Strategies for a Successful FISMA Audit

Tyler Harding, CPA, CISA, CISSP, FITSP-A
IT Principal, Kearney & Company, P.C.
Tyler.Harding@Kearneyco.com
703-244-8137 (cell)

November 7, 2018
1. What Can Go Wrong with a Federal Information Security Modernization Act of 2014 (FISMA) Audit?
2. What Is a FISMA Inspector General (IG) Audit?
3. Overview of FY 2018 FISMA IG Metrics
4. Different Office of Inspector General (OIG) Approaches to FISMA
5. Five Strategies for Successful Outcomes
6. Closing Thoughts and Questions
What Can Go Wrong?

• Wasted hours in countless meetings
• Endless disagreements with auditors
• Non-issues reported by the OIG
• Information Technology (IT) resources and priorities shifted to address insignificant security risks
• Real security risks left unaddressed
• Ineffective audits hinder Security Program progress
• High distrust between OIG and agency management
• Agency horror stories
What Is a FISMA Audit?

FISMA legislation mandates:

“Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices. Each evaluation ... shall include (a) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency’s information systems;

The evaluation ... may be based in whole or in part on an audit, evaluation or report relating to programs or practices of the applicable agency.”

Problem: OIGs interpret requirement differently
## 2018 DHS IG FISMA Reporting Metrics (May 24, 2018)

### 2018 Cybersecurity Framework Function (Domains)

<table>
<thead>
<tr>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.A Identify – Risk Management</td>
</tr>
<tr>
<td>2.A Protect – Configuration Management</td>
</tr>
<tr>
<td>2.B Protect – Identity and Access Management</td>
</tr>
<tr>
<td>2.C Protect – Data Protection and Privacy <em>(New for 2018)</em></td>
</tr>
<tr>
<td>2.D Protect – Security Training</td>
</tr>
<tr>
<td>3. Detect – Information Security Continuous Monitoring</td>
</tr>
<tr>
<td>4. Respond – Incident Response</td>
</tr>
<tr>
<td>5. Recover – Contingency Planning</td>
</tr>
</tbody>
</table>
2018 OIG FISMA Metrics

General Observations

1. OIG and CIO questions align across the Cybersecurity Framework (Exception is Risk Management domain)

2. Replaced Yes/No questions with five maturity levels (1-Ad Hoc, 2-Defined, 3-Consistently Implemented, 4-Managed and Measurable, and 5-Optimized)

3. Total of 67 questions with eight “summary” questions (no maturity level response). Added five new questions on Data Protection and Privacy

4. Positive change to see emphasis on real-time risk management via automation versus emphasis on paper compliance

5. The Department of Homeland Security (DHS)/Council of Inspectors General on Integrity and Efficiency (CIGIE) requires agencies achieve Level 4 or Level 5 maturity to receive an effective Information Security Program designation
## Three Approaches to FISMA Audits

OIG approaches to annual FISMA audit/evaluation requirement:

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Audit</th>
<th>Evaluation</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performed to GAO’s <em>Government Auditing Standards</em> (GAS) – Requires sufficient and appropriate evidence to provide reasonable assurance on conclusions reached. Often selected so IT results may support the annual financial statement audit</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIGIE’s Quality Standards for Inspection and Evaluation</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Includes analysis of agency’s information security policies and procedures to FISMA legislation, Office of Management and Budget (OMB), and National Institute of Standards and Technology (NIST) guidance</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Includes responses to annual DHS IG security metrics</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Includes test of controls’ operating effectiveness for a representative subset of agency’s information systems</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Increased discussion of control weaknesses (condition, cause, criteria, effect, and recommendation)</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Increased disclosure of objective, scope, methodology, sampling methods, fraud considerations, and criteria used</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Key Audit Concepts

What is an Audit?

• Involves the comparison of agency practices to a written standard (e.g., OMB, NIST, agency policy)
• Emphasis on internal controls and business processes

Audit Implications to Agencies:

• **Golden Rule:** If it is not written down, then it does not count
• Agency policies, procedures, and practices need to define, in writing, the who, what, where, why, and how frequently a security control occurs
• Agencies must define their technical standards and baseline security requirements
• Agencies must identify how they monitor a security control for effectiveness (Level 4) and assign a performance goal (Level 5)

*Can you see the looming problems?*
Key FISMA Challenge

IT Management Direction:
1. Just get it done
2. I needed XYZ solution deployed yesterday
3. We need to be efficient

OIG / Audit Community Response:
1. Develop policies and procedures
2. Increased emphasis on evidence (e.g., paperwork)
3. More IT security audits (cycle repeats)

Final Outcomes
1. Cost-effective risk management does not occur
2. FISMA becomes a paper exercise in security

How to solve the FISMA audit problem?
5 Strategies for Success

Five Simple Strategies for Success

1. Understand the audit process
2. Practice sound project management
3. Frequent communication with OIG/auditor
4. Document only what is necessary and implement it
5. Expand the Information Security Continuous Monitoring Program to include a “Pre-FISMA Self Assessment”
5 Strategies for Success:
(1) Understand Audit Process

Planning
- Set scope and objectives
- Audit Entrance Meeting and auditors release data call (Provided by Client [PBC] list)
- Process walkthroughs and follow-up on prior-year findings

Testing
- Confirm security controls exist and are properly designed
- Detailed interviews with IT personnel
- Testing of operating control effectiveness
- Identify control deficiencies
- Periodic status meetings with the FISMA auditors

Reporting
- Develop and issue written findings (Notifications of Findings and Recommendations)
- IT responds to individual findings
- OIG issues draft report inclusive of all significant findings for management comment
- OIG and IT Department hold an Exit Meeting to discuss audit results and conclusion
- OIG revises draft report and issues final report with management comments
5 Strategies for Success:
(2) Practice Project Management

Suggested Project Management Activities for Success (Pre-Audit)
1. Assign senior management official to be responsible for pre-FISMA effort
2. Create a simple Project Plan to prepare for the FISMA audit
3. Review prior-year FISMA audit issues and data requests
4. Update system inventory and include all FISMA required information including interfaces
5. Obtain the annual IG FISMA Metrics and Evaluation Guide as early as possible
6. Update PBC documents frequently requested (e.g., IT security policies and procedures)
7. Update Plans of Action and Milestones (POA&M)
8. Update Information Security Continuous Monitoring approach
9. Conduct a “pre-audit” of commonly tested audit areas and triage weaknesses
10. Request the auditor’s FISMA PBC list four weeks in advance of audit

Project Management Goal: Get the IT auditors OUT of your IT Department fast!

Shorter IT audits translate into:
1. Fewer audit findings
2. Focused FISMA audit or evaluation
3. Fewer distractions for IT Department
4. Happy OIG, Chief Information Officer (CIO), and agency management
5 Strategies for Success:
(3) Frequent Communication

Suggested Communication Activities
1. Assign senior management official to be responsible for communications
2. Assign a single agency point of contact (POC) for all data requests
3. Contact OIG/external auditors to learn testing timeframe, testing approach, etc. three to six months before the FISMA audit begins
4. Request the auditor’s FISMA PBC list and necessary meetings four weeks in advance of FISMA audit start
5. Schedule meetings between IT Department and IT auditor well in advance (at least two weeks)
6. Develop “ground rules” for ad hoc meetings during the audit
7. Entrance Meeting – Cover key FISMA audit areas:
   a. Agency’s implementation of NIST Risk Management Framework (RMF) and agency security policy
   b. Ground rules for managing and reporting findings – Agency needs sufficient time (seven days) to verify facts and respond to any recommendations
   c. Auditor’s project timeline (When are responses due back to the OIG?)
8. Require weekly meetings to: a) review updates to PBC list with auditor; b) discuss preliminary concerns/observations; and c) confirm last day of fieldwork!

Goals of Frequent Communication
1. Fast and fair FISMA evaluation
2. Reduce miscommunication and silly findings
Targeted Documentation Activities

1. Adopt a Keep-It-Simple-Stupid (KISS) strategy:
   a. Do not over-document
   b. Identify common security and privacy controls
   c. Utilize templates (Microsoft [MS] Excel and Word) wherever possible
   d. Avoid regurgitating NIST Special Publication (SP) 800-53 controls
   e. Incorporate a monitoring element and establish a performance goal

2. Prioritize documentation efforts:
   a. Prior-year findings
   b. Updates to existing security policies to meet new OMB/DHS requirements
   c. Frequently requested PBC items (e.g., System Security Plan [SSP], POA&Ms, Contingency Plans)
   d. Current-year OMB/DHS priority areas (Continuous Monitoring Plan)

Goals of Targeted Documentation:

1. Avoid documentation for “auditor’s sake”
2. Document only what is necessary to establish “standard”
3. Avoid petty findings of “Establish policies and procedures to …”
5 Strategies for Success:
(5) Pre-FISMA Self Assessment

Suggested Pre-FISMA Self Assessment Activities
1. Identify frequently tested FISMA audit areas with operational components
   a. Access controls (e.g., employee separations, transfers)
   b. Configuration baseline, configuration change process (security-focused)
   c. Vulnerability management (security patching, vulnerability identification, and remediation)
   d. POA&Ms Updates
   e. Contingency Plan /Disaster Recovery Plan testing
2. Integrate FISMA self-assessment activities into broader Information Security Continuous Monitoring Program
3. Perform a self-assessment using the IG FISMA Evaluation Guide
4. Build a central repository of frequently requested FISMA documents

Goals of Pre-FISMA Self Assessments
1. Identify and correct weaknesses before the IT auditors do
2. Demonstrate automated and manual aspects of Information Security Continuous Monitoring
3. Improve agency risk management practices and security posture
To promote mobility and the implementation of Federal security guidance, Kearney & Company, P.C. (Kearney) developed the first-ever mobile application that aggregates and organizes the most-referenced Federal IT security standards, policies, and guidance from OMB and NIST.

The Control-IT application organizes standards by topical area (i.e., security, network, cryptography, identity management, mobile) into a user-friendly interface that includes search and download capabilities.

The Control-IT application is free to download from Apple’s App store and is compatible with iPhones and iPads.
A computer lets you make more mistakes faster than any invention in human history – with the possible exceptions of handguns and tequila.

– Mitch Ratcliffe

Questions?

Contact Information:

• Tyler Harding, Principal
  tyler.harding@kearneyco.com
  Phone: 703-244-8137