Building a NIST Risk Management Framework for HIPAA and FISMA Compliance

Anurag Shankar
Center for Applied Cybersecurity Research
Indiana University

NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure
August 16, 2016

Schedule

1. Introduction	9:00 – 9:05
2. Research Compliance	9:05 – 9:15
3. HIPAA & FISMA	9:15 – 10:00
4. Risk Management	10:00 – 10:15
5. The NIST Risk Management Framework	10:15 – 11:00
Break	11:00 – 11:30
6. Leveraging the Framework	11:30 – 12:00
7. Addressing HIPAA & FISMA	12:00 – 12:30
8. The Future	12:30 – 12:45
9. Conclusion	12:45 – 1:00

Introductions

1. Introduction

Motivation

- Threats to privacy and security
  - Security of identifiable healthcare data, in original or derived form
  - Security of government owned data

Threats to Health Data

- Healthcare is growing to be one of the most heavily targeted sectors now, breaches up 25%.
- Patient records – conveniently consolidated, exploitable info – yield the highest price on the black market today ($50-100/record).
- Data being used for identity & insurance fraud, blackmail/extortion, celebrity snooping, etc.

The Going Rate*

- Medical records: $82.90
- Social Security: $55.70
- Payment details: $45.10
- Physical location info: $38.40
- Marital status: $6.10
- Name and gender: $2.90

* Privacy Rights Clearinghouse data survey

Threats to Govt. Data

- Massive attack volume: 300 million attacks/day against the State of Utah alone.
- A survey* in 2015 revealed that govt. IT personnel now consider “the negligent insider” a bigger threat than hackers in China.
- GAO survey** in 2015 found 15-24 agencies with “persistent weaknesses”.

* https://fcw.com/pages/hpsp/hpsp-10.aspx
** http://www.gao.gov/products/GAO-15-714

New Trends

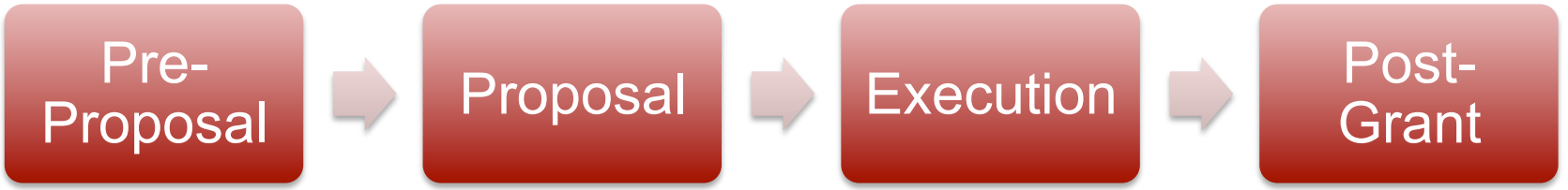
- Scary new attack targets - transportation, medical devices, smart homes (Internet of Things or IoT).
- Attack sophistication ⬆ - we are now seeing “ghostware”, “morphware”, & “virtualware”. Low-tech phishing is still a huge threat.
- Intelligence agencies have identified data manipulation attacks as the next big threat.

Challenges for Researchers

- Increasingly stringent cybersecurity strings attached to government funding.
- Confusing laws.
- Lack of in-house compliance expertise.
- Knowledgeable peers not always easy to find.
- Cost.

2. Research Compliance

Research Workflow & Cyber Compliance



Preliminary Investigation
IRB
CI Design

Preparation
Budgeting
Funding

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

Data Archival
Data Disposal

red = may involve compliance

Compliance requires protecting data end to end, through its entire lifecycle.

Laws

- Common Rule (Protection of Human Subjects) - 1981
- Health Insurance Portability & Accountability Act (HIPAA) - 1996
- FDA CFR 21 Part 1 – 1997
- Federal Information Security Management Act (FISMA) – 2002

NIH

- Funds health research; identifiable health data may be* subject to HIPAA.
- Traditional NIH funded researchers use a well established structure for HIPAA and FDA compliance (IRBs, Offices of Human Subjects Research/HIPAA Compliance, etc.)
- NIH & its subcontractors are subject to FISMA.

* HIPAA doesn't apply to all health data

NSF

- HIPAA has not been a big issue so far since NSF doesn't directly fund health research.
- NSF does fund human subjects research (e.g. psychology) subject to the Common Rule*/IRBs.
- But health data leaking into NSF facilities = HIPAA.
- NSF/subcontractors also subject to FISMA.

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

Issues

- Cyber regulations are not prescriptive; you have to interpret them.
- Interpretation is often difficult because scientists/IT providers are not regulatory experts.
- Results in misinterpretation/fear.
- Drastic, unneeded reactions are common.

3. HIPAA & FISMA

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 (HHS).
- 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, during analysis, etc.

  * ePHI = patient data with one or more of 18 identifiers

18 PHI 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 protected by HIPAA

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, e.g. CA.
- HHS makes the determination upon request.
- HIPAA is a floor, not a ceiling.

Who is covered by HIPAA?

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

Am I covered?

- Not if you are not involved in patient healthcare operations directly.
- Yes if you are a CE's covered component.
- Yes if you serve a CE (as a subcontractor or vendor) and create, receive, maintain, or transmit PHI for them.
- It is extremely important to be certain of your status.

Can I claim innocence?

- No.
- There is no plausible deniability under HIPAA.
- You cannot say “I didn’t know we had PHI” after a breach.
- HIPAA has penalties for the “didn’t know” category.
- HIPAA requires you to know where your PHI is.

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*."
- A BA's BA with access to PHI is also subject to HIPAA, all the way down the chain.

* BA is a HIPAA specific term

Am I a Business Associate?

- Not if you belong to the same CE.
- Yes if you are (a) providing services to a CE completely separate from yours, and (b) create, receive, maintain, or transmit PHI for them.
- If you're a BA, the external CE must have a BAA with you.
- Both you/they are in violation if not. You are a BA and subject to HIPAA in the government's eye whether or not you have a BAA.

Business Associate Agreement

- HIPAA may require a Business Associate Agreement (BAA) with vendors that have access to 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 HHS site.)
- You also need to do due diligence to ensure that the BA can protect your PHI as per HIPAA.

* HIPAA allows authorized disclosures

What is a HIPAA Breach?

- An incident where an unauthorized disclosure of PHI has occurred.
- E.g. an attack where a hacker accesses PHI on a server, theft of an unencrypted device with PHI, a hospital worker accessing PHI without need.
- Not every security incident is a reportable breach. It's for you to determine. (You may decide that it isn't if forensics etc. can prove a high likelihood that no PHI access occurred.)

Breach Notification

- HIPAA requires a breach of PHI to be reported to the HHS & the patients affected within 60 days.
- For breaches involving > 500 individuals, local media outlets must also be notified.
- Breaches can be highly damaging.
- Not reporting a breach is a serious HIPAA violation & makes you liable to penalties.

Enforcement

- OCR has the authority to levy civil monetary penalties against a covered entity for HIPAA violations*.
- … & individuals can face criminal penalties (imprisonment up to 10 years) if implicated.
- The OCR was funded via ARRA/HITECH to institute a random audit program. They have just started an audit of 167 CEs.

* A breach is not necessarily a violation

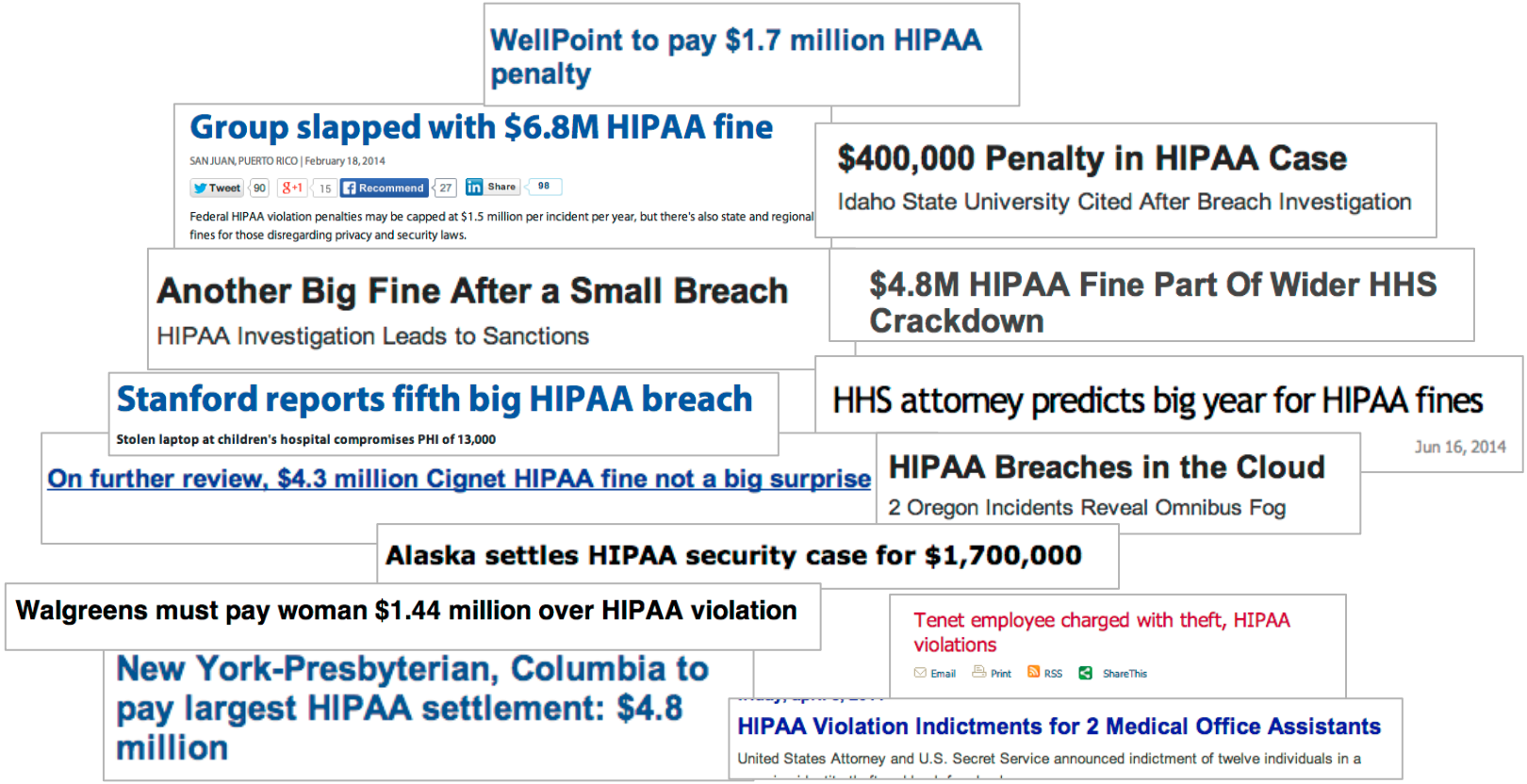
Civil Monetary Penalties

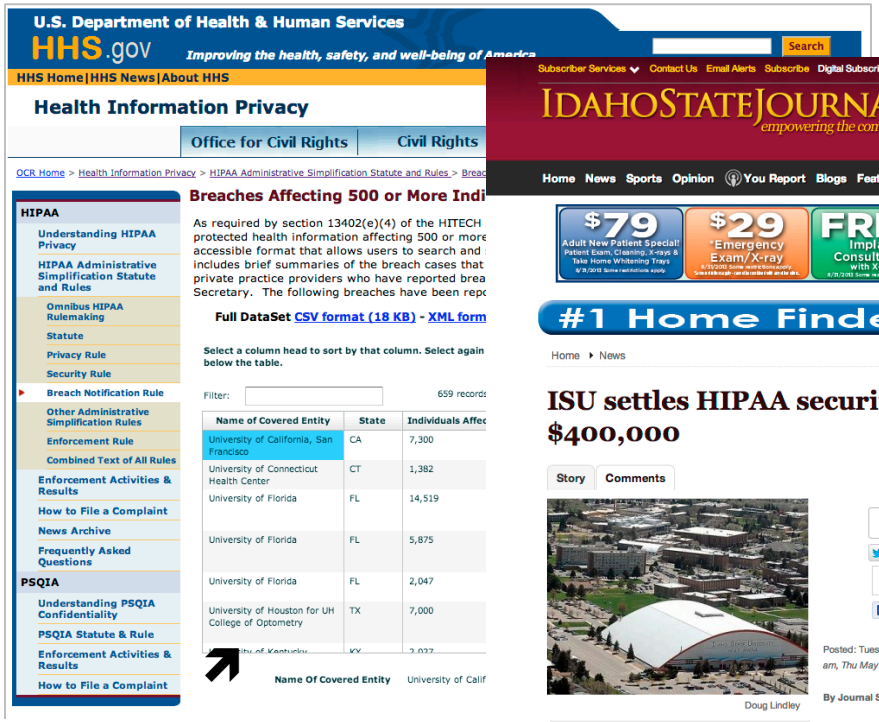
Violation Category	Each Violation		All Identical Violations Per Calendar Year	
	For violations occurring before 2/18/2009	For violations occurring on or after 2/18/2009	For violations occurring before 2/18/2009	For violations occurring on or after 2/18/2009
Did Not Know (that a violation occurred)	Up 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		

Wonders of Multiplication

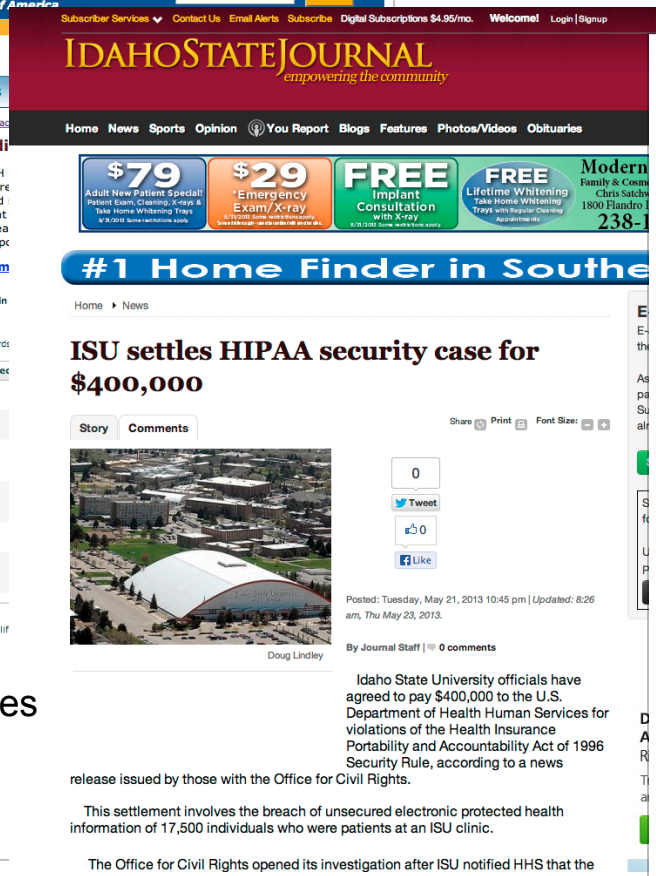
- HIPAA penalties are levied per violation.
- Breach of an individual record is one violation. To calculate your total, multiply by the number of affected individuals. The largest penalty so far has been $5.5 million.
- The actual cost may be as high as $200/patient record for notification, lawsuits, identity protection for those affected, etc..

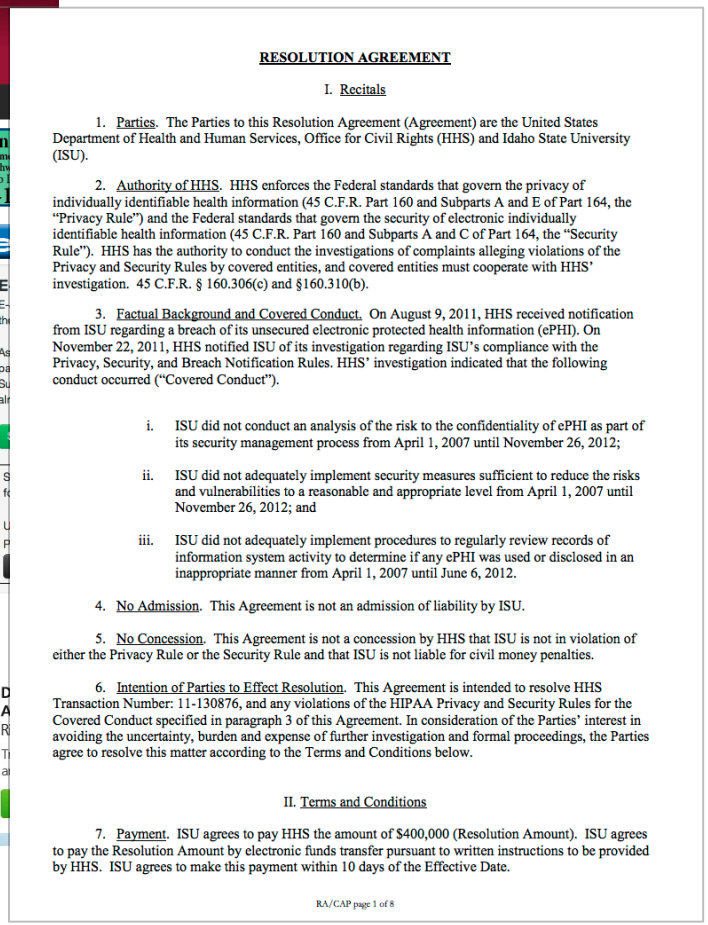
HIPAA Civil/Criminal Penalties in Action





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 worst is being on the front page

What happens after a breach?

- The OCR, affected individuals, and media are notified.
- OCR will want to see evidence that HIPAA was being complied with.
- OCR may open an investigation or let you go if they see due diligence, swift response, and existing risk mitigation measures.
- OCR may require a "Corrective Action Plan" and/or levy a penalty if it finds you in violation.

Breach Investigation

During an investigation, the OCR looks for

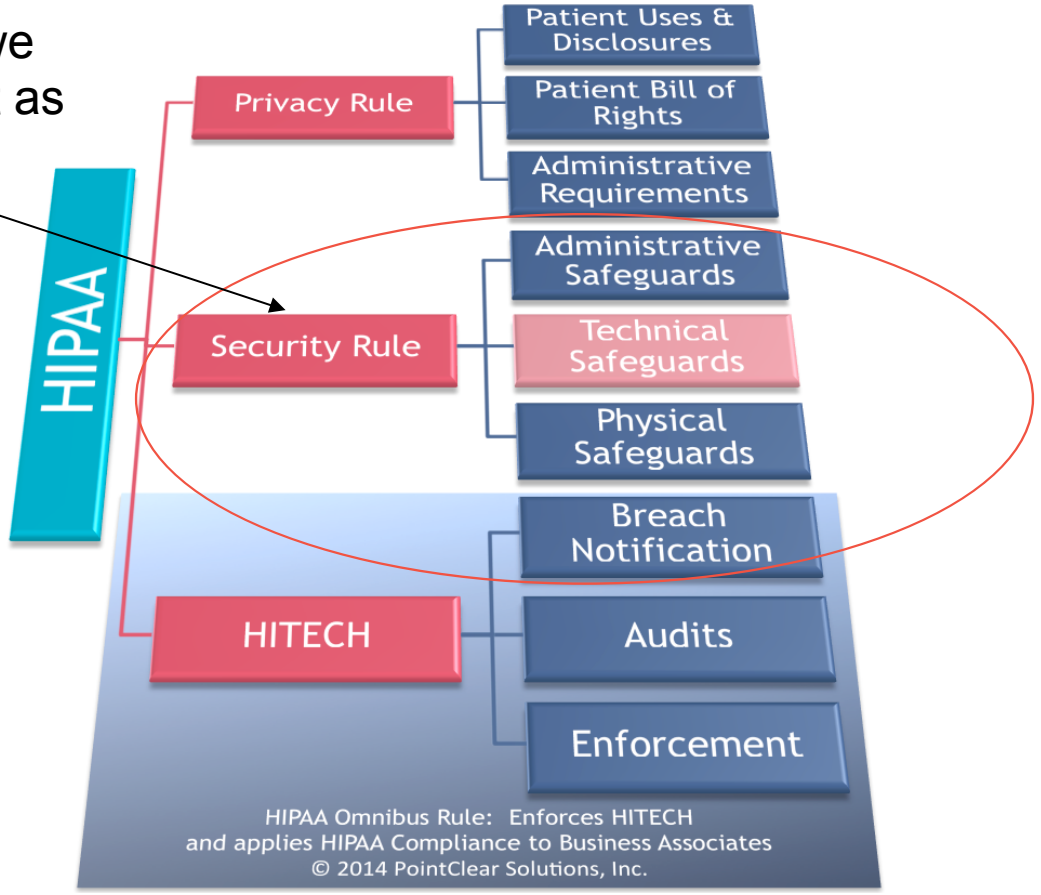
- Documented Policies & Procedures
- Implementation of Policies & Procedures
- Internal investigation reports, interview statements, etc.
- Appropriate sanctions applied
- Documented Training
- Business Associate Agreements
- Documented Risk assessment, mitigation
- Encryption & mobile device policies,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

Recent HIPAA Changes

- The HIPAA Omnibus Final Rule added HITECH & GINA provisions, new business associate & breach notification requirements, and audits/enforcement.
  - HITECH was 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 (yet) subject to HIPAA.

HIPAA after Omnibus

The part of HIPAA we need to worry about as IT providers



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

+ organizational/policies/documentation requirements

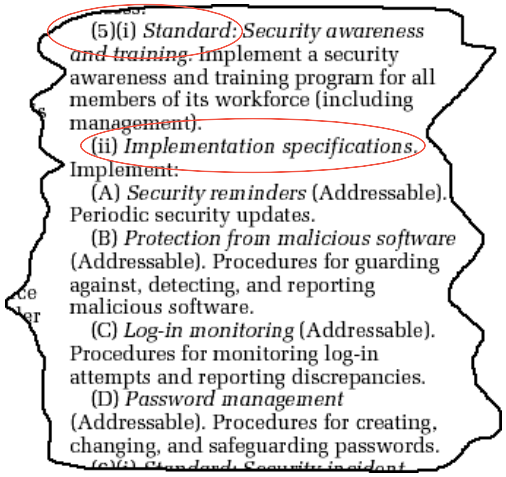
* HIPAA Security Officer

Required & Addressable

- Each Security Rule safeguard is either required or addressable.
- Required = what it says.
- Addressable = must address but ok if you document 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, i.e. how standards are to be implemented.
- It's the implementation specifications that are either required or addressable.

Does HIPAA apply to all Health Data?

- No. Only CEs and BAs are bound by HIPAA. Identifiable health data outside a healthcare context is not PHI (though Common Rule and state rules may still apply).
- Data, if properly de-identified, is no longer subject to HIPAA.
- There are a few other contexts* where health data is not subject to HIPAA.

* Student health records are subject to FERPA, not HIPAA

Who does HIPAA Cover at my organization?

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

Just Good System Security?

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

Technical controls alone do not make you secure

Do I firewall & encrypt it all?

- The Security Rule does not prescribe particular solutions or specifications, only broad guidelines, to be interpreted by individual implementers according to their environment.
- It wants reasonable & appropriate safeguards.
- … & lots of documentation. If it is not documented, it doesn't exist as far as OCR is concerned.

Local Risk Tolerance

- Since HIPAA gives such wide berth, it is often your institutional risk tolerance that in reality determines what you must do.
- Some build walled gardens; we didn't at IU.
- Instead, we worked closely with our HIPAA Privacy and Security Officers. They are intimately engaged in our risk management process & ensure that we are doing our due diligence.

HIPAA Myths

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

None are true

The Reality

- Compliance is not deterministic. Nothing signifies 100% compliance. The OCR may still find you lacking.
- No one is authorized by HHS to declare you compliant. You can only do due diligence.
- Compliance (= risk management), once started, becomes a continuous, baseline activity as long as the system with ePHI is in operation.

Here is what the HHS says:

U.S. Department of Health & Human Services

HHS.gov *Improving the health, safety, and well-being of America*

Search Search OCR All HHS

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.

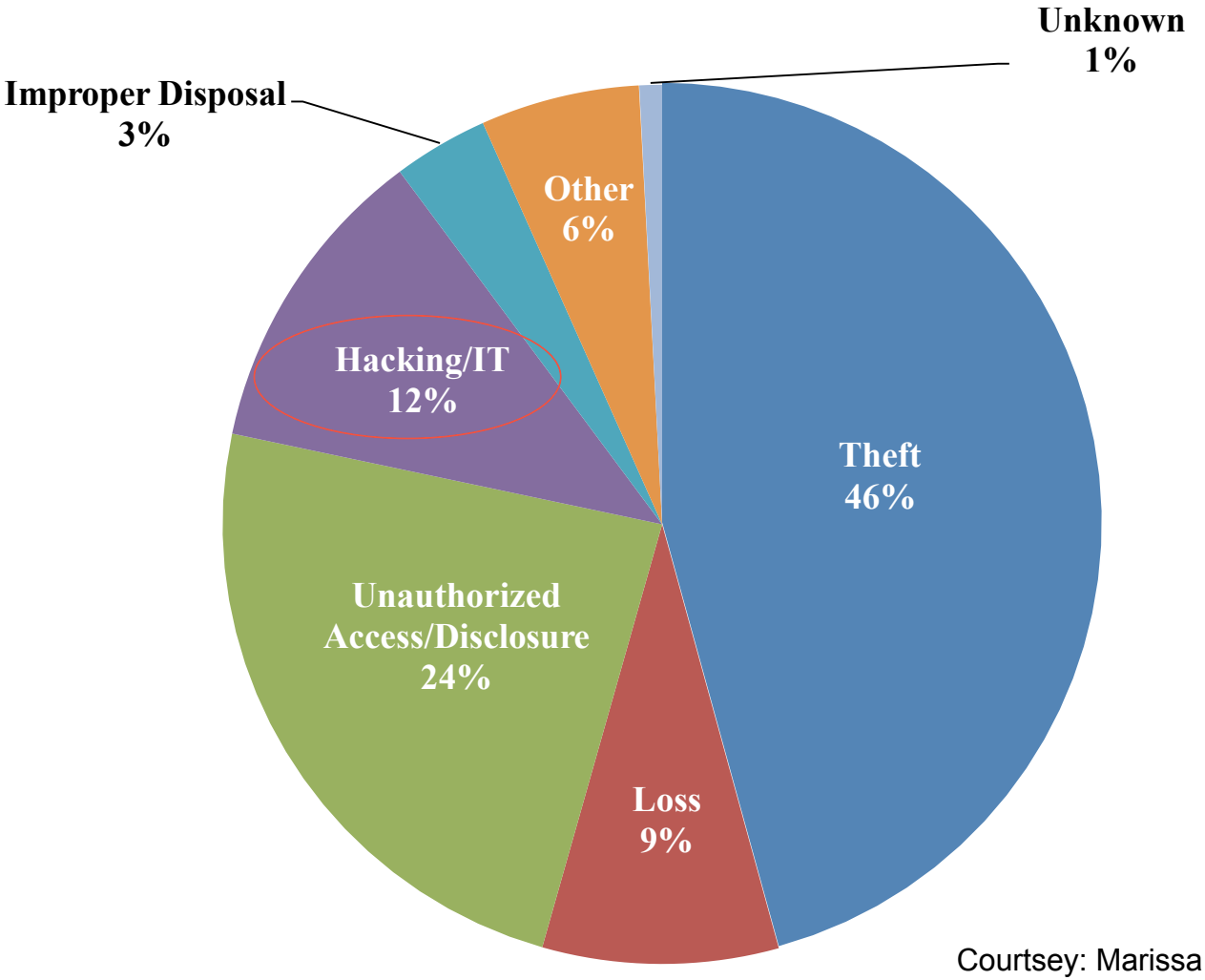
IU Disclaimer

UITS provides several systems and services that meet certain requirements established in the HIPAA Security Rule, thereby enabling their use for research involving data that contain PHI. However, using a UITS resource does not fulfill your legal responsibilities for protecting the privacy and security of data containing PHI. You may use these resources for research involving data that contain PHI only if you institute additional administrative, physical, and technical safeguards that complement those UITS already has in place.

HIPAA is Fuzzy

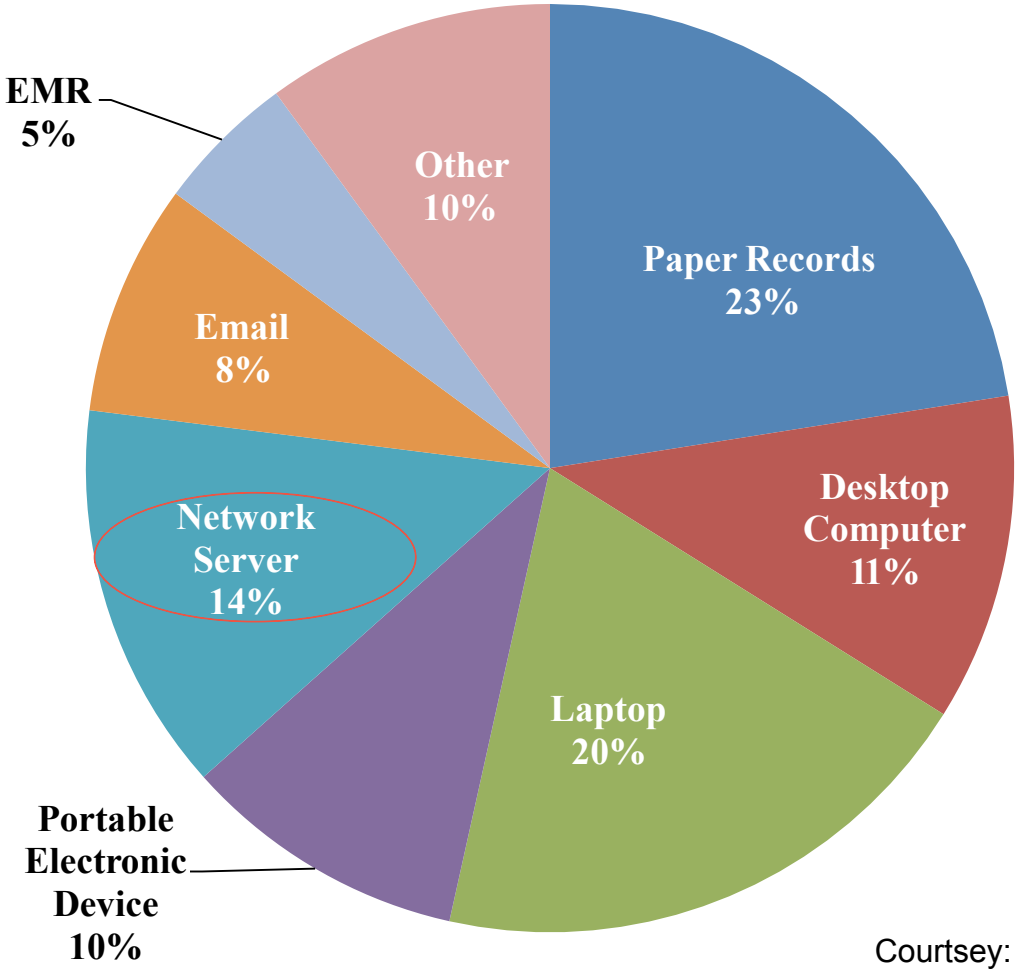
- The HIPAA Security Rule allows you a lot of latitude depending on factors such as your size, budget, etc.
- This is both a boon and bane.
- Use your local HIPAA Compliance office to clarify what HIPAA means in your environment.
- If you don’t have such a unit, check with legal.

500+ Breaches by Type of Breach as of May 31, 2016



Courtesy: Marissa Gordon-Nguyen, OCR

500+ Breaches by Location of Breach as of May 31, 2016



Courtesy: Marissa Gordon-Nguyen, OCR

Lessons from Breaches

- Most of the breaches occur due to theft/loss & improper disclosure.
- Hacking or IT incidents is only at 12%. However, even one breach is too many.
- 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

FISMA

- Federal Information Security Management Act of 2002.
- All government agencies must comply.
- They are required to follow cybersecurity guidelines from NIST.
- Requires subcontractors* to comply as well.
- The Office of the Inspector General audits agencies annually and assigns FISMA scores.

* Including laboratories and research centers

Recent Changes

- Federal Information Security Modernization Act of 2014 modifies the 2002 Act.

- Establishes Office of Management and Budget (OMB) as the oversight authority for FISMA and DHS as the agency which administers its implementation.
- Requires agencies to notify Congress of major security incidents within seven days. OMB will be responsible for developing guidance on what constitutes a major incident.
- Places more responsibility on agencies looking at budgetary planning for security management, ensuring senior officials accomplish information security tasks, and that all personnel are responsible for complying with agency information security programs.
- Changes the reporting guidance focusing on threats, vulnerabilities, incidents, the compliance status of systems at the time of major incidents, and data on incidents involving personally identifiable information (PII).
- Calls for the revision of OMB Circular A-130 to eliminate inefficient or wasteful reporting.
- Provides for the use of automated tools in agencies' information security programs, including periodic risk assessments, testing of security procedures, and detecting, reporting, and responding to security incidents.

Latest FISMA Score Card

Agency	FY 2015 (%)	FY 2014 (%)	FY 2013 (%)	FY 2012 (%)
GSA	91	99	98	99
Justice	89	99	98	94
DHS	86	98	99	99
NRC	86	96	98	99
NASA	85	95	91	92
SSA	84	96	96	98
NSF	81	87	88	90
Labor	79	82	76	82
EPA	77	84	77	77
VA	75	80	81	81
Energy	75	78	75	72
USAID	73	86	83	66
ED	73	91	89	79
OPM	69	74	83	77
Treasury	58	67	76	76
HHS	58	35	43	50
Interior	57	92	79	92
Commerce	55	N/A†	87	61
SBA	51	58	55	57
DOT	48	63	61	53
USDA	43	53	37	34
HUD	39	19	29	66
State	34	42	51	53
DOD	N/A*	N/A*	N/A*	N/A*

Does FISMA apply to me?

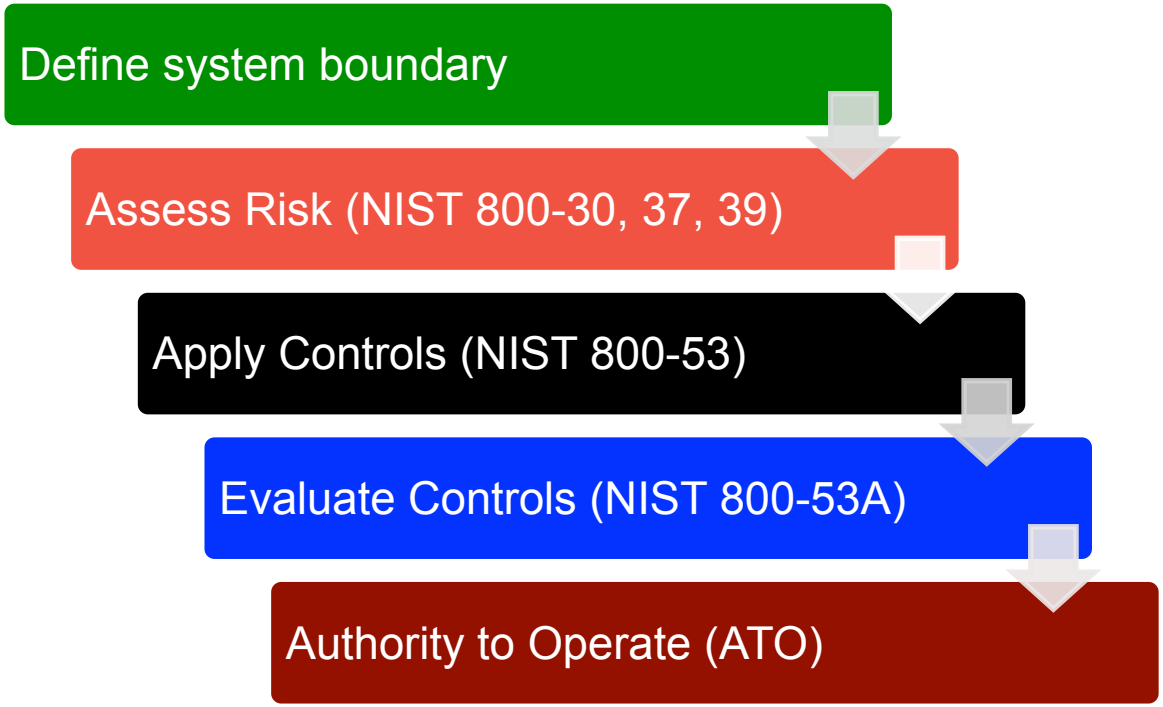
- Yes if your system collects, processes, stores, transmits, or uses government owned data on behalf of a govt. agency (as part of a grant or subcontract).
- The contract specifies which FISMA compliance level (Low, Moderate, or High) is required.
- Most grants/contracts don't require FISMA (yet) but this is changing.
- New FISMA language may be added to existing contracts (as per 2015 OMB Memo M-16-3 requiring contract reviews).

HHS' FISMA 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.

FISMA Process



Define System Boundary

- Also known as the “accreditation boundary” = where the system begins and ends.
- “System” defined loosely; can be a server, part of a network, an application, or a logical collection of disparate components.
- The boundary may include all direct and indirect users of the system that receive output.
- It is up to you to determine and define.

Assess Risk

- Follow NIST documents NIST 800-30, 37, and 39 for guidance on risk and risk assessment.
- Threats, vulnerabilities, & attack likelihood and impact are identified.
- Risk is calculated by multiplying likelihood and impact. Can also be qualitative (L/M/H).

Apply Controls

- Use NIST 800-53 control catalog to select controls that mitigate risk.
- FISMA Low, Moderate, High requirements equate to adopting the NIST 800-53 Low, Moderate, High security baselines.
- A significant undertaking, especially FISMA High.
- Many organizations will not accept FISMA High contracts as a result.

Evaluate Controls

- Follow NIST 800-53A and institute regular evaluation of NIST 800-53 controls you put in place.
- Involves testing the controls to gauge their effectiveness in mitigating risk.
- Evaluations can be done by internal or external assessors.

Authority to Operate

- The information security plan, etc. is submitted to the agency.
- If no remediation is needed, an ATO letter is issued by the agency authorizing operation of the system.
- If some remediation is needed, the agency may issue an Interim Authority To Operate (IATO). The IATO will have a defined end date. The problems must be fixed by that date to get the full ATO.

Plan of Action & Milestones

- The POA&M describes risk remediation.
- Even if you have an ATO, there still may be individual 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 must track these items and ensure that they are completed.

FISMA Evolution

- FISMA costs the government $2.3 billion annually.
- $1 billion of this goes into FISMA audits.
- “Check-the-box” type audits were found to be wasteful and not necessarily leading to improved security.
- Government has therefore increasingly focused on a “continuous monitoring” approach to cybersecurity.

Continuous Monitoring

- CM requires constant vigilance and monitoring of the security state of systems.
- See NIST SP 800-137 “Information Security Continuous Monitoring for Federal Information Systems and Organizations” for details.
- Security Information Event Management (SIEM) is key (e.g. Splunk, etc.) to CM.

Evaluations & Reporting

- FISMA mandates annual independent evaluations and reporting.
- Reports must include compliance status, security incidents, incident details, etc.
- DHS provides a website called “Cyberscope” to make reporting easier.

Research & FISMA

- Only a few research institutions are prepared to handle FISMA compliance. One noteworthy implementation is Duke Medicine. They have built an IaaS based, FISMA cloud environment.
- Still, Duke will not accept FISMA High contracts due to the burden it imposes.
- Tackling FISMA requires a strategy.

Costs

- Duke estimates that, for each contract, it takes 23-25 hours to review all documentation, make suggested contractual changes for agency negotiation, and create a FISMA management plan.
- They handle FISMA cost by having the PIs write in FISMA as a line item in the contract budget.

5. Risk Management

Why Risk?

- Cybersecurity started as technical controls.
- Experience over time showed that technology alone is not the answer.
- The discipline evolved as it borrowed from areas such as finance & defense that have had a long experience with threats.
- They focus on minimizing risk, not on controls.

Risk vs Controls

- Cyber risk = the likelihood that a threat will exploit an existing vulnerability and create an adverse impact.
- A risk focus is more inclusive of factors that plugging system security holes alone ignores.
- Controls can sound sexy, but have little or no effect in reality. For instance encryption at rest on a server located in a highly secure data center.

Types of Cyber Risks

- System risk – arising from (lack, misapplication, or failure of) technical/physical controls at the system end
- User risk – arising from the manner in which the system is used by users
- Governance risk – arising from (lack, misapplication, or failure of) administrative controls

Total Risk = Sum of all three

Cyber Risk Management

- Focuses on the right controls = optimizes $$.
- = Identify, assess, prioritize, and respond to risk on an ongoing basis.

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

- The beginning of the road in the process of managing risk. You cannot do it without knowing what individuals risks are.
- There are many ways to assess risk, all the way from pedestrian (& cheap) to highly complex (& expensive).
- Can do risk self-assessment, use internal audit/ security office, or hire a third party.

Risk Response

- One of three - Mitigate, Transfer, or Accept.
- Examples:
  - Mitigate = add CCTV monitoring
  - Transfer = use a cloud storage provider
  - Accept = no backup generator (no $$)
- Response should be commensurate with budget, risk tolerance, and complexity.

Risk Management Framework

A 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

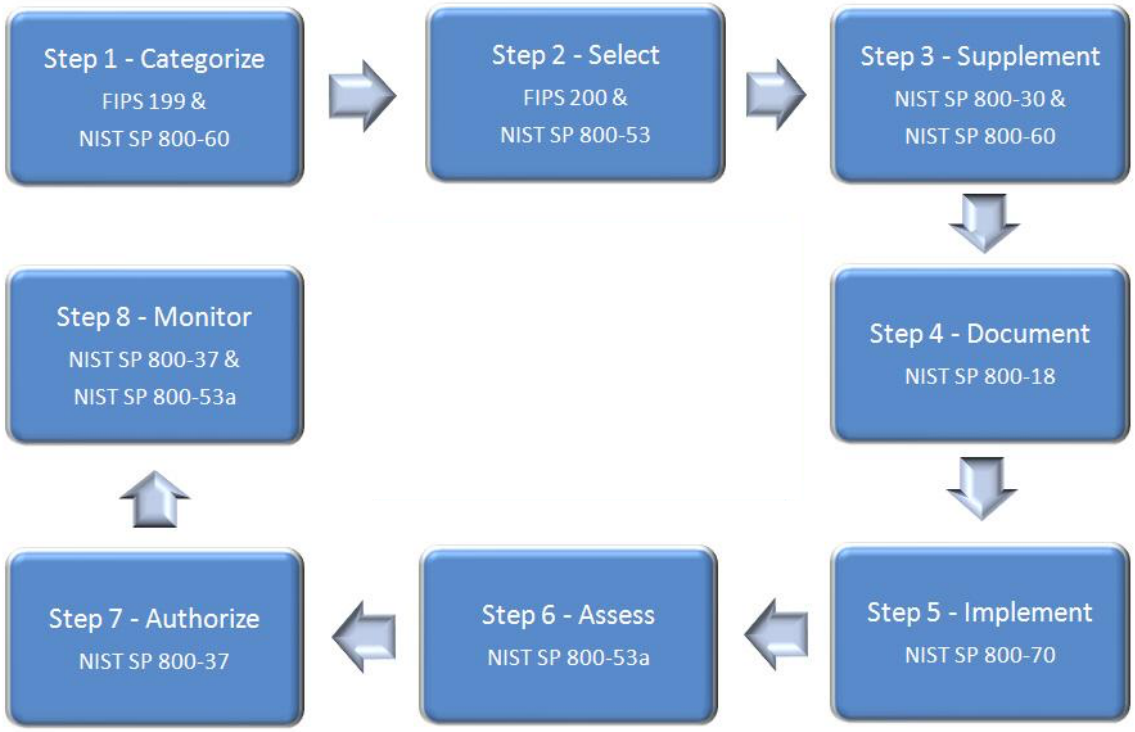
- NIST RMF = National Institute of Standards and Technology RMF
- ISO 27005 = International Organization for Standardization RMF
- OCTAVE = Operationally Critical Threat, Asset, and Vulnerability Evaluation
- HITRUST CSF = Health Information Trust Common Security Framework
- FAIR = Factor Analysis of Information Risk

5. The NIST Risk Management Framework

The NIST RMF

- According to NIST: “The (NIST) Risk Management Framework provides a structured, yet flexible approach for managing the portion of risk resulting from the incorporation of information systems into the mission and business processes of the organization.”
- It is intentionally broad-based. Details are provided by the NIST security standards and guidelines, primarily described by 800 series of NIST special publications (SP).

NIST Security Lifecycle



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.

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) a catalog of ~1000* security controls divided into families with a baseline control and zero or more control enhancements (more granular controls).

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

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 800-171

- NIST has recently issued a new special publication 800-171 (Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations) to provide relief from the massive 800-53 catalog.
- It is addressed specifically at govt. subcontractors not dealing with classified information.
- It condenses 800-53 tenfold to its most essential controls, from ~1000 to ~100.

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

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.

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 requires determining threats, vulnerabilities, and assigning likelihood and impact of exploitation.

4. 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 controls and enhancements.

5. 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.

6. 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.

8. 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.

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.

6. Building a Risk Management Framework

Choosing a RMF

- 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.
- Most rules/regulations can be mapped to these.

Indiana Univ. Case Study

- Scope: IU's large (~1000), central IT shop.
- Developed HIPAA specific, largely homegrown, ad-hoc (= much fumbling) process in 2008.
- It began showing its age by 2013 as other rules & regulations such as FISMA, a new IU IT risk management policy appeared on the horizon.
- As most rules and regulations require nearly identical set of cybersecurity controls, a unified approach to compliance was needed to avoid duplication of effort.

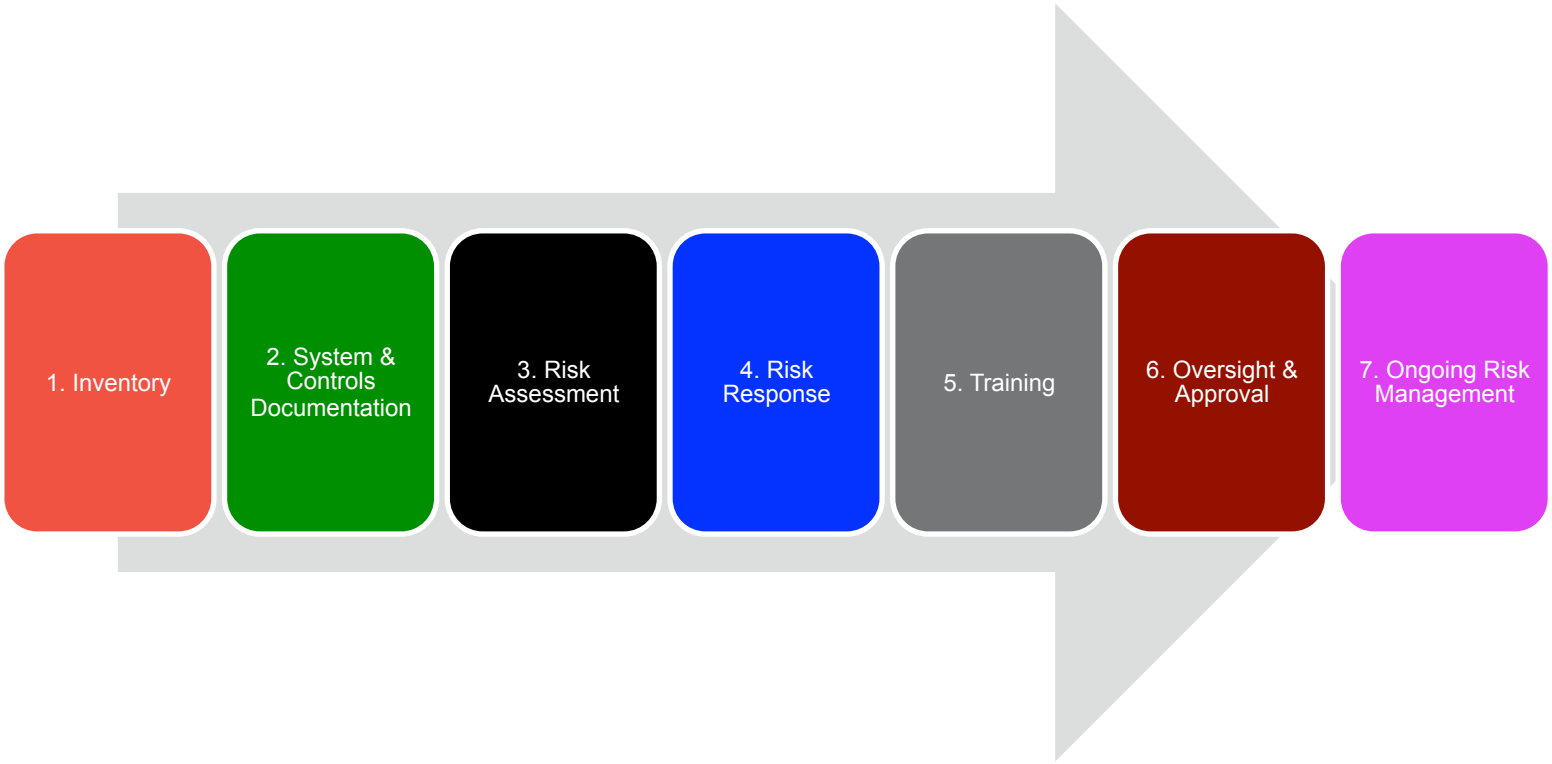
Choice of RMF

- NIST was chosen because it
  - is a federal standard, not an arbitrary, locally determined list of best practices,
  - can address both HIPAA & FISMA,
  - is flexible, and
  - provides a persistent and evolving risk management framework along with a huge catalog of security controls.

Implementation

- The essential elements existed already.
- In 2013 added missing components - risk self assessment & mitigation, inventory, training, and more detailed documentation of controls.
- Documentation fashioned after FISMA templates from HHS/NASA, etc.
- We do not use the NIST process literally. It's been adapted to meet our goals & needs. It also adds workflow security.

Process


1. Inventory
2. System & Controls Documentation
3. Risk Assessment
4. Risk Response
5. Training
6. Oversight & Approval
7. Ongoing Risk Management

1. Inventory

- System details, ePHI location, security settings, BAAs, scan info, access methods, disposal information, etc.
- Software, version, patch level, BAAs, scanning date, 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
<System>	1/3/14	?	?	?	ISO IDS	1/4/14	Patch #XXX applied ?	1/10/14

ATO = Authority to Operate

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	

2. System & Control Documentation

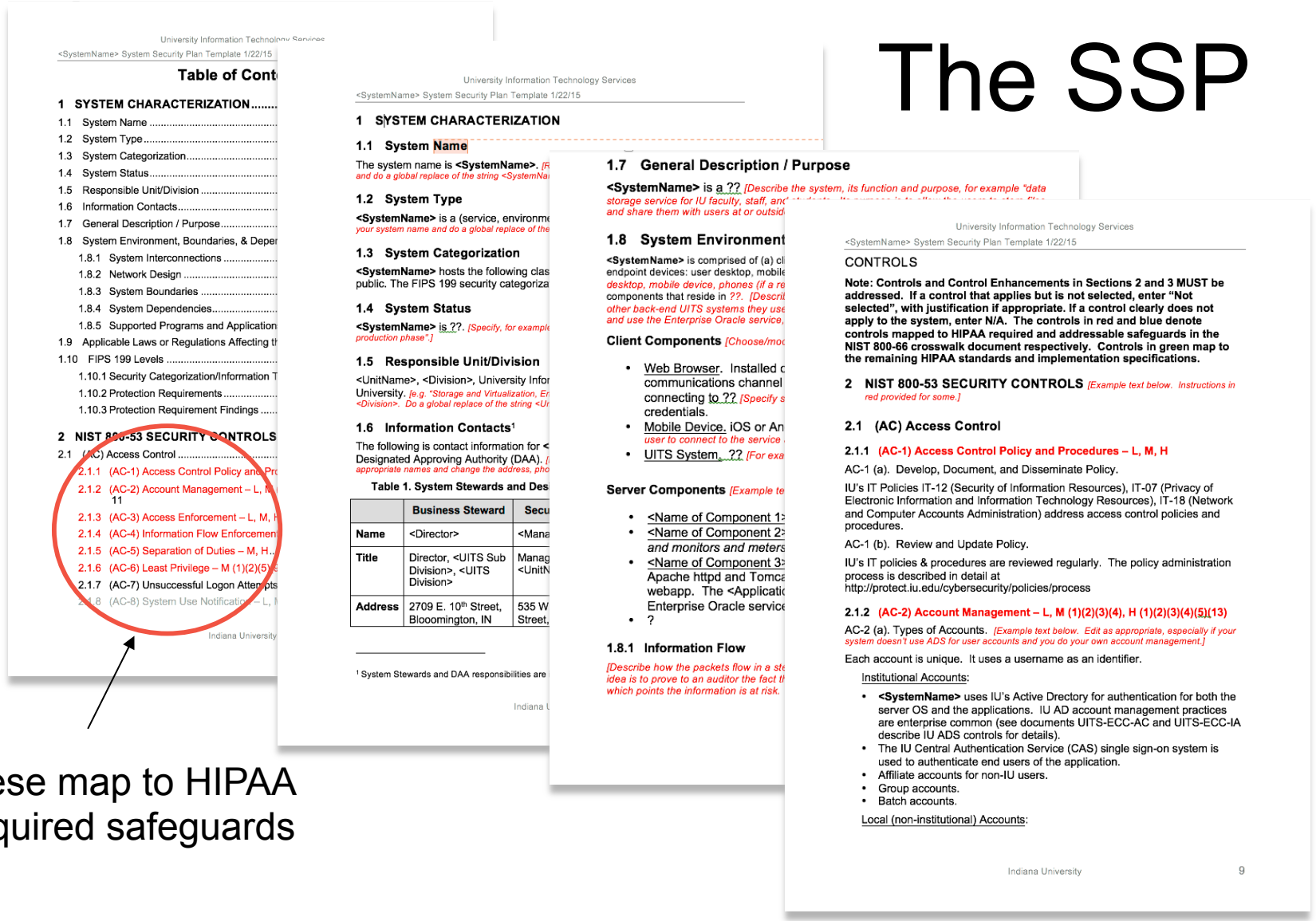
- Documented in a "System Security Plan" or SSP.
- The SSP documents the system name, categorization, contacts, purpose, components, interconnections, boundaries, dependencies, and all NIST 800-53 security & privacy controls in place*.
- We align with the NIST "low" security baseline but also document pre-existing control enhancements.

* You can begin with NIST 800-171 & add more later

NIST Controls

- Having ~1000 controls in front of you is
  - scary,
  - highly educational because you likely have never seen some of them,
  - extremely useful in guiding you in your risk assessment.
- Reading Appendix F of NIST SP 800-53 should be required reading for every IT administrator.

The SSP



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, H
2.1.4 (AC-4) Information Flow Enforcement
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, En <Division>. Do a global replace of the string <Un*

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 Des

	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 c 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 <Applicatio 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 th 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

These map to HIPAA Required safeguards

Common Controls

- Individual SSPs can include hundreds of controls.
- A large number of these will necessarily be enterprise common controls (ECC) inherited from the organization such as security governance, institutional authentication (active directory), etc..
- It is wasteful to describe them in each SSP so we document ECCs separately.
- Individual SSPs simply point to the ECC docs where needed. This saves a LOT of time.

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

The UITS-ECC-AC document

The SSP

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.

The ECC Document & How it's used in SSP

3. 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 Risk Self Assessment 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

Workflow Risk

- Where possible, the user end is also addressed for end to end security.
- Since every single workflow cannot be secured, representative research use cases/workflows are constructed and ”risk-optimized”.
- This extends risk management beyond what is used traditionally.

Research workflows

Risk optimized institutional solutions

	Use Case	Solution
1	A research team wants to store and share working data that can be accessed on user desktops as a "drive", via the web, and from an II VM	Use RFS. Install an OpenAFS client on Windows/Linux desktops and the II VM and set up RFS ACLs to authorize access for team members.
2	A research team wants to archive massive amounts of data for 6 years and share the archive	Use SDA. Pack the data in large chunks before storing. Set up SDA ACLs to authorize access for team members. Use the SDA web interface or CIFS/Samba to map a drive.
3	A researcher wants to manage data remotely via the web but wishes to avoid using a browser on the local desktop workstation for enhanced security	Log into IUanyWare and use a browser there. This not only avoids using a local browser (except to access IUanyWare), it enhances security further owing to the fact that all operations in the IUanyWare occur in reality on a Citrix server. The browser a user sees is merely a virtual representation of the browser process running on the server.
4	A research team wants to publish massive amounts of data via the web	Develop a web application that uses the HPSS API to access the SDA. The consumer may incur a time penalty (up to a minute) before the data is read from tape.
5	A research team wants to examine and manage data which is stored in Excel or CSV files and export managed data for ingest by statistical packages such as SAS, SPSS, etc.	Import data into REDCap. Log into REDCap, set up ACLs to authorize access for team members, and manage/export data. REDCap allows one to develop surveys using point and click, manage tabular data, share it with IU/Non-IU users, and export in a comma delimited format readable by SAS, SPSS, R, Excel, etc.
6	A research team wants to analyze data using a Windows stats package	Use the pre-installed statistical packages[3] in IUanyWare. Transfer data into Box Health Data Account, log into IUanyWare, import data from Box, launch the application to analyze data, and

4. Risk Response

- A "Plan of Action & Milestones" or POA&M documents the response to residual risks.
- 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

5. 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 started using our own phishing attacks to raise awareness.
- As we work individually with researchers, we train them as we help them create their own (HIPAA) documentation that describe how they are protecting their end.

6. Oversight

- The complete compliance documentation package is sent to the University HIPAA Privacy and Security Office, Information Security Office, and Internal Audit.
- They review as necessary and intervene if necessary.
- High impact systems and those that have had major incidents may get more attention.

Authority to Operate

- There is not a formal ATO process for HIPAA in place today.
- HIPAA compliance is essentially self asserted (with oversight as stated earlier).
- For FISMA, this will need to change.

7. Ongoing Risk Management

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

7. Addressing HIPAA and FISMA

From Risk Mgmt 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. Ongoing compliance is much simpler.
- Having a RMF allows one to concentrate on the system under question without needing to worry about infrastructure and dependencies.
- It gives you the confidence in your ability to survive audits.

The IU Approach

- Align the system with NIST, not with individual regulations.
- Use the NIST low security baseline.
- Map the regulation to NIST.
- Mappings either exist already or can be created.

Handling HIPAA

- Use NIST SP 800-66 (An Introductory Resource Guide for Implementing the HIPAA Security Rule). It includes a HIPAA to NIST mapping.
- The System Security Plan contains a separate HIPAA section that addresses HIPAA safeguards that do not map to NIST.
- Similar sections could be added to address other rules and regulations.

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

SSP Section Addressing HIPAA

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

1. IT unit needs to align an existing or new system
2. They come to us for help
3. We work with them 1:1 to create the compliance package
4. We mediate between them and the authorities during review
5. We help them with ongoing risk management

Handling FISMA*

- 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 – incidents, vulnerabilities discovered, security impact analysis, security control monitoring

* IU doesn't have a FISMA process in place

FISMA Workflow

- 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.

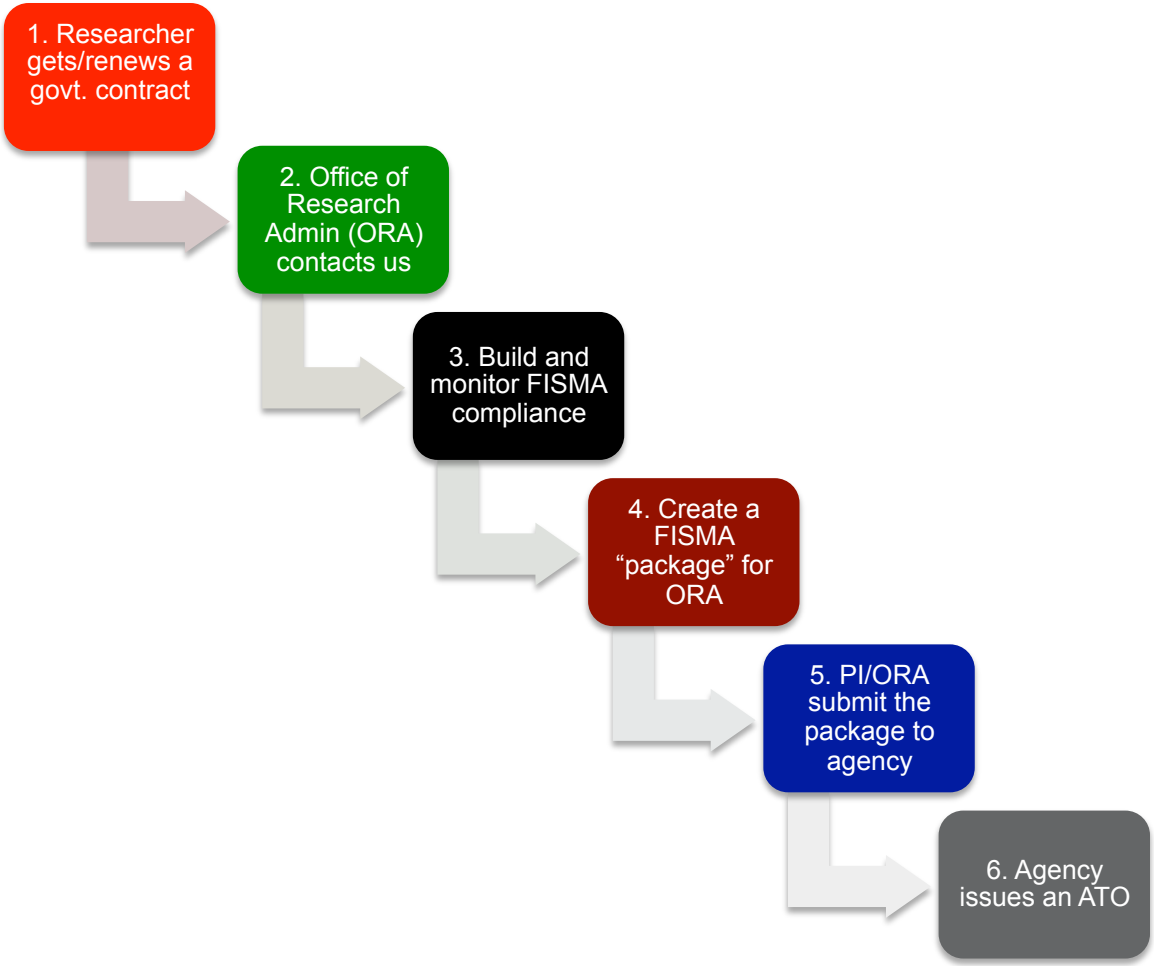
Local Administrative Process*

- 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

* Duke Medicine's process

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



NIST RMF Outcomes

- At IU, NIST has allowed us to leverage a single standard and creates a unified process.
- It gives us a structure capable of addressing current and future regulations.
- It has prepared us for FISMA.
- Units engaged in compliance like the process.
- We feel confident in our ability to handle audits.

8. The Future

1. Cloud

- Cloud 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 cloud solutions now.
- IU allows ePHI on IU’s enterprise Box. Approval required much due diligence and local controls.

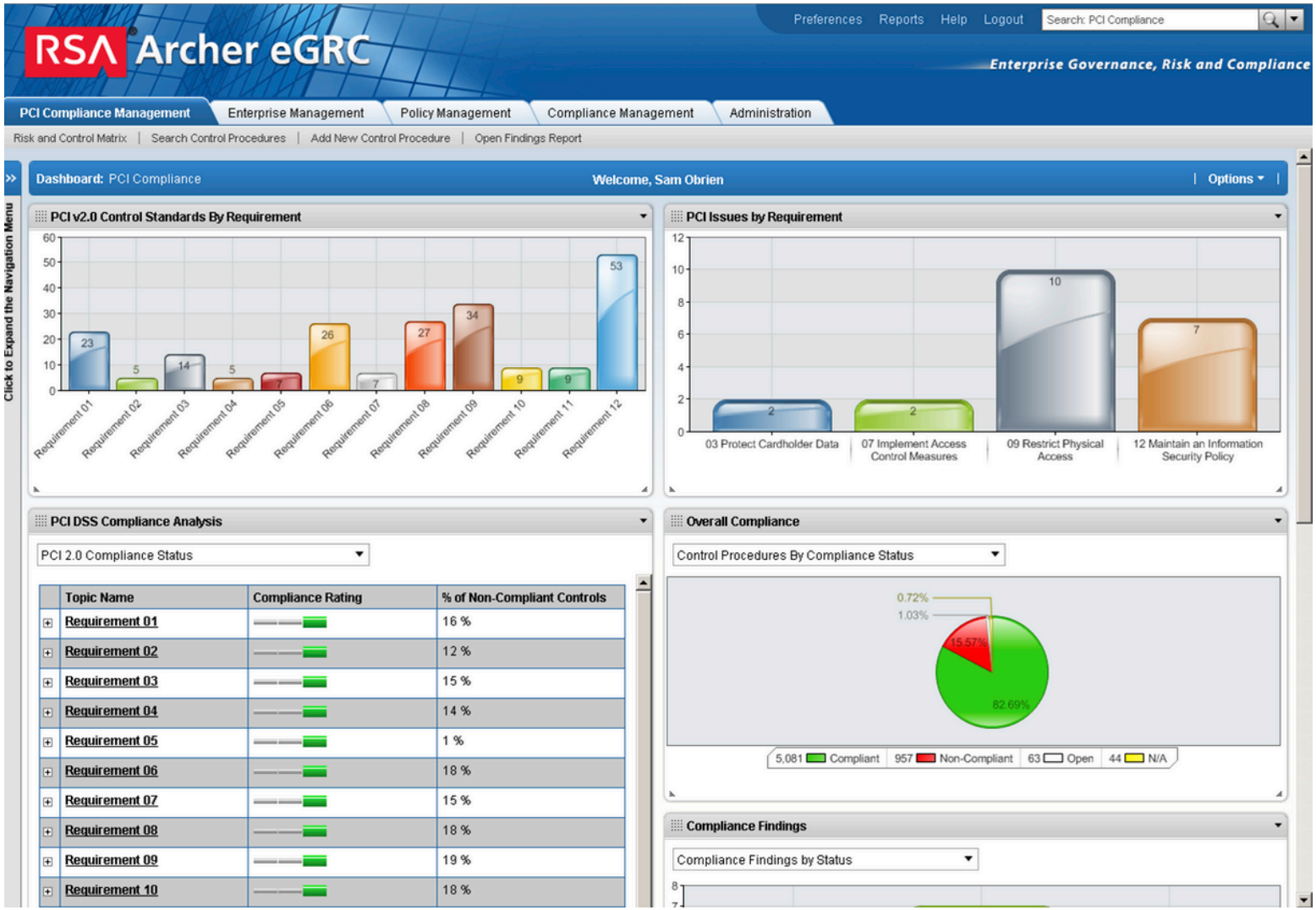
FedRAMP

- 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, but it's not cheap.

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 lacks good metrics or models that are useful in practice.
- Quantitative cybersecurity is still a 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 theory.
- Most useful are their “low hanging fruits”, controls that can prevent a majority of the common attacks.

4. Resilience

- A new movement within cybersecurity.
- Accepts the reality that attacks/breaches are a given now, like real world bacteria/viruses/disease.
- So why not use the same approach that medicine uses in the real world?
- Focuses on prevention, detection, response, and recovery assuming constant attacks/breaches.
- Prevention = risk management, Detection = realtime telemetry and analysis, Response = automated response, incident response, Recovery = DR, BCP

9. Conclusion

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 doesn'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?

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