Hello

Mike Cullen
Senior Manager, Higher Education
Baker Tilly
- CSA, CEEP, CIPP/US
- 10+ years experience
  - Conducts IT risk assessments and audits
  - Develops information privacy and security programs
  - Performs ethical hacking and digital forensic investigations
- Visited 46 of the 50 states (with the last 4 planned for next month)

Hello

Mark Phillips
Director of Internal Audit – IT
Duke University / Duke Medicine
- CIA
- 19 years of Experience
  - Director IT Audit - Duke University / Duke Medicine - since June 2006
  - Senior IT Audit Manager - Sara Lee Corporation - 1997 to 2006
- Avid guitar collector
Hello

• Where are you from:
  o AMC, Large Research Institutions, other

• What is your role:
  o Compliance, IT Security, Internal Audit, other

• Experience with FISMA:
  o Newbie, Intermediate, Expert

Objectives

• Overview of FISMA and the supporting NIST guidance and why it matters to Higher Education
• Understand the Department of Education’s (ED) efforts to ensure FISMA compliance
• Discuss practices for FISMA within a compliance program

Agenda

• FISMA
  o What
  o Who
  o Requirement categories
  o Steps for compliance
  o Authorization
  o Gap analysis
  o What’s new

• ED’s Efforts
• FISMA Compliance Practices
What is FISMA?

- Federal Information Security Management Act, became law in 2002 as part of the E-Government Act of 2002
- Requires federal agencies to strengthen information security programs and report progress back to Congress on an annual basis, in a consistent manner (using letter grades, A, B, C, D, F)
- Goal is to protect federal information (the data in both electronic and paper forms) and information systems (the computers and networks)

Why are we talking about FISMA?

- FISMA is increasingly applied to federal contractors – all of you
  - Check terms of the federal contract or subcontract.
- Are federal grantees next?
  - Manner in which FISMA is applied to awardees
    - “Thrust” into federal contracts without grace period for compliance
  - Requires decision-making about institutional information security

Why are we talking about FISMA?

- “FISMA compliance” is not an overnight accomplishment
- Requires representations and certifications
- Cyber security legislation pending – changes are coming.
- What is internal audit to do?
  - Vast misinformation about FISMA applicability
  - FISMA standard ≠ HIPAA standard
FISMA’s Goals

- Provide a comprehensive information security framework to protect federal operations and assets
- Establish minimum controls necessary to protect federal systems and assets through standards developed by the National Institute of Standards and Technology (NIST)
- Establish a means to effectively manage information security-related risks
- Provide oversight relating to federal information and information systems
- Encourage the use of commercially developed information security products created by the public sector
- Provide individual agencies the discretion to select appropriate information security products that best meet their needs

Who must comply with FISMA?

- All federal agencies, although level of compliance differs based on type of agency (e.g., national security, micro-agency) and type of information and systems involved (based on risk level)
- Government contractors and other organizations that:
  - collect or maintain information on behalf of the agency
  - that use or operate information systems on behalf of the agency

What type of contractors and other organizations must comply?

- Government Owned, Contractor Operated facilities (GOCO)
- Laboratories and Research centers
- Management and Operating Contracts
- Service Providers
- Contractor Support
How does this affect institutions?

- Agencies have been instructed to require FISMA compliance in grants and contracts
- Federal Acquisition Regulation, Part 7, Acquisition Planning, Subpart 7.1, Acquisition Plans

How does this affect institutions?

- FISMA is unambiguous regarding the extent to which security authorizations and annual IT security assessments apply. To the extent that contractor or grantee systems process, store, or house Federal Government information (for which the agency continues to be responsible for maintaining control), their security controls must be assessed against the same NIST criteria and standards as if they were a government-owned or -operated system. [From OMB M-11-33]

What are the compliance requirements categories?

- General requirements
  - Information Security Program
  - Integration of security into processes
  - Annual reporting of compliance
  - Training

- Senior Agency Officials requirements
  - Risk assessment
  - Categorization of information and systems
  - Policies and procedures creation and maintenance
  - Certifying and authorizing information systems for use
What are the compliance requirements categories?

- CIO requirements
  - Designate a Senior Agency Information Security Officer
  - Provide security assistance to senior agency officials
  - Policies and procedures creation and maintenance
  - Training
- Information Security Program requirements
  - Risk assessment
  - Policies and procedures creation and maintenance
  - Security planning
  - Security awareness training
  - Controls testing
  - Remediation of weaknesses
  - Incident response
  - Continuity of operations

Summarized from "FISMA Principles and Best Practices Beyond Compliance"; Howard, P.

How do you comply (high-level steps)?

- Determine if you need to comply (check contracts, talk to researchers, talk to agency IG)
- Perform a risk assessment
- Categorize government information and systems in use
- Perform a gap analysis between requirements and current state of your organization
- Develop plan to remediate gaps
- Test design and effectiveness of controls
- Remediate control issues
- Re-test design and effectiveness of controls
- Report on compliance
Practices

• Review federal awards for FISMA language
• Work with General Counsel or Legal to determine if FISMA applies
• Check subawards and subcontracts
• Analyze whether institution is operating “on behalf of” the government
• Review data security communications and representations to the government
• Review type of information/data generated under the award
  o Is it “federal” data? Is it sensitive? What is the magnitude of harm?
• Is it appropriate to limit FISMA’s applicability to specific departments or institutes?

How do you comply (practical tips)?

• Segregate federal data and systems used for government contracts and grants from the rest of the institution’s data and systems
  o Contractor systems used for internal management (e.g., HR, financial/billing systems) are generally not required to be part of FISMA compliance as long as they don’t store federal data or have direct system interfaces with systems that are covered by FISMA
• Specific FISMA policy, training, and controls can be targeted at only contract and grant related employees and systems and not the entire institution

Authorization

• To be considered for authorization, system manager/SSO must complete the following:

  • Risk Assessment Report
  • Security Test and Evaluation
  • Security Evaluation Report
  • Contingency Plan
  • System Security Plan
  • Configuration Management Plan
  • Plan of Action and Milestones (POA&M)
FISMA Resources

- National Institute of Standards and Technology (NIST) Special Publications (SP):
  - NIST SP 800-18
  - NIST SP 800-37
  - NIST SP 800-39
  - NIST SP 800-47
  - NIST SP 800-53
  - NIST SP 800-53A
  - NIST SP 800-60

- Federal Information Processing Standards (FIPS) 199 & 200
- Office of Management and Budget (OMB) Circular A-130 Appendix III
- OMB yearly memos on FISMA (most recent is M-11-33)

Gap Analysis tied to resources

Gap Analysis:
Step 1: Categorization
Step 2: Security Control Selection
Step 3: Implement Controls
Step 4: Assess Controls
Step 5: Authorize
Step 6: Continuous Monitoring

Step 1: Categorization
FIPS 199: Security Categorization Standards
SP 800-60: Mapping Types to Categories

Step 2: Security Control Selection
FIPS 200: Minimum Security Requirements
800-53v3 Security Controls Catalog

Step 3: Security Controls Implementation
NIST Control Families
Minimum Security Requirements: FIPS 200
Recommended Security Controls: SP 800-53 v3

Step 4: Assessment
Assessing Security Controls: SP 800-53a
Assessment Technical Guide: SP 800-115

Step 5-6: Authorization & Monitoring
Continuous Monitoring: SP 800-137
CAESAR's Framework Extension: IR 7736
What is new in FISMA?

• Move from annual testing and reporting (point-in-time audit) to continuous real-time monitoring

• Newer OMB guidance directs agencies to:
  o Focus effort and resources on developing controls to address the highest risk security concerns
  o Report metrics monthly and quarterly on these key controls that are continuously monitored

• SANS Institute 20 Critical Security Controls provide a new list of the key control activities (mapped to NIST) that organizations should implement and monitor

FISMA Applicability

• Grants/Cooperative Agreements
  o NIH Notice NOT-OD-08-032 (January 8, 2008)
    • FISMA applies to grantees (and recipients of cooperative agreements) only when they collect, store, process, transmit or use information “on behalf of” HHS or any of its component organizations
    • No definition of “on behalf of” in FISMA

• Contracts
  o No FAR contract clause (yet!)
  o Patchwork of agency-level clauses (VA, HHS, DOS, NASA)
  o Flow down to subcontractors explicitly required in some clauses

Keys to Success

• The keys to success in the FISMA project are the same factors for successful implementation of any project. The Duke Medicine FISMA initiative is fully supported, and is characterized by:
  o Senior Leadership buy-in
  o Human and financial resources allocated
  o Metrics tracking key deadlines and measuring success
  o Common Vision
    • School of Medicine and Duke Health System are working together on a common goal
  o Training and Communications
    • Significant amount of FISMA research training from the Office of Research Administration that is coordinated with the Information Security Office
FISMA Compliance Challenges

- Identifying funding instruments & clauses dealing with FISMA
- What kinds of certifications and representations have already been made?
- What do we do with the FISMA clause going forward?
- Single project approach / institution wide approach / off-site hosting
- What do we do in a security plan submitted to the government?
- Compliance costs (allowable costs to federal awards?)
- Taking “ownership” of FISMA
- Integration with HIPAA & HITECH
- Cloud computing challenges

Department of Education Efforts

Dept. of Education

Task Order 2009 Requirements – FISMA (Student Loan Companies) Dept. of Education contracts:

- C.2 SUBCONTRACTORS AND THIRD PARTIES
  - C.2.1 Flow-Down Provisions
  - “The Contractor shall ensure that subcontracts include flow-down provisions where required by clauses incorporated into this Task Order or into the Contractor’s GSA Schedule contract. Any subcontract under which the subcontractor will have access to ED data or systems must include provisions incorporating the requirements of Statement of Work Section 4.2. Security Requirements, and clauses H.11 Privacy Act, H.12 Security Clearance and User ID Requests, and H.13 Removal of access.”
6.2 SECURITY REQUIREMENTS

To ensure the confidentiality, integrity and availability of the Department’s business assets, the Contractor shall ensure that all ED security requirements are met and in accordance with all Department of Education Security and Privacy Directives, Policy and Procedures including, but not limited to, the Departmental Directive, Handbook OCCO-01, Handbook for Information Assurance Security Policy, OMB Circular A-130, A-123 and A-127, NIST Special Publications, FISMA, the Federal Information Processing Standard (FIPS) publications and the Payment Card Industry Data Security Standard (PCI DSS). The Department’s Security Policies provide a full list of applicable regulations and standards for what is a necessary tool for U.S. Department of Education Page 63 Federal Student Aid Private Collection Agency Task Order No. ED-FSA-09-O-0022 ensuring adequate controls under this Task Order. ED may also require contractor adherence to future and/or additional government security policies, reports, and memorandums necessary to safeguard and protect the Department’s information and Information Technology (IT) resources. The Contractor shall comply with and also include all appropriate security provisions in any subcontract(s) awarded pursuant to this Task Order.

FISMA Compliance Practices

Compliance in action @ Duke

Duke Org Structure

Campus (non-medical)

Duke University Health System

School of Medicine

School of Nursing
DUKE FISMA Process – A High-level Overview

System Boundaries → Risk Assessment → Application of Controls → Evaluation of Controls → Authority to Operate → POA&M

- Defining system boundaries is determining where the system begins and ends. This is a task that the Duke Medicine Information Security Office performs with input from the IT professionals that support the system. A boundary can be defined many ways, such as a part of a network, a major application, business ownership, etc.

Note: OMB Circular A-130, Appendix III, defines major application as an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. There is a lot of flexibility in defining boundaries, however, it does have to be reasonable, defensible and logical.
DUKE FISMA Process – A High-level Overview

System Boundaries and Risk Assessment

- Grants Administrators/Business Development
  - Identify and notify the Office of Research Administration (ORA) if there are FISMA terms
  - Make sure the budget includes FISMA costs
  - Identify and document key personnel for the ISO
  - 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 Support
  - Clearly describe all data flows
  - In detail, describe all systems used to support the contracts

Roles, Responsibilities and Outputs

System Boundaries and Risk Assessment

- Grants Administrators/Business Development
  - Identify and notify the Office of Research Administration (ORA) if there are FISMA terms
  - Make sure the budget includes FISMA costs
  - Identify and document key personnel for the ISO
  - 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 Support
  - Clearly describe all data flows
  - In detail, describe all systems used to support the contracts

Note: The scope of work, data flows, information systems, etc. are generally documented on the FISMA Guidelines form.

The ISO will evaluate the reasonableness of the categorization based on FIPS 199 and SP 800-16.

The Risk Assessment step is determining the “C&A” level. C&A means Certification and Accreditation. To determine the level, the agency is drawing on two documents: FIPS 199 and NIST SP 800-16. From review of the contract language, it appears that the agencies uniformly assess data confidentiality, integrity and availability, and mission criticality. There are other potential criteria, but I don’t see where they are considered.

Nearly 100% of the time, the contract specifies the overall risk level, and Duke does not have to perform this assessment. The contract will state the overall risk level as (H) High, (M) Moderate, or (L) Low.

The biggest potential problem for Duke is an agency over-classifying the data. The ISO reviews the overall risk level and will propose an argument to the agency if the risk assessment appears to be in error. This is not frequent, but it has been done multiple times.
Application of controls is implementing or utilizing specified internal controls. The number of controls that must be implemented is dependent upon the overall risk level. There are a significant (approx. 150 or more) number of controls which must be implemented and documented.

The Information Security Office determines if Duke can provide these controls or if an off-site hosting provider will be needed.

Evaluation of controls is performing security tests and evaluations. This includes tests such as verifying that security events are generated and recorded, verifying that data can be restored from backup, validating surveillance cameras are working, reviewing that output from environmental controls software is being reviewed, penetration testing, etc.

Depending on the overall risk level, evaluation of controls can either be done internally (using Duke personnel) or it must be done using independent, third-party auditors. If the overall risk level is Low, the evaluation of controls may be performed using Duke personnel.
Roles, Responsibilities and Outputs
Application & Evaluation of Controls (cont.)

- The Duke Medicine Information Security Office makes the determination regarding which option is best for the contract based on review of the results of the system boundaries and risk assessment steps.
  - Decision is documented in a "FISMA Management Plan" which documents ISO positions on terms which should be negotiated and which solution (internal hosting, external hosting, etc.) is appropriate.
- The key to making a proper decision is obtaining all documentation in a timely manner.
  - It generally takes us 23 – 25 hours to read all relevant contract documentation, document systems, make suggested contractual changes (for negotiation) and create the FISMA Management plan.

DUKE FISMA Process – A High-level Overview

- System Boundaries
- Risk Assessment
- Application of Controls
- Evaluation of Controls
- Authority to Operate
- POA&M

**Authority to Operate** is normally referred to by its acronym ATO. The ATO is a letter which is issued from the government agency to the business owner of the system and the ISO authorizing operations of the system.

- If there is some remediation that needs to be accomplished that is not too serious, the agency will issue an Interim Authority to Operate (IATO). The IATO will have a defined end date. Therefore, the problems must be fixed by a certain date.

- An ATO is the end goal

  - This can be done!**

**POA&M** means Plan of Action And Milestones. Even if Duke (or any other contractor) receives an ATO, there still may be items for which the agency requires remediation. These weaknesses were not significant enough to withhold an IATO or an ATO but they still must be corrected.

- The ISO would track these items and ensure that they are completed. Duke does not have a POA&M associated with any of our hosted contracts yet, but it may come with or shortly after the ATO that we are have just received for one of our contracts.

- Duke Medicine does have a POA&M for the Duke Medicine internal Infrastructure (IaaS).
Roles, Responsibilities and Outputs
- ATO & POAM Process

- Duke has one ATO (associated with an off-site commercial hosting solution) and long-term plans to obtain an ATO for all services provided by Duke Health Technology Solutions (DHTS) in support of federal contracts.
- This ATO and related POA&M process is being orchestrated through the Duke Medicine Information Security Office.

Duke’s Current FISMA Initiatives

- Create a FISMA-compliant Infrastructure as a Service (IaaS) model. The FISMA controls can be inherited for any systems that are served through the primary data centers.
  - SSP for the Infrastructure has been completed and POA&M items have been documented
  - Next step is prioritization and remediation of POA&M items.
- Centralizing FISMA administrative controls
  - Creation of a central FISMA training site and centralized tracking of training and certificates
  - Creation of a central process to ensure that all rosters of employees are accurate, updated with staff changes, and submitted to the agencies.
- Centralization of all contract and related IT controls data
  - All data associated with contract and IT controls is being centralized on a single SharePoint site.

Duke’s Current FISMA Initiatives (cont.)

- Implement Workstation Controls
  - Standardized “Research workstation”
  - Virtual desktop that eliminates the control issues associated with administrative rights.
- Centralize monitoring of key FISMA controls
  - Configuration Management – Tivoli Endpoint Manager project
  - Security Information Event Management (SIEM)
Resources

Contact Info
- Mark Phillips
  - mark.phillips@duke.edu
  - LinkedIn
- Mike Cullen
  - mike.cullen@bakertilly.com
  - LinkedIn

Additional Thanks To:
- Chuck Kelser, CISO Duke Medicine
- Rosemary Herhold, Sr. Security Analyst Duke University School of Medicine and School of Nursing