reasonable Cause	Up to $100	$1000 - $50,000		
Willful Neglect - Corrected	Up to $100	$10,000 - $50,000		
Willful Neglect - Not Corrected	Up to $100	$50,000		

HIPAA Health Insurance Portability & Accountability Act

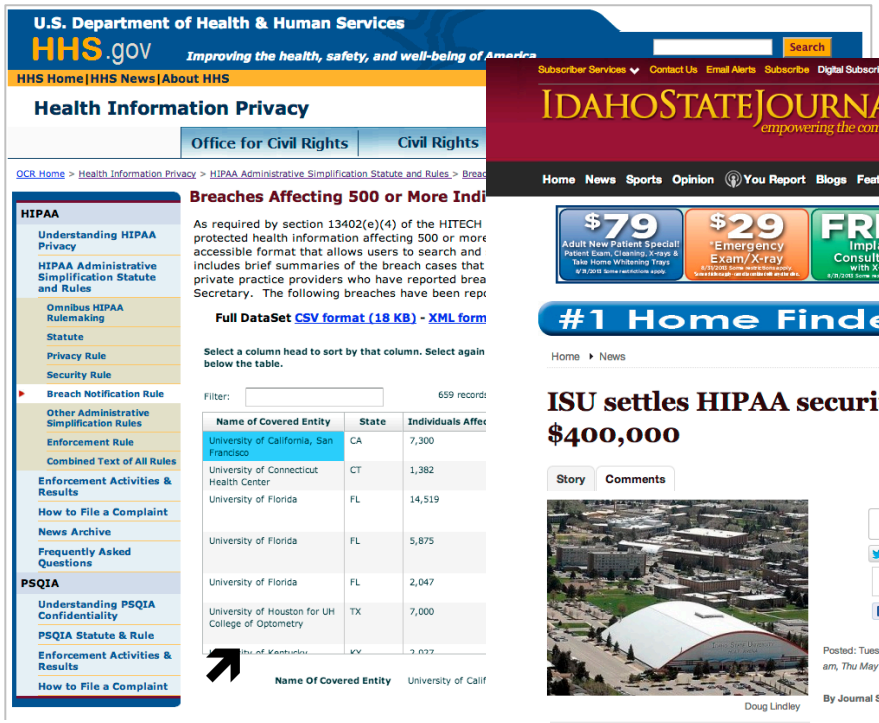
Wonders of Multiplication

- HIPAA penalties are levied per violation.
- Breach of an individual record is one violation. To calculate your total, multiply by the number of affected individuals.
- Fortunately, there are maximums. Still, we are talking serious numbers here.
- Identity protection is universally expected after a beach. It's not cheap!

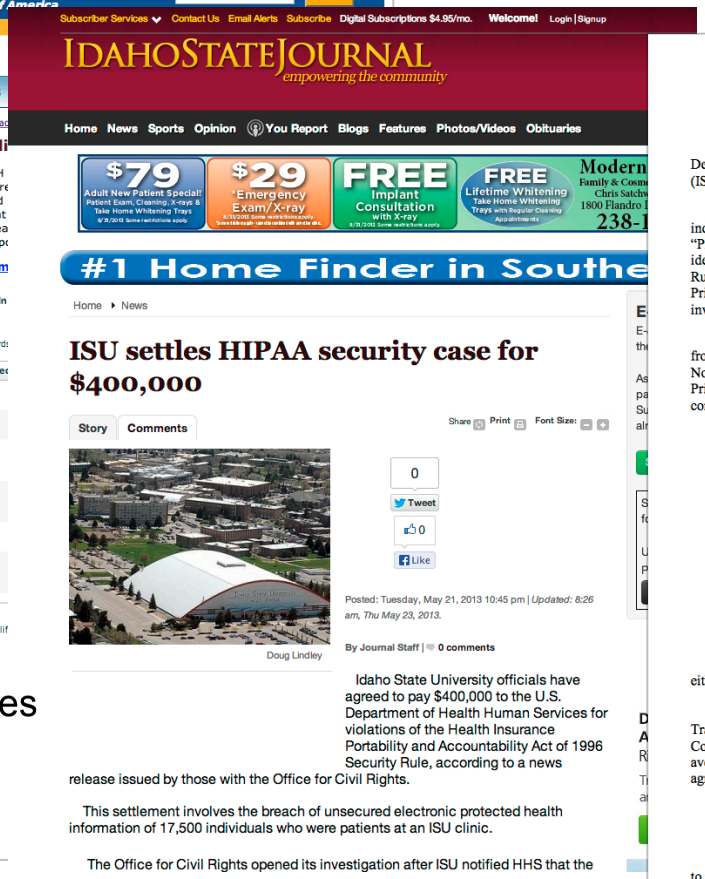
HIPAA Civil/Criminal Penalties in Action

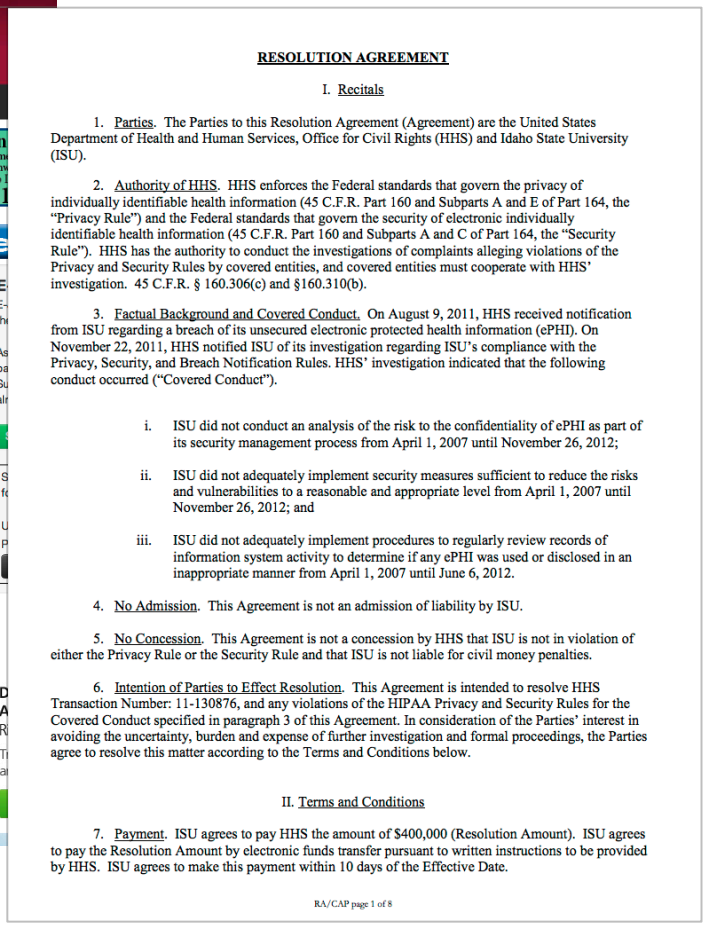


HIPAA Health Insurance Portability & Accountability Act



Breaches reported by universities





RESOLUTION AGREEMENT

I. Recitals

1. Parties. The Parties to this Resolution Agreement (Agreement) are the United States Department of Health and Human Services, Office for Civil Rights (HHS) and Idaho State University (ISU).

2. Authority of HHS. HHS enforces the Federal standards that govern the privacy of individually identifiable health information (45 C.F.R. Part 160 and Subparts A and E of Part 164, the "Privacy Rule") and the Federal standards that govern the security of electronic individually identifiable health information (45 C.F.R. Part 160 and Subparts A and C of Part 164, the "Security Rule"). HHS has the authority to conduct the investigations of complaints alleging violations of the Privacy and Security Rules by covered entities, and covered entities must cooperate with HHS' investigation. 45 C.F.R. § 160.306(c) and §160.310(b).

3. Factual Background and Covered Conduct. On August 9, 2011, HHS received notification from ISU regarding a breach of its unsecured electronic protected health information (ePHI). On November 22, 2011, HHS notified ISU of its investigation regarding ISU's compliance with the Privacy, Security, and Breach Notification Rules. HHS' investigation indicated that the following conduct occurred ("Covered Conduct").

i. ISU did not conduct an analysis of the risk to the confidentiality of ePHI as part of its security management process from April 1, 2007 until November 26, 2012;

ii. ISU did not adequately implement security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level from April 1, 2007 until November 26, 2012; and

iii. ISU did not adequately implement procedures to regularly review records of information system activity to determine if any ePHI was used or disclosed in an inappropriate manner from April 1, 2007 until June 6, 2012.

4. No Admission. This Agreement is not an admission of liability by ISU.

5. No Concession. This Agreement is not a concession by HHS that ISU is not in violation of either the Privacy Rule or the Security Rule and that ISU is not liable for civil money penalties.

6. Intention of Parties to Effect Resolution. This Agreement is intended to resolve HHS Transaction Number: 11-130876, and any violations of the HIPAA Privacy and Security Rules for the Covered Conduct specified in paragraph 3 of this Agreement. In consideration of the Parties' interest in avoiding the uncertainty, burden and expense of further investigation and formal proceedings, the Parties agree to resolve this matter according to the Terms and Conditions below.

II. Terms and Conditions

7. Payment. ISU agrees to pay HHS the amount of $400,000 (Resolution Amount). ISU agrees to pay the Resolution Amount by electronic funds transfer pursuant to written instructions to be provided by HHS. ISU agrees to make this payment within 10 days of the Effective Date.

RA/CAP page 1 of 8

The absolute worst is being in the newspapers

HIPAA Health Insurance Portability & Accountability Act

What happens after a breach?

- The OCR, affected individuals, and media are notified.
- All documentation (incident response, policies & procedures, risk assessment, management, etc.) is submitted to OCR.
- OCR may open an investigation or bless due diligence if response is swift and addresses the underlying risks.
- OCR may require a “Corrective Action Plan” and levy a fine.
- A CAP response is submitted to OCR.
- OCR closes the investigation.

HIPAA Health Insurance Portability & Accountability Act

Breach Investigation

During an investigation, the OCR looks for

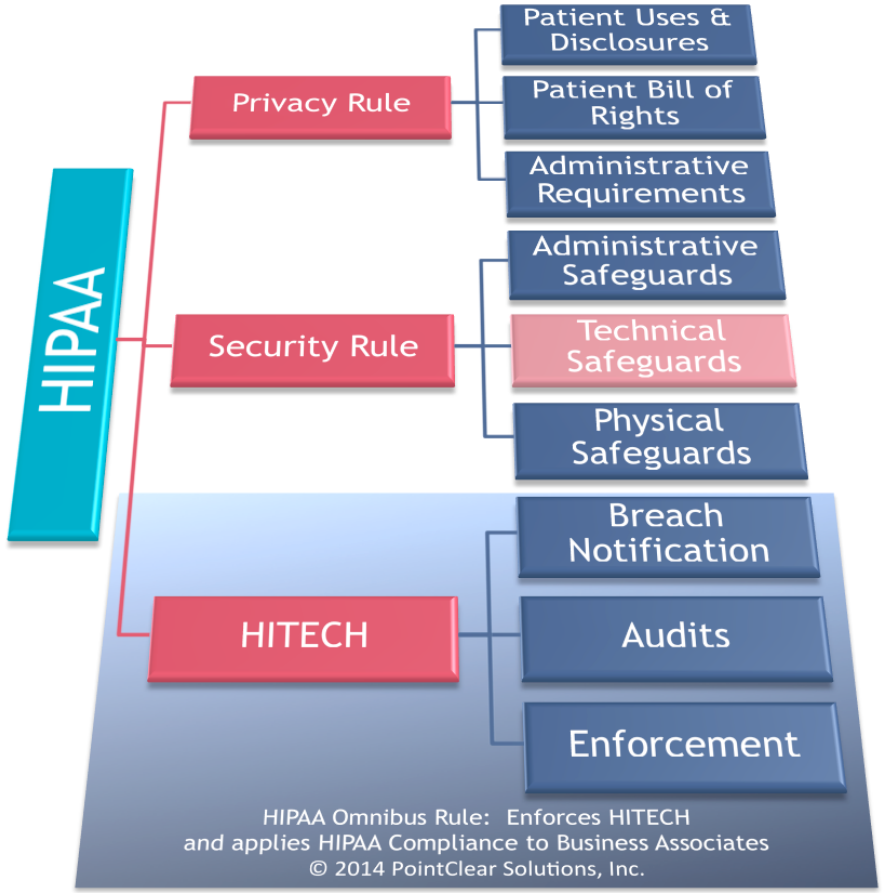
- Documented Policies & Procedures
- Implementation of Policies & Procedures
- Internal investigation reports, interview statements, etc.
- Appropriate sanctions applied
- Documented Training
- Business Associate Agreements
- Documented Risk assessment, mitigation
- Encryption & mobile device policies/ implementation

HIPAA Health Insurance Portability & Accountability Act

Recent HIPAA Changes

- The HIPAA Omnibus Final Rule added HITECH & GINA provisions, new business associate & breach notification requirements, and audits/enforcement.
  - HITECH was part of ARRA and enacted to promote the adoption of Health Information Technology, especially Electronic Health Records (EHR).
  - GINA prohibits insurers from using human genetic data to deny coverage based on genetic predisposition to future diseases. However, genetic data without the 18 identifiers is not subject to HIPAA.

HIPAA after Omnibus



Courtesy Pointclear Solutions, Inc.

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 (e.g. HSO* *required)*, workforce security, access management, incident response, disaster planning, evaluations, etc.
- Physical – facilities access, workstation use/ security, device/media controls.
- Technical – access/audit control, integrity, authentication, transmission security.

  + organizational/policies/documentation requirements

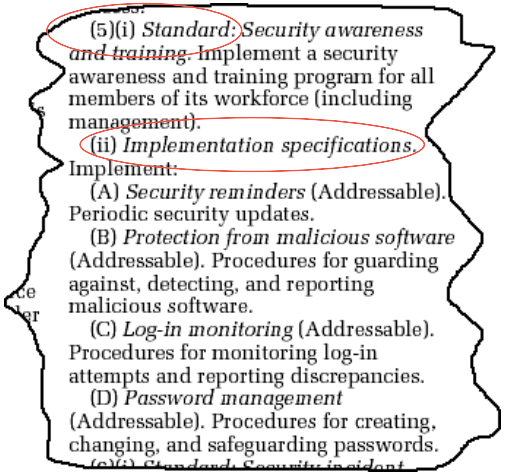
* HIPAA Security Officer

Required & Addressable

- Each Security Rule safeguard is either required or addressable.
- Required = what it says.
- Addressable = must address, but ok if you describe why it is not in place or how you will otherwise address the risk.
- A risk assessment (RA) identifies where to concentrate your effort.

Standards and Implementation

- The Security Rule defines standards and implementation specifications.



(5)(i) *Standard: Security awareness and training.* Implement a security awareness and training program for all members of its workforce (including management).

(ii) *Implementation specifications.* Implement:

(A) *Security reminders* (Addressable). Periodic security updates.

(B) *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

(C) *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

(D) *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

- Standards address broad categories.
- Implementation specifications are just what it says; how they are to be implemented.
- It's the implementation specifications that are either required or addressable.

HIPAA Health Insurance Portability & Accountability Act

Does HIPAA apply to all Identifiable Health Data?

- No. Only healthcare providers, facilities, and insurers are bound by HIPAA. Identifiable health data outside a healthcare context is not ePHI (though Common Rule still applies*).
- Data, if properly de-identified, is not subject to HIPAA.

If unsure, contact your HIPAA Compliance office!

* state rules may also apply

Who does HIPAA Cover at my organization?

- Employees, healthcare providers, trainees & volunteers at the medical school and affiliated healthcare sites or programs.
- Employees who work with university or organizational health plans.
- Employees who provide financial, legal, business, administrative, or IT support to the above.

Just Good Security?

Q: So, the HIPAA Security Rule means we just need to provide good IT security for systems?

A: No. The Security Rule is about managing risk, and security is only PART of that management. HIPAA requires administrative controls, training, governance, policies, formal review, etc.

Do I firewall & encrypt it all?

- Maybe. The Security Rule does not prescribe particular solutions or specifications, only broad guidelines, to be interpreted by individual implementers according to their environment.
- It requires a managed risk approach that proves due and ongoing diligence to OCR.
- Documentation is key. If it is not documented IN DETAIL, it doesn't exist as far as OCR is concerned.

Local Risk Tolerance

- Since HIPAA gives such wide berth, it is typically your institutional risk tolerance that in reality determines what you must do.
- Some build walled gardens; we didn't.
- Instead, we worked closely with our HIPAA Privacy and Security Officers. They are intimately engaged in our risk management process. They feel that we do sufficient due diligence and can survive a breach/audit.

"We all deal with it differently."

HIPAA Health Insurance Portability & Accountability Act

HIPAA Myths

- That HIPAA compliance is a boolean = there is a threshold which, when crossed, makes you compliant.
- That you can have a qualified third party review your environment and certify your HIPAA compliant.
- That the whole compliance exercise is a one time deal.

Sorry, none are true!

Here is what the DHHS says:

U.S. Department of Health & Human Services
HHS.gov *Improving the health, safety, and well-being of America*
Search
HHS Home | HHS News | About HHS
Font Size Print Download Reader

Health Information Privacy

Office for Civil Rights | Civil Rights | Health Information Privacy

OCR Home > Health Information Privacy > Frequently Asked Questions

HIPAA
- Understanding HIPAA Privacy
- HIPAA Administrative Simplification Statute and Rules
- Enforcement Activities & Results
- How to File a Complaint
- News Archive
- Frequently Asked Questions

PSQIA
- Understanding PSQIA

Are we required to "certify" our organization's compliance with the standards of the Security Rule?

Answer:

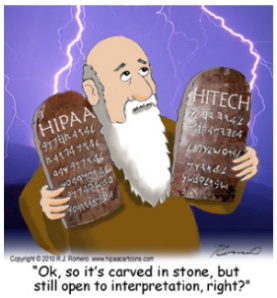
No, there is no standard or implementation specification that requires a covered entity to "certify" compliance. The evaluation standard § 164.308(a)(8) requires covered entities to perform a periodic technical and non-technical evaluation that establishes the extent to which an entity's security policies and procedures meet the security requirements. The evaluation can be performed internally by the covered entity or by an external organization that provides evaluations or "certification" services. A covered entity may make the business decision to have an external organization perform these types of services. It is important to note that HHS does not endorse or otherwise recognize private organizations' "certifications" regarding the Security Rule, and such certifications do not absolve covered entities of their legal obligations under the Security Rule. Moreover, performance of a "certification" by an external organization does not preclude HHS from subsequently finding a security violation.

→ You can only establish the extent to which you are compliant.
We therefore use the word "aligned" rather than "compliant".

HIPAA Health Insurance Portability & Accountability Act

HIPAA Facts

- There is nothing that assures that you are 100% compliant. The OCR may still find you lacking.
- There IS one way to be sure - an OCR audit! Due diligence is a lot easier.
- So you read the Security Rule carefully, do your best to implement the requisite administrative, physical, and technical safeguards, and self-assert compliance.



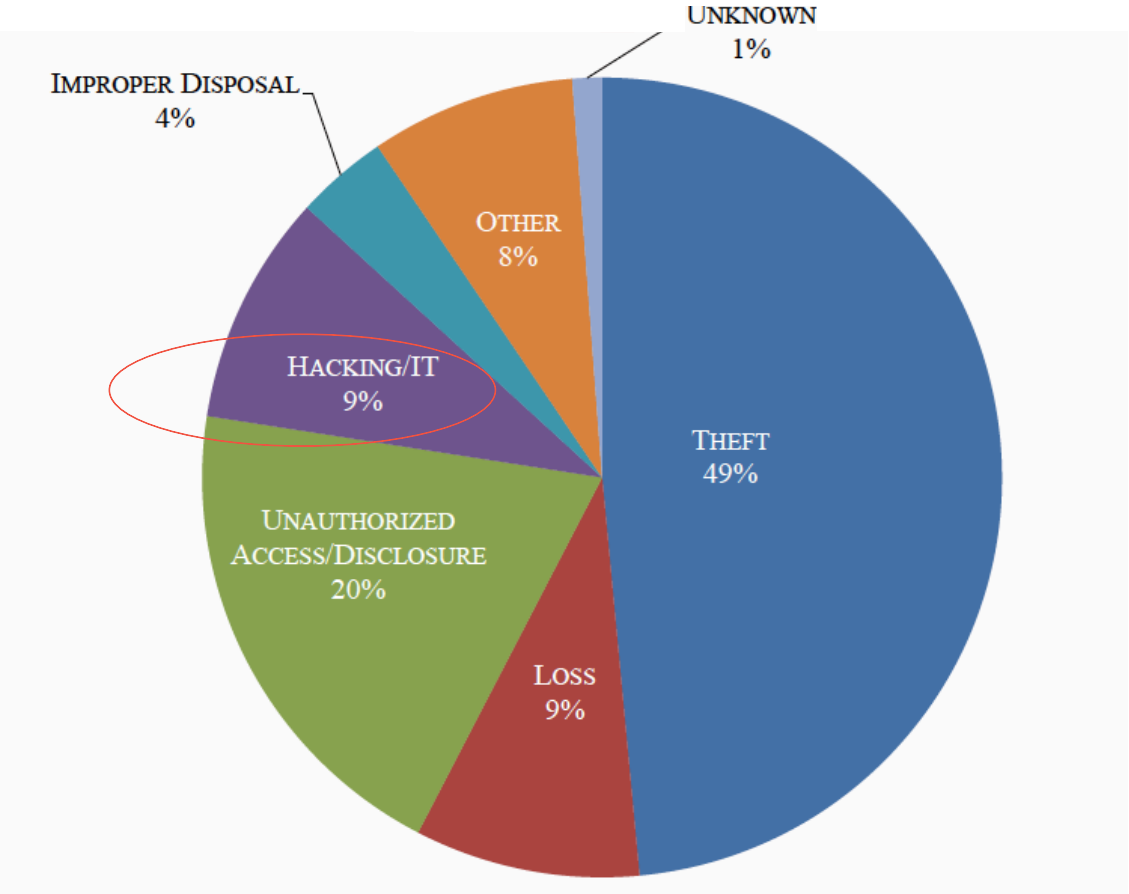
"Ok, so it's carved in stone, but still open to interpretation, right?"

HIPAA is Fuzzy

- The HIPAA Security Rule allows you a lot of latitude depending on factors such as your size, budget, etc.
- This is both a boone and bane.
- It is highly open to local interpretation.
- Use your local HIPAA Compliance office to clarify what HIPAA means in your environment.
- If you don't have such a unit, check with legal.

HIPAA Health Insurance Portability & Accountability Act

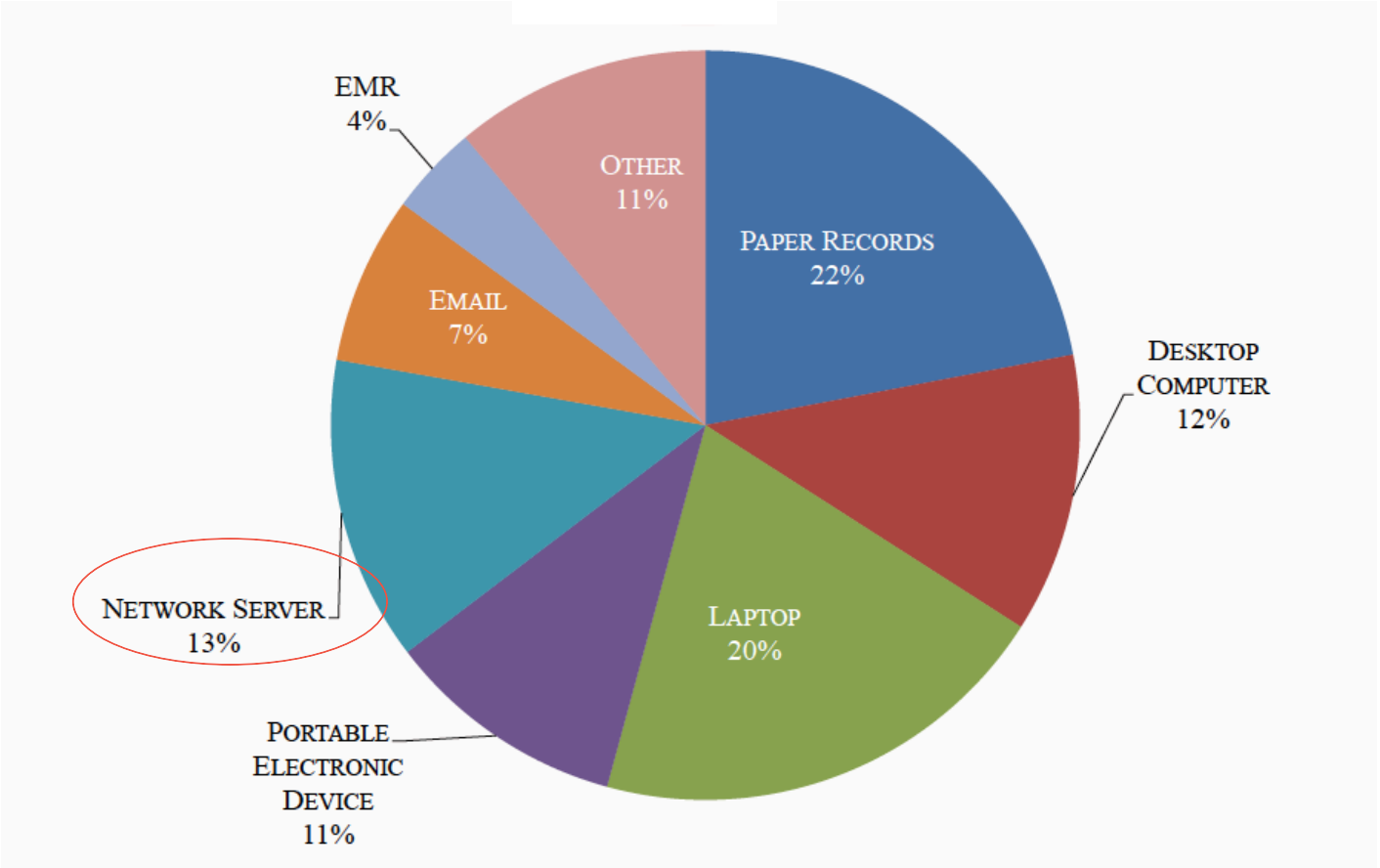
Breach Notification Stats as of 5/15: 500+ Breaches by Type



Courtsey Linda Sanchez, OCR

HIPAA Health Insurance Portability & Accountability Act

Breach Notification Stats as of 2/14: 500+ Breaches by Location



Courtesy Linda Sanchez, OCR

HIPAA Health Insurance Portability & Accountability Act

Lessons from Breaches

- Most of the breaches occur due to theft/loss & improper disclosure.
- Hacking or IT incidents is only at 9%. However, even one breach is too many since it can be highly damaging to the CE.
- A lot of breaches occur at the user end & have to do with (unencrypted) mobile devices & media (laptops, USB sticks, phones).
- Paper records are still big.

Top Areas of Weakness Revealed by Breach Stats

- Risk Assessments
- Granting or Modifying Access
- User Activity Monitoring
- Authentication and Integrity
- Media Reuse and Destruction
- Contingency Planning

Most Common Causes of Citation from Recent OCR Audits

- No risk assessments
- Improper media movement and disposal
- No/inadequate audit controls and monitoring

4. A Gentler FISMA Primer

What is FISMA?

- Federal Information Security Management Act of 2002.
- Requires government agencies to secure their system as per NIST guidelines.
- The Office of the Inspector General does FISMA audits.
- There are also regular reporting requirements.
- Agency subcontractors (=you) also have to comply (similar to the HIPAA BA rule).

When does FISMA Apply?

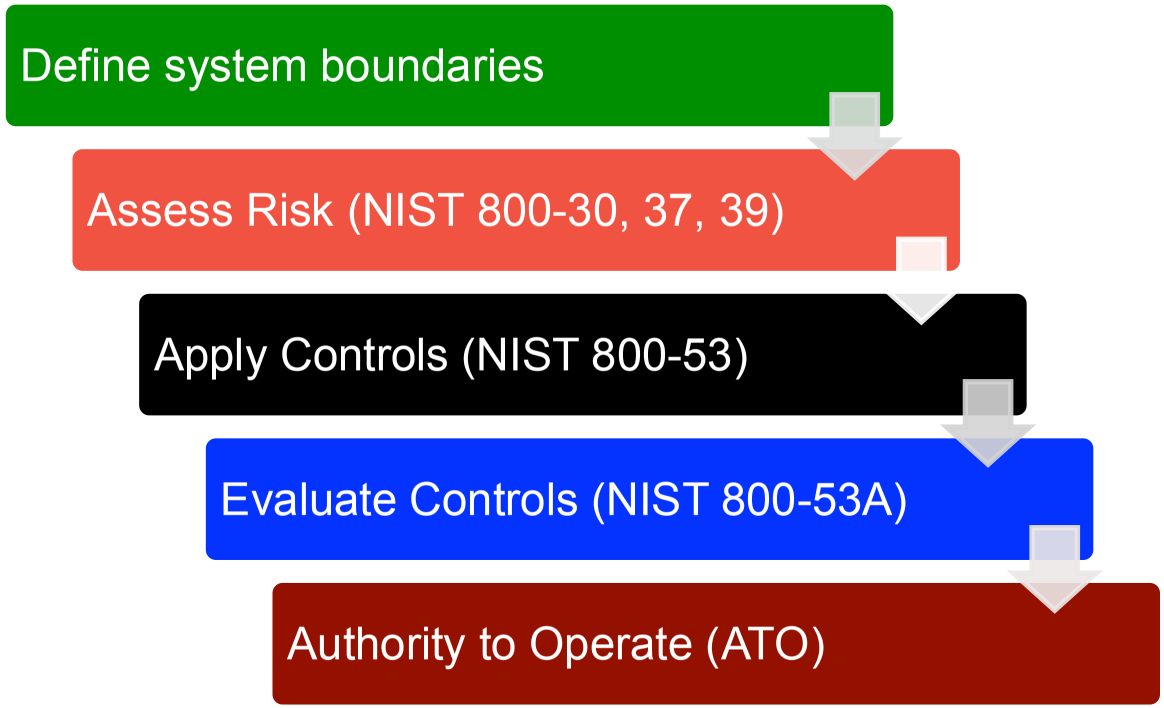
- When your systems collect, process, store, transmit, or use govt. owned data on behalf of the agency as part of a contract, and possibly, grant.
- The contract or grant will explicitly state FISMA terms (L, M, or H).
- New FISMA language may be added to existing contracts.
- Most grants and contracts don't involve FISMA.

DHHS 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 DHHS (or a component) is the principal, are covered by FISMA.

FISMA


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 boundary”.
- 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 to determine.

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 by severity is created.

Apply Controls

- The NIST guidance document NIST 800-53 is used to select controls that mitigate risk.
- The contract specifies the required security baseline (High, Medium, or Low).
- This can be a significant undertaking, especially for FISMA High. There are over 800 controls to consider.
- Many organizations will not accept FISMA High contracts as a result.

Evaluate Controls

- Evaluation includes detailed, regular security assessments.
- Evaluation 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

- The information security plan, etc. is submitted to the government agency.
- An ATO letter is issued by the agency to the business owner (and some authoritative information security unit like the ISO) authorizing operations of the system.
- If remediation is required and is not too serious, the agency will issue an Interim Authority To Operate (IATO). The IATO will have a defined end date. The problems must be fixed by that date.

Plan of Action & Milestones

- The POA&M describes remediation steps.
- Even if a contractor receives an ATO, there still may be items for which the agency requires remediation. These weaknesses may not be significant enough to withhold an IATO/ATO, but they still must be corrected.
- Someone at your institution (the ISO?) must track these items and ensure that they are completed.

Academic FISMA Infrastructures

- IU does not have a formal FISMA process in place yet. We're studying others.
- Of particular interest is Duke Medicine which has a relatively robust FISMA process.
- They have built an IaaS based, external FISMA hosting environment.
- Still, FISMA burdens are such that Duke won't accept FISMA High contracts.

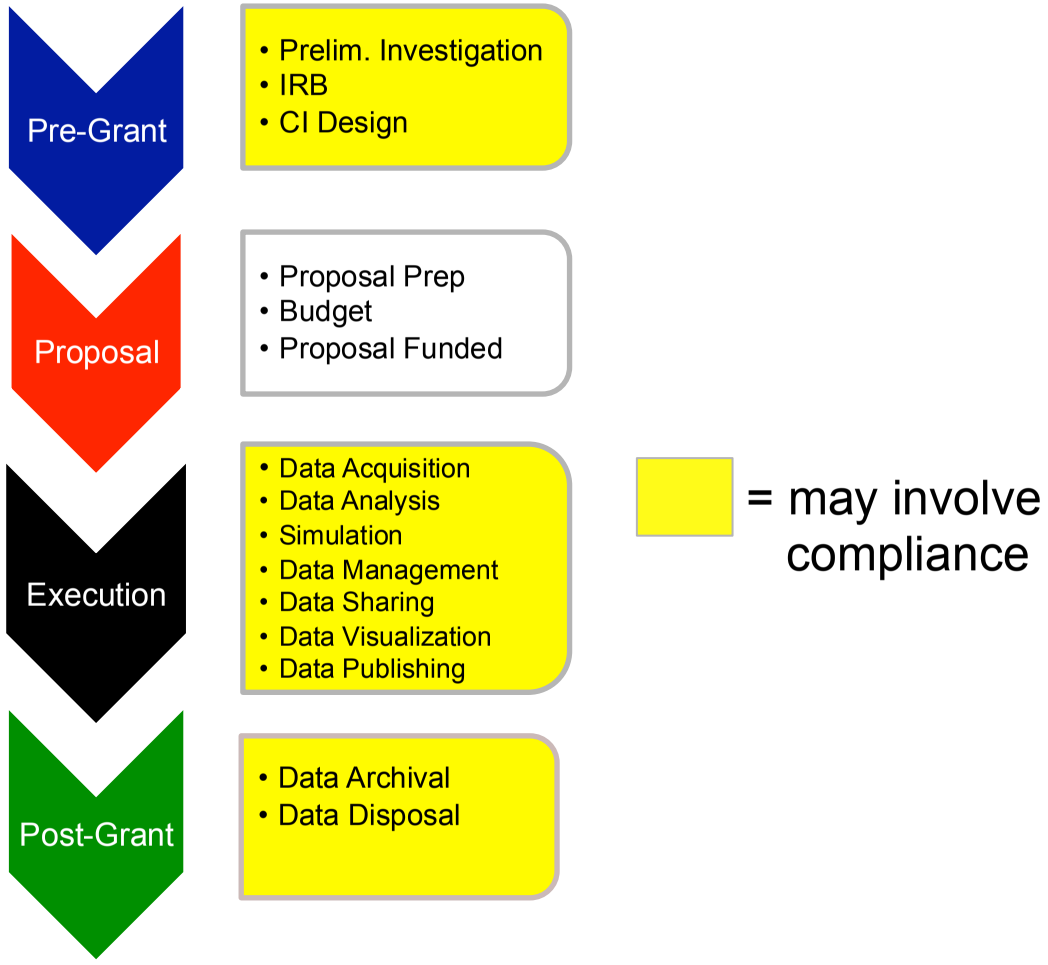
FISMA Requires Resources

- Duke estimates that, for each contract, it takes them 23-25 hours to review all documentation, make suggested contractual changes for agency negotiation, and create a FISMA management plan.
- They have PIs write in a FISMA line item in the budget.
- Be prepared to dedicate significant resources.

5. A Brief Risk Management Primer

Research Workflow & Compliance

Compliance in practice translates into protecting data end to end through its entire lifecycle, using sound risk management principles.



Managing Cybersecurity Risk

- = Identify, assess, prioritize, and mitigate risk to information security, on an ongoing basis.
- Focuses on risk, not just plugging security holes willy nilly.

Risk = {Threat/Vulnerability x Likelihood x Impact}

- A big threat from an existing vulnerability that is highly unlikely to be exploited or has little impact is low risk. You don't kill yourself over it.

Risk Assessment

- ... is the beginning of the road in cyber risk management. You cannot manage risk without first figuring it out.
- Many ways to assess risk, ranging all the way from pedestrian (& cheap) to highly complex (& expensive).
- Effort should be commensurate with budget, risk tolerance, and complexity.

Risk Management Framework

A mature RMF addresses risk holistically. It covers:

- Governance = institutional security organization, policies, sanctions, enforcement
- Risk management = assessment, mitigation through appropriate physical, administrative, technical controls, documentation
- Review = regular monitoring, reviews, reassessment, and mitigation
- Awareness and training

Industry Standard RMFs

- NIST RMF = National Institute of Standards and Technology RMF
- DIACAP = Dept. of Defense Information Assurance Certification Process
- OCTAVE = Operationally Critical Threat, Asset, and Vulnerability Evaluation
- HITRUST CSF = Health Information Trust Common Security Framework
- FAIR = Factor Analysis of Information Risk
- TARA = Threat Agent Risk Assessment

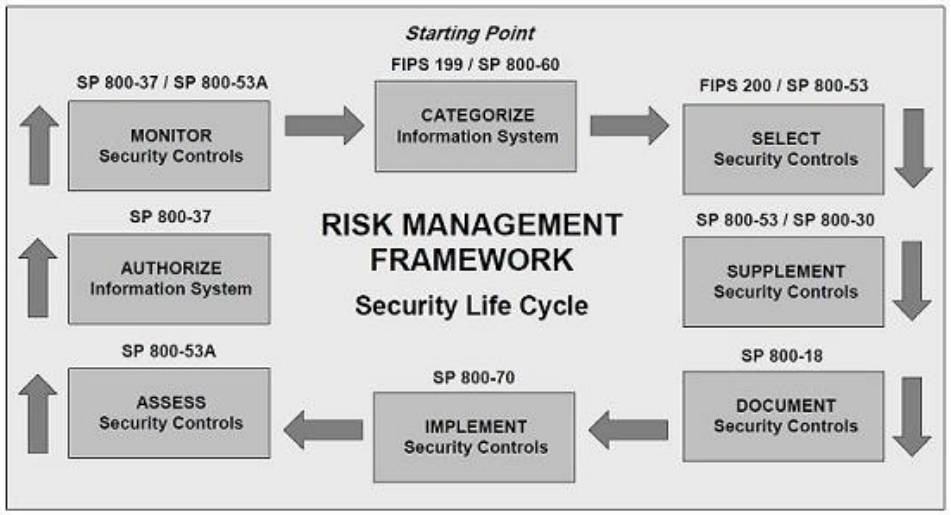
6. The NIST Risk Management Framework

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

The NIST RMF

- The FISMA slides earlier provide a taste of the NIST process to managing risk.
- Now we will take a detailed look at how the NIST RMF enables a comprehensive and yet flexible approach that adapts to any environment/scale.
- Translates into a security lifecycle.
- Steps are informed by NIST and other govt. guidance documents.

NIST Security Lifecycle



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

1. Categorize System

- FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems) helps categorize data based on confidentiality, integrity, and availability.
- Categories are Low, Medium, and High.
- NIST 800-60 (Guide for Mapping Types of Information and Information Systems to Security Categories) outlines a process for categorization.

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

FIPS 199 Categorization

Security Objective	Low	Moderate	High
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [44 USC, SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 USC, SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 USC, SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

2. Select Controls

- FIPS 200 (Minimum Security Requirements for Federal Information and Information Systems) essentially points to NIST 800-53.
- NIST 800-53 (Security & Privacy Controls for Federal Information Systems and Organizations) provides a catalog of ~1000* security controls. They are divided into control families with a baseline control and zero or more control enhancements (enhanced controls).

* 800-53 v4 has 240 baseline controls, 670 control enhancements, and 16 controls covering program management = 926 controls

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

Table D-2 provides a summary of the security controls and control enhancements from Appendix F that have been allocated to the initial security control baselines (i.e., low, moderate, and high). The sequence priority codes for security control implementation and those security controls that have been withdrawn from Appendix F are also indicated in Table D-2. In addition to Table D-2, the sequence priority codes and security control baselines are annotated in a priority and baseline allocation summary section below each security control in Appendix F.

TABLE D-2: SECURITY CONTROL BASELINES[92]

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P2	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	**Withdrawn**	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P1	AC-14	AC-14	AC-14
AC-15	**Withdrawn**	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P2	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1

[92] The security control baselines in Table D-2 are the initial baselines selected by organizations prior to conducting the tailoring activities described in Section 3.2. The control baselines and priority codes are only applicable to non-national security systems. Security control baselines for national security systems are included in CNSS Instruction 1253.

Controls

Security Baselines

FAMILY: ACCESS CONTROL

Control Family

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

1. Access control policy [*Assignment: organization-defined frequency*]; and
2. Access control procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW AC-1	MOD AC-1	HIGH AC-1

Baseline Control

AC-2 ACCOUNT MANAGEMENT

Control: The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];

b. Assigns account managers for information system accounts;

c. Establishes conditions for group and role membership;

d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

e. Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts;

f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];

g. Monitors the use of, information system accounts;

Control Enhancements

Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

Control Enhancements:

(1) *LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*

The organization explicitly authorizes access to [*Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information*].

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

(2) *LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*

The organization requires that users of information system accounts, or roles, with access to [*Assignment: organization-defined security functions or security-relevant information*], use non-privileged accounts or roles, when accessing nonsecurity functions.

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

(3) *LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*

The organization authorizes network access to [*Assignment: organization-defined privileged commands*] only for [*Assignment: organization-defined compelling operational needs*] and documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

(4) *LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS*

The information system provides separate processing domains to enable finer-grained allocation of user privileges.

Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; (ii) employing hardware and/or software domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32.

(5) *LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*

The organization restricts privileged accounts on the information system to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information

Control Baselines

- If you are aligning with the “low” security baseline*, you choose just those controls that are in the “LOW” column.
- More and more controls get added as you move to “medium” and “high” baselines**.
- FISMA low, medium, and high requirements correspond to these L,M,H security baselines.

* = Does not correspond to low (bad) security

** = Not to be confused with the FIPS 199 low, medium, high categorization

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

NIST Risk Assessment & Response

- Step 1: System Categorization
- Step 2: Threat Identification
- Step 3: Vulnerability Identification
- Step 4: Control Analysis
- Step 5: Likelihood Determination
- Step 6: Impact Analysis
- Step 7: Risk Determination
- Step 8: Control Recommendations
- Step 9: Results Documentation

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

Risk Assessment/Response Documentation

- The risk assessment process is documented. The documentation (the RA report) describes the methodology used, areas of risk and vulnerabilities, and severity.
- Risk response is documented in a document called the Plan of Action & Milestones (POA&M). It documents whether the risk was accepted, mitigated, or transferred and outlines the timelines and actions for mitigation.

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

3. Supplement Controls

- Results of the risk assessment may indicate supplemental controls needed to mitigate risk.
- NIST 800-30 (Guide for Conducting Risk Assessments) provides the steps to carry out a risk assessment.
- NIST risk assessment is based on threat/ vulnerability/likelihood/impact determination.

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

Document Controls

- NIST 800-18 (Guide for Developing Security Plans for Federal Information Systems) describes what to document how in what is known as the System Security Plan (SSP).
- The SSP describes system details and documents every NIST 800-53 security and privacy control currently in place, both base and enhancements.

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

4. Implement Controls

- Many 800-53 controls will already be in place (typically).
- You will need to implement supplemental/missing controls.
- Controls don't have to be implemented all at once. All you need is an implementation plan and timeline and document it in the Plan of Action and Milestones.

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

5. Assess Controls

- NIST 800-53A (Guide for Assessing the Security Controls in Federal Information Systems & Organizations) describes how to develop a plan to assess desired security controls.
- It helps build assurance into the RMF.
- The organization is left to devise details of the assessment, for instance regular penetration testing.

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

6. Authorize Information System

- NIST 800-37 (Guide for Applying the Risk Management Framework to Federal Information Systems) describes how to leverage the NIST RMF once it is in place. It describes all of the NIST steps in the previous figure in detail.
- Authorization is based upon the information in the authorization package, namely the POA&M, the SSP, and the RA report.

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

7. Monitor System

- NIST 800-37 also describes how security controls should be monitored on an ongoing basis for system changes & their impact.
- It provides guidance on regular security/risk assessments, remediation, system removal, decommissioning, etc.
- Continuous monitoring is an essential requirement of FISMA.

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

7. Building a Risk Management Framework

Choosing a RMF

- You can choose from any number of RMFs available today.
- FAIR is a good one at modest scales.
- OCTAVE makes you sit down, brainstorm, and figure out risk.
- NIST is good for HIPAA and mandated for FISMA.
- We chose NIST because it's a standard. Most any rule/regulation can be mapped to it.

Building a RMF at IU

- We chose NIST.
- We wanted to create a standards based foundation capable of handling all cyber compliance at IU (ultimately).
- It is in use now to align with HIPAA.

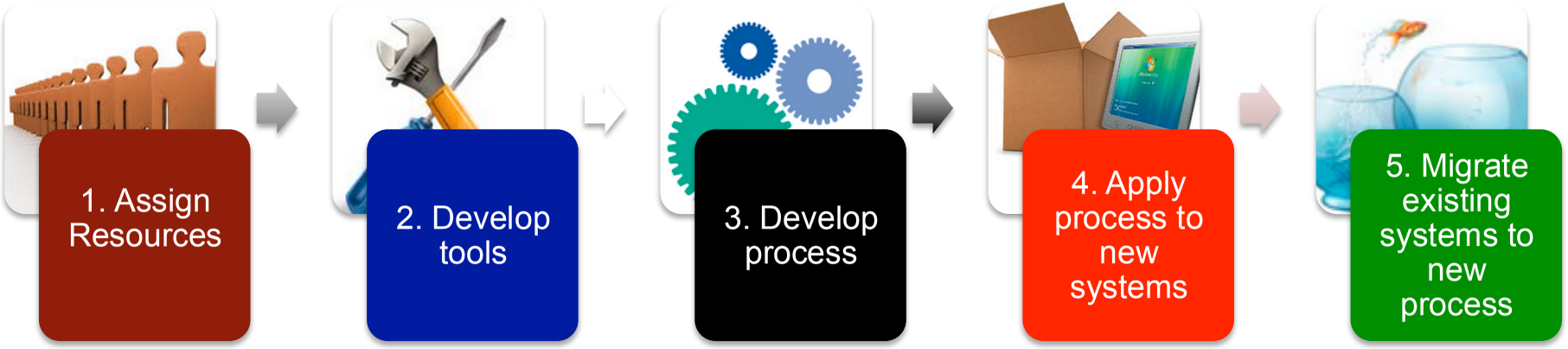
Design Goals

- Should be
  - lightweight and nimble
  - easily extensible to FISMA, etc.
  - reusable
  - doable (within budget, other constraints)
  - able to leverage pre-existing structure
- ??.

Pre-existing Structure

- Resources
  - Staff
  - HIPAA tools & expertise
- Processes
  - Workflows
  - Oversight
- Relationships
  - Compliance Office
  - IT units

Implementation Steps



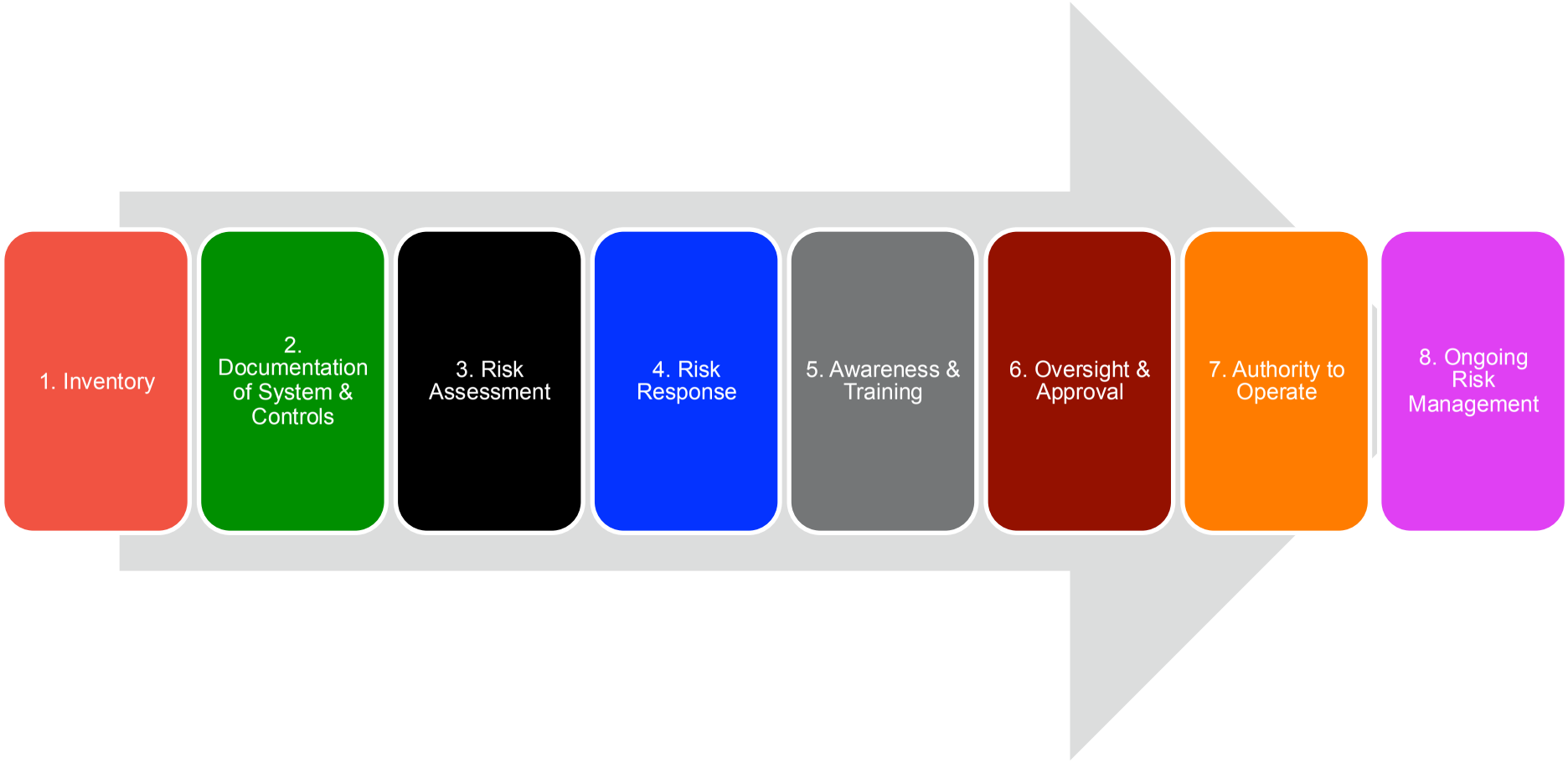
1. Assign Resources

- The project took about a year and 1 FTE.
- We align with the NIST “low” security baseline but also document pre-existing control enhancements.

2. Develop Tools

- We do not use the NIST process literally. We have adapted it to meet our goals & needs.
- The project took about a year and 1 FTE.
- We align with the NIST “low” security baseline but also document pre-existing control enhancements.

3. Develop Process



Inventory

- 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.

The Inventory

System Inventory

System	Location	Prod/Test	HW	PII Location	H/W Maint. Contract?	HIPAA BAA(1)?	OS	Version	Highest Data Classi-fication	Critical Data Category	HIPAA Aligned?	Access Method	Accessed Directly by End Users?	End User Facing Applica-tions	Authen. Methods	Open Host Ports	Data Center Firewall allows ports	Host Firewall allows ports	Last Host Scan & Result	Retire Date & How Disposed
system1.uits.iu.edu	<Location> Data Center	P	Dell PowerEdge XXXX	/var/html /var/lib/mysql	Yes	No, vendor does not have access to the system	RHEL	6.4	Critical	ePHI	No	SSH, HTTP, HTTPS	Yes	<Name>	Active Directory, /etc/passwd	80, 22, 443	80, 443	22, 80, 443	1/1/2014, Clean	1/5/13, Storage media removed and destroyed
system2.uits.iu.edu			II																	

Software Inventory

System	Software	Version	Patch Level	Support Contract?	HIPAA BAA?	Last App Scan	Vulns Found?	How Addressed ?	Authentic ation
<System>	Apache HTTPD	2.4		N	N/A	N/A	N/A		AD
	MySQL	5.8		N	N/A	N/A	N/A		
	Perl	8.4.1		N	N/A	N/A	N/A		
	Java	7.1		N	N/A	N/A	N/A		

Incident Log

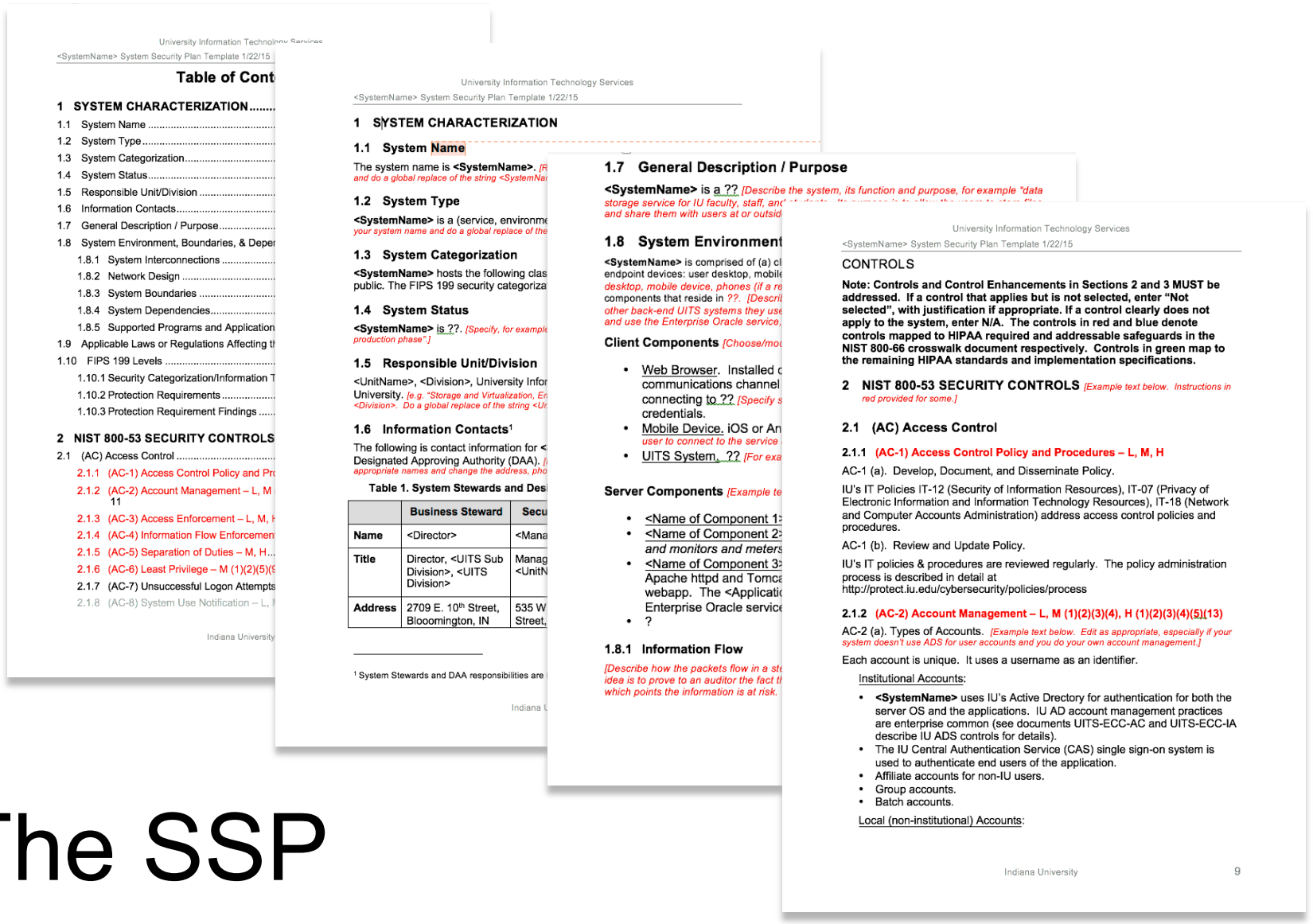
Name	Incident Date	Software	Vuln. Exploited	Incident Details	How Detected?	Date ISO Notified	How Responded?	ISO ATO Issued on	ATO = Authority to Operate
<System>	1/3/14	?	?	?	ISO IDS	1/4/14	Patch #XXX applied ?	1/10/14	

Privileged Access Inventory

System	Name	Access Authorized	Type of Access	Access Terminated
<?>.uits.iu.edu <?>.uits.iu.edu	Name1	1/1/2010	System Administrator	
	Name2	1/1/2010	System Administrator	
	Name3	1/1/12	System Administrator	
	Name4	1/1/12	System Administrator	
	Name5	1/1/12	System Administrator	

Documentation of System & Controls

- Controls are documented in the "System Security Plan" or SSP.
- 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.



University Information Technology Services
<SystemName> System Security Plan Template 1/22/15

Table of Cont

1 SYSTEM CHARACTERIZATION.....
1.1 System Name
1.2 System Type
1.3 System Categorization
1.4 System Status
1.5 Responsible Unit/Division
1.6 Information Contacts
1.7 General Description / Purpose
1.8 System Environment, Boundaries, & Deper
1.8.1 System Interconnections
1.8.2 Network Design
1.8.3 System Boundaries
1.8.4 System Dependencies
1.8.5 Supported Programs and Application
1.9 Applicable Laws or Regulations Affecting t
1.10 FIPS 199 Levels
1.10.1 Security Categorization/Information T
1.10.2 Protection Requirements
1.10.3 Protection Requirement Findings
2 NIST 800-53 SECURITY CONTROLS
2.1 (AC) Access Control
2.1.1 (AC-1) Access Control Policy and Pr
2.1.2 (AC-2) Account Management – L, M
11
2.1.3 (AC-3) Access Enforcement – L, M,
2.1.4 (AC-4) Information Flow Enforcemen
2.1.5 (AC-5) Separation of Duties – M, H...
2.1.6 (AC-6) Least Privilege – M (1)(2)(5)(
2.1.7 (AC-7) Unsuccessful Logon Attempts
2.1.8 (AC-8) System Use Notification – L,

Indiana University

University Information Technology Services
<SystemName> System Security Plan Template 1/22/15

1 SYSTEM CHARACTERIZATION

1.1 System Name

The system name is **<SystemName>**. *[R*
and do a global replace of the string <SystemNa

1.2 System Type

<SystemName> is a (service, environme
your system name and do a global replace of the

1.3 System Categorization

<SystemName> hosts the following clas
public. The FIPS 199 security categoriza

1.4 System Status

<SystemName> is ??. *[Specify, for example*
production phase".]

1.5 Responsible Unit/Division

<UnitName>, <Division>, University Infor
University. *[e.g. "Storage and Virtualization, Er*
<Division>. Do a global replace of the string <Ur

1.6 Information Contacts[1]

The following is contact information for <
Designated Approving Authority (DAA). *[*
appropriate names and change the address, pho

Table 1. System Stewards and Desi

	Business Steward	Secu
Name	<Director>	<Mana
Title	Director, <UITS Sub Division>, <UITS Division>	Manag <UnitN
Address	2709 E. 10th Street, Blooomington, IN	535 W Street,

[1] System Stewards and DAA responsibilities are

Indiana U

1.7 General Description / Purpose

<SystemName> is a ?? *[Describe the system, its function and purpose, for example "data*
storage service for IU faculty, staff, and
and share them with users at or outsid

1.8 System Environment

<SystemName> is comprised of (a) cl
endpoint devices: user desktop, mobile
desktop, mobile device, phones (if a re
components that reside in ??. *[Descri*
other back-end UITS systems they use
and use the Enterprise Oracle service,

Client Components *[Choose/mo*

- Web Browser. Installed
communications channel
connecting to ?? *[Specify s*
credentials.
- Mobile Device. iOS or An
user to connect to the service
- UITS System. ?? *[For exa*

Server Components *[Example te*

- <Name of Component 1>
- <Name of Component 2>
and monitors and meters
- <Name of Component 3>
Apache httpd and Tomca
webapp. The <Applicati
Enterprise Oracle service
- ?

1.8.1 Information Flow

[Describe how the packets flow in a st
idea is to prove to an auditor the fact t
which points the information is at risk.

University Information Technology Services
<SystemName> System Security Plan Template 1/22/15

CONTROLS

Note: Controls and Control Enhancements in Sections 2 and 3 MUST be addressed. If a control that applies but is not selected, enter "Not selected", with justification if appropriate. If a control clearly does not apply to the system, enter N/A. The controls in red and blue denote controls mapped to HIPAA required and addressable safeguards in the NIST 800-66 crosswalk document respectively. Controls in green map to the remaining HIPAA standards and implementation specifications.

2 NIST 800-53 SECURITY CONTROLS *[Example text below. Instructions in red provided for some.]*

2.1 (AC) Access Control

2.1.1 (AC-1) Access Control Policy and Procedures – L, M, H

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

IU's IT Policies IT-12 (Security of Information Resources), IT-07 (Privacy of Electronic Information and Information Technology Resources), IT-18 (Network and Computer Accounts Administration) address access control policies and procedures.

AC-1 (b). Review and Update Policy.

IU's IT policies & procedures are reviewed regularly. The policy administration process is described in detail at http://protect.iu.edu/cybersecurity/policies/process

2.1.2 (AC-2) Account Management – L, M (1)(2)(3)(4), H (1)(2)(3)(4)(5)(13)

AC-2 (a). Types of Accounts. *[Example text below. Edit as appropriate, especially if your system doesn't use ADS for user accounts and you do your own account management.]*

Each account is unique. It uses a username as an identifier.

Institutional Accounts:

- **<SystemName>** uses IU's Active Directory for authentication for both the server OS and the applications. IU AD account management practices are enterprise common (see documents UITS-ECC-AC and UITS-ECC-IA describe IU ADS controls for details).
- The IU Central Authentication Service (CAS) single sign-on system is used to authenticate end users of the application.
- Affiliate accounts for non-IU users.
- Group accounts.
- Batch accounts.

Local (non-institutional) Accounts:

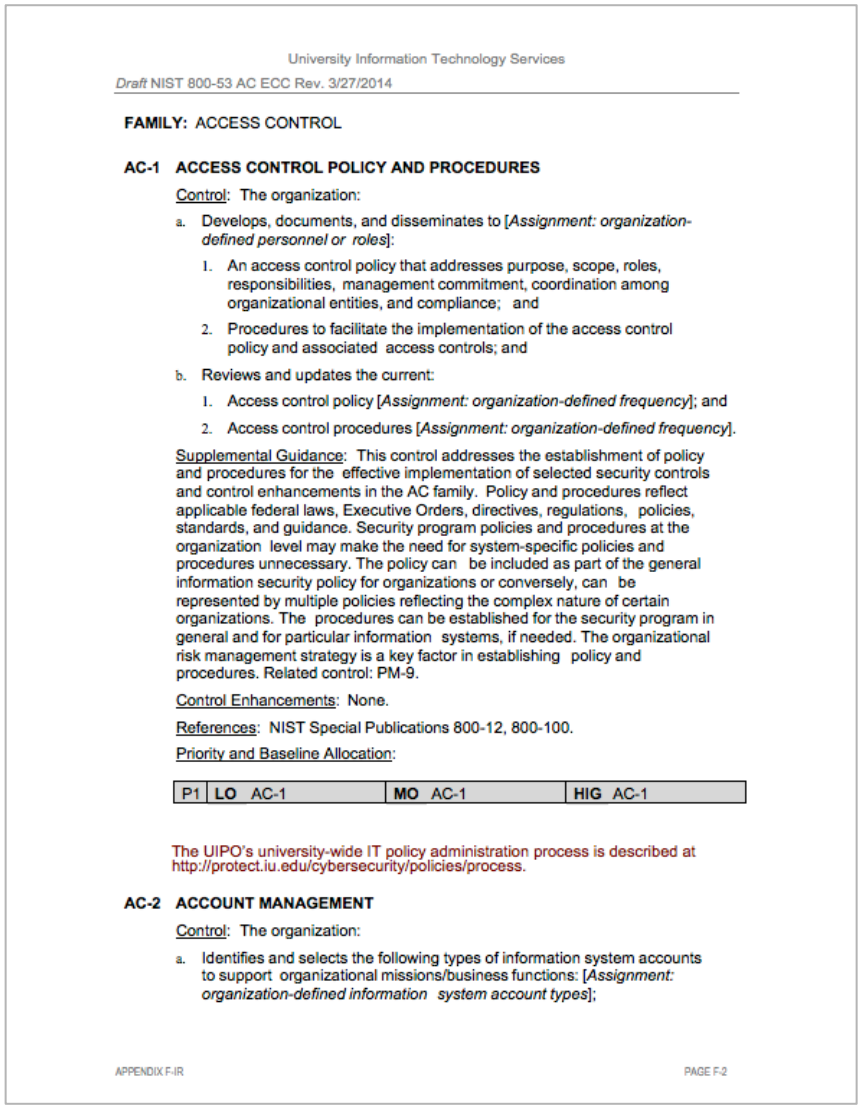
Indiana University 9

The SSP

Enterprise Common Controls

- Individual SSPs describe hundreds of controls.
- A large number of these are inherited from the organization. They apply to all systems (enterprise common controls).
- It is wasteful to include them every time in each SSP.
- So enterprise common controls (ECC) are documented separately.
- Individual SSPs simply point to the ECC docs where needed.

The ECC Document



University Information Technology Services

Draft NIST 800-53 AC ECC Rev. 3/27/2014

FAMILY: ACCESS CONTROL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

1. Access control policy [*Assignment: organization-defined frequency*]; and
2. Access control procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LO** AC-1	**MO** AC-1	**HIG** AC-1

The UIPO's university-wide IT policy administration process is described at http://protect.iu.edu/cybersecurity/policies/process.

AC-2 ACCOUNT MANAGEMENT

Control: The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];

APPENDIX F-IR PAGE F-2

Risk Assessment

- External, third party (expensive!) assessments every few years.
- The unit does internal risk self-assessments (RSA).
- Managers & sys admins brainstorm and identify areas of vulnerabilities and risk for the system.
- The RSA report documents risk areas, controls that address those risks, residual vulnerabilities and risks, and risk severity.

The RSA Report

					Existing Controls				
Threat/Vuln. Pair #	Threat Event	Area of Exploitable Vulnerability	Risk Category	Risk Details	Mitigating NIST Controls	Mitigating NIST Controls/Factors Summary	Residual Vulnerability	Residual Risk Level	Risk Response
1	Attack	Account management	Compromise of confidentiality and integrity, lack of accountability	Data exposure due to weak account management practices (account provisioning, locking, deprovisioning)	AC-2	Use of institutional accounts and mature account management practices.		Low	Mitigated by existing controls
2	Attack	Password management	Compromise of confidentiality and integrity	Data exposure due to weak password management practices (password strength, expiration, password changes without validation, passwords in scripts)	IA-2, IA-4, IA-5, IA-6, IA-7	Use of institutional accounts and mature password management practices. No passwords in scripts.		Low	Mitigated by existing controls
3	Attack, reconnaisance	Logical access controls	Compromise of confidentiality and integrity	Data exposure due to unauthorized access (firewall ports, generic accounts, accounts with no passwords, unsecured remote access)	AC-3, AC-5, AC-6, IA-2, IA-3, IA-4, SC-7	Most system components behind Data Center firewall. Generic accounts/accounts with blank passwords disabled.	(a) Application access to external data sources (b) <device> located outside Data Center firewall	(a) Moderate (b) Moderate	See POA&M
4	Attack	Privilege management	Compromise of confidentiality and	Data exposure due to unauthorized access resulting from weak privilege mismanagement (direct administrator account use, no	AC-1, AC-2, AC-3, AC-4, AC-13,	Explicit privilege authorization	No individual accountability due to administrative account	Moderate	See POA&M

Risk Response

- A "Plan of Action & Milestones" or POA&M documents the response to residual risks not addressed by existing controls.
- 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. We try our best to address them, for instance through training.

The POA&M

Risk	Risk Level	Action	Milestone	Date
Application access to external data sources	Moderate	Risk accepted pending evaluation. Risk will be calculated for each specific application installed and the nature of connection and addressed accordingly.	Each application connecting to an external source will be analyzed independently to evaluate and mitigate risk.	
<device> located outside Data Center firewall	Moderate	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.		
No individual accountability due to shared administrative accounts	Moderate	Risk addressed in the next column. The Citrix application requires the use of administrative accounts.	The risk will be mitigated via an access inventory of privileged access.	6/1/14

Staff Training

- Annual training is mandated for both management and staff responsible for operating the system.
- 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
- All security related is documented in a training log.

User Training

- We provide online training and awareness via our Knowledge Base, YouTube videos, local media, in person classes, and email alerts.
- We recently (really) raised awareness by launching our own phishing attack.
- Fortunately, big breaches are having some effect.
- As we work individually with researchers, we train them as we help them create their own (HIPAA) documentation describing how they are protecting their end.

Oversight

- The complete compliance documentation package is sent to the IU HIPAA Privacy and Security Office, the University Information Security Office, and Internal Audit.
- They only do a light review presently due to lack of resources. This will hopefully change soon.
- High impact systems and those that have had major incidents do get a more thorough review.

Authority to Operate

- There is not a formal ATO process in place today.
- Alignment is essentially self asserted (with oversight as stated earlier).
- No one is willing to sign on a dotted line accepting risk for the institution (this is very typical of most institutions).
- For FISMA, all this will need to change.

Ongoing Risk Management

- Once a system comes under alignment, it becomes subject to regular, ongoing risk management until decommissioning. We require:
  - Semi-annual reviews, risk re-assessments, and documentation updates.
  - Continuous, automatic monitoring of systems.
  - Annual training.
  - Oversight.
  - External assessments.

4. Apply Process to New Systems

- Having started in 2007, most of our systems had gone through the old, non-NIST process.
- New systems needing alignments were naturally suited to the new process.
- While we worked on the NIST process, more and more ePHI began landing on our systems.
- Luckily, we were ready.
- To date, around 5 systems have gone through the new process.

5. Migrate Existing Systems

- Around 30 systems had gone through the old process.
- We are just starting to migrate these systems to the new process.
- Migration involves gutting the old documentation, salvaging what we can from it for the new, and adding the risk self-assessment/response piece.
- We expect it will take at least a year to finish the migration.

8. Using the RMF to Address HIPAA and FISMA

RMF to Compliance

- The RMF by itself does not give you compliance … but it makes complying a lot easier.
- Building the RMF is a demanding but one time exercise. Compliance is an ongoing activity as new systems are aligned.
- Having the RMF allows you to concentrate on the system being aligned and not worry about common dependencies, etc.
- It gives you confidence in your ability to comply.

The IU Approach

- Align all systems with NIST first, not individual regulations.
- Map the regulation to NIST. Such mappings already exist, for instance for HIPAA.
- We can do the same for other rules and regulations such as IU's critical data requirements.

From NIST to HIPAA

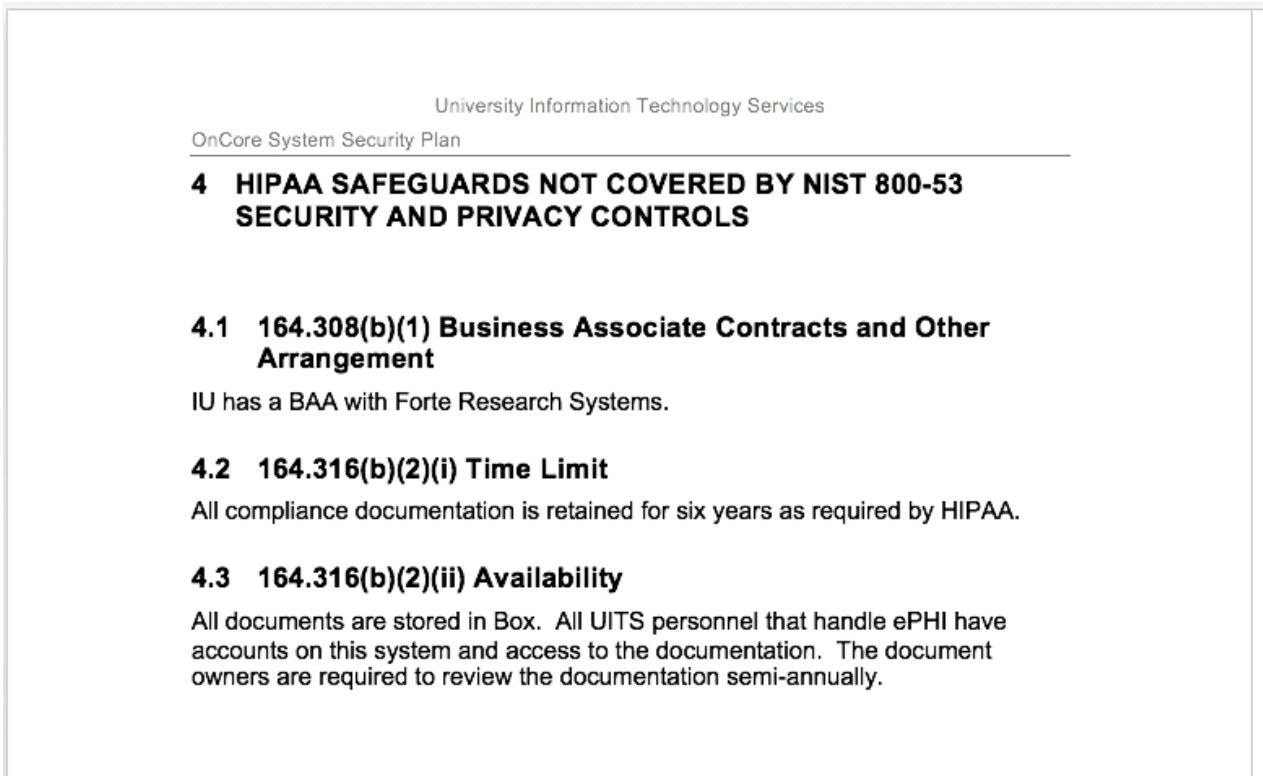
- NIST 800-66 (An Introductory Resource Guide for Implementing the HIPAA Security Rule) provides HIPAA to NIST mapping.
- Our System Security Plan contains a HIPAA section that addresses HIPAA requirements that do not map to NIST.
- We can do the same for other rules and regulations such as IU's critical data requirements.

NIST 800-66 HIPAA to NIST Map

Table 4. HIPAA Standards and Implementation Specifications Catalog

Section of HIPAA Security Rule	HIPAA Security Rule Standards	Implementation Specifications	NIST SP 800-53 Security Controls Mapping	NIST Publications Crosswalk
Administrative Safeguards				
164.308(a)(1)(i)	Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.		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 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-2, RA-3, RA-4	
164.308(a)(1)(ii)(B)		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)(C)		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)(D)		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)(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	NIST SP 800-12 NIST SP 800-14 NIST SP 800-37 NIST SP 800-53 NIST SP 800-53A NIST SP 800-100

IU SSP Section Addressing HIPAA



University Information Technology Services

OnCore System Security Plan

4 HIPAA SAFEGUARDS NOT COVERED BY NIST 800-53 SECURITY AND PRIVACY CONTROLS

4.1 164.308(b)(1) Business Associate Contracts and Other Arrangement

IU has a BAA with Forte Research Systems.

4.2 164.316(b)(2)(i) Time Limit

All compliance documentation is retained for six years as required by HIPAA.

4.3 164.316(b)(2)(ii) Availability

All documents are stored in Box. All UITS personnel that handle ePHI have accounts on this system and access to the documentation. The document owners are required to review the documentation semi-annually.

HIPAA Process for Researchers

HIPAA Process for IT Units

FISMA for Agencies

- FISMA = NIST + Accreditation + ATO + Reporting.
- Accreditation:
  - Security certification
  - Submission of documentation (SSP, RA, POA&M)
- ATO or interim ATO by the agency.
- Reporting:
  - SSP update
  - POA&M update
  - Status of continuous monitoring activities - vulnerabilities discovered, security impact analysis, security control monitoring

FISMA in Academia

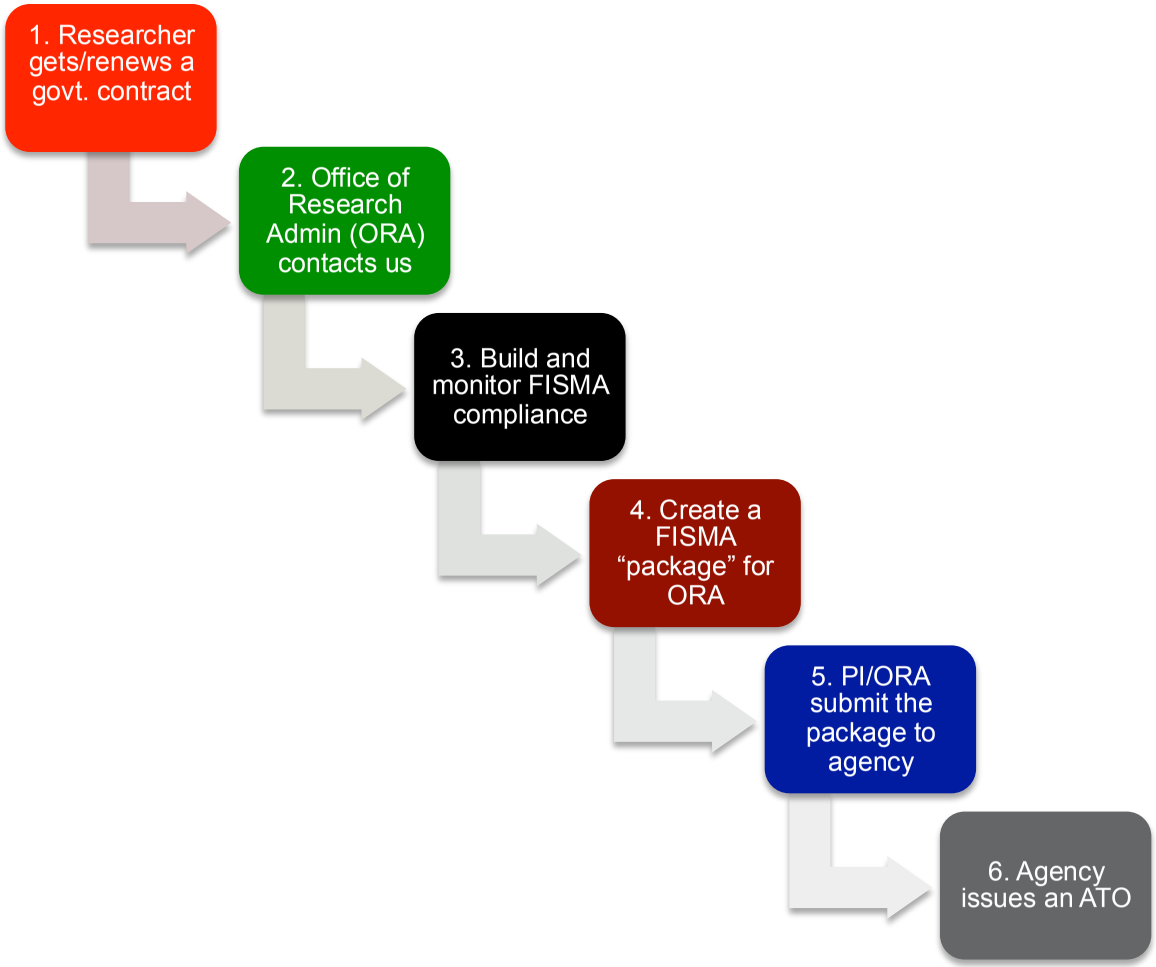
- Starts with FISMA language in a grant/contract.
- Triggers a local administrative process.
- Requires the NIST RMF/documentation.
- The local administrative unit submits FISMA paperwork to the agency.
- The agency responds. An iATO may be issued.
- Remediation and more paperwork is then required.
- The final result is an ATO by the agency.

Local Administrative Process

- Grants Administrators/Business Development
  - Identify and notify Research Administration of FISMA terms in contract
  - Make sure the budget includes FISMA costs
  - Identify and document key IT security personnel
  - Make sure all documents that are referenced are included
- PI/Study Team
  - Clearly describe the scope of work
  - Identify all potential subcontractors and their scope of work
- PI/Study Team and IT Team
  - Clearly describe data flows
  - In detail, describe all systems used for contract work

However, a PI may be able to negotiate things down to something agreeable to the agency depending on factors such as the origin or sensitivity of the data, etc.

Institutional FISMA Process



Outcomes

- At IU, NIST has allowed us to focus on a single standard and process for cyber compliance.
- We are beginning to establish an institutional structure for HIPAA/FISMA & other current and future regulations.
- Units engaged in compliance like the process.
- We feel confident in our ability to handle audits.

9. The Future

1. Cloud

- Cloud seriously complicates compliance.
- … but, many cloud vendors are now providing HIPAA "compliant" solutions and willing to sign a HIPAA BAA.
- This includes Amazon (AWS) and Microsoft (Azure). It's possible to build compliant solutions.
- IU just allowed ePHI on IU's enterprise Box … but it required much due diligence and many local controls.

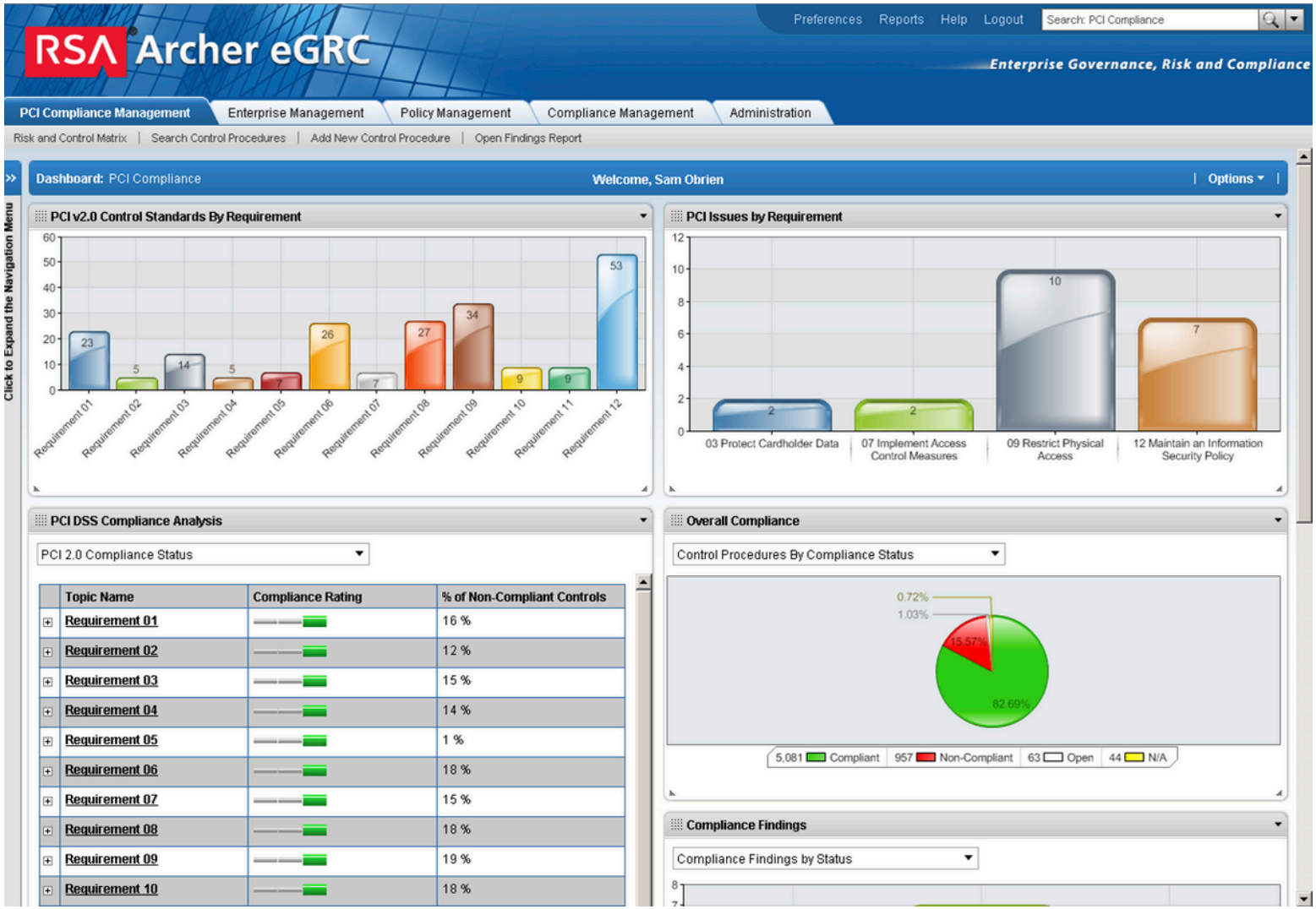
FedRAMP

- Federal Risk and Authorization Management Program for secure cloud certification.
- Cloud vendors must have a FedRAMP certification to comply with FISMA and thus be eligible for govt. contracts.
- Presumably, one can use a FedRAMP certified cloud solution to build a FISMA compliant solution. It's unlikely to be cheap though.

2. Automation

- Automated inventory & configuration management systems, automated checks for existing/new vulnerabilities & changes in regulations, automated alerts, continuous monitoring for evolving risks, etc. (SANS top 20 is a good source for information.)
- Electronic governance, risk, and compliance (e-GRC) systems fed by a these which also manages BAAs, policies, audits, vendors, incidents, etc.

  (Examples of e-GRC systems includes RSA Archer, LockPath, Compliance 360, GRC Cloud, Modulo, Agiliance, Accelus, etc.)


RSA Archer eGRC
Preferences Reports Help Logout
Search: PCI Compliance
Enterprise Governance, Risk and Compliance
PCI Compliance Management
Enterprise Management
Policy Management
Compliance Management
Administration
Risk and Control Matrix | Search Control Procedures | Add New Control Procedure | Open Findings Report
Click to Expand the Navigation Menu
Dashboard: PCI Compliance
Welcome, Sam Obrien
Options
PCI v2.0 Control Standards By Requirement
Requirement 01
Requirement 02
Requirement 03
Requirement 04
Requirement 05
Requirement 06
Requirement 07
Requirement 08
Requirement 09
Requirement 10
Requirement 11
Requirement 12
PCI Issues by Requirement
03 Protect Cardholder Data
07 Implement Access Control Measures
09 Restrict Physical Access
12 Maintain an Information Security Policy
PCI DSS Compliance Analysis
PCI 2.0 Compliance Status
Topic Name
Compliance Rating
% of Non-Compliant Controls
Requirement 01 16 %
Requirement 02 12 %
Requirement 03 15 %
Requirement 04 14 %
Requirement 05 1 %
Requirement 06 18 %
Requirement 07 15 %
Requirement 08 18 %
Requirement 09 19 %
Requirement 10 18 %
Overall Compliance
Control Procedures By Compliance Status
0.72%
1.03%
15.57%
82.69%
5,081 Compliant
957 Non-Compliant
63 Open
44 N/A
Compliance Findings
Compliance Findings by Status

3. Metrics Based Security?

- Cybersecurity today is mostly devoid of metrics or models that are useful.
- There is a desire to move to quantitative cybersecurity but it's long ways away.
- SANS has done a great job with their top 20 controls. While not quantitative, they are based on actual attack metrics, not theoretical attacks.
- Most useful are their "low hanging fruits", controls that can prevent a majority of the common attacks.

4. Evolution of Approach

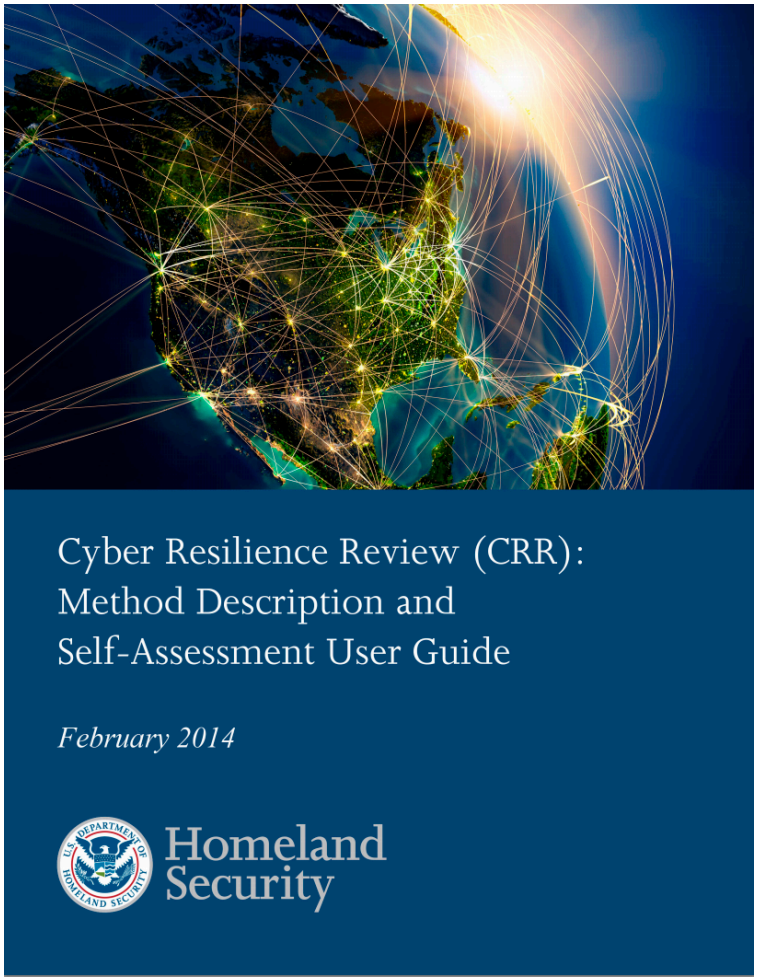
- The internet started with little to no security.
- This was followed by security “best practices”.
- Cybersecurity standards such as ISO, NIST, etc. emerged.
- Existing risk management concepts were then borrowed from other areas.
- There is growing hopelessness and realization that the bottom line is to achieve the ability to function despite attacks/incidents.

"Cyber Resilience"

We can approach cybersecurity in human health terms:

- Diseases (successful cyber attacks) are inevitable.
- Prevention, detection, intervention (incident response, DR/BCP), monitoring & ongoing treatment (cyber risk management) are known to be effective in curing or containing disease.

- A major difference is the absence of cure!
- Change assumption from "if I have enough controls, all will be well" to *"I will be hacked"*.
- Approach the problem holistically, not piecemeal.



Fore more information, see US-CERT's Cyber Resilience Review (CRR) site.

https://www.us-cert.gov/ccubedvp/self-service-crr

10. Conclusion

Compliance is Imminent

- Biomedical research is on a collision course with research CI.
- With little biomedical research CI around, an increasingly larger volume of ePHI can be expected to land on our systems.
- Grants and contracts will be asking for FISMA compliance.
- … So embrace it.

HIPAA/FISMA are Doable

- The government does not expect you to undertake herculean measures or build walled gardens.
- Rules and regulations affecting information security are about using best practices, something we should be doing anyway.
- Most of us have sufficiently good information security in place already. It won't take a gargantuan effort to go all the way.

Opportunities and Threats

- Not having a compliance process in place means missed opportunities, particularly for ‘Big Data’ applications in health sciences research.
- … and therefore for funding.
- Managing ePHI without a RMF in place makes life hard and creates a potential for institutional liability and reputational damage.

Benefits

- A standards based RMF implementation makes you rule/regulation proof.
- Customers with sensitive data will trust your shop, bringing new business.
- Your compliance folks will send people your way (ours do).
- You will better serve researchers/your mission.

Questions/Discussion

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
  http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
- NIST 800-53: Recommended Security Controls
  http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
- NIST 800-53A: Guide for Assessing Security Controls
  http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf
- FIPS 199: Federal Systems Minimum Security Requirements
  http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- FIPS 200: Federal Systems Minimum Security Requirements
  http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
- NIST HIPAA Security Rule Toolkit
  http://scap.nist.gov/hipaa/
- NIST Templates (email me)

Interesting Reading

- "Why Cybersecurity is Not Enough: You Need Cyber Resilience": http://www.forbes.com/sites/sungardas/2014/01/15/why-cyber-security-is-not-enough-you-need-cyber-resilience/
- "Why FISMA is Not Enough for the IoT": http://fcw.com/articles/2014/08/15/iot-security-concerns.aspx
- "FISMA Continues to Challenge": http://fcw.com/articles/2012/03/14/federal-agencies-fisma-compliance.aspx
- "Federal Agencies Still Lag on FISMA Compliance": http://www.darkreading.com/risk-management/federal-agencies-still-lag-on-fisma-compliance/d/d-id/1103399?

Contact

Anurag Shankar
ashankar@iu.edu