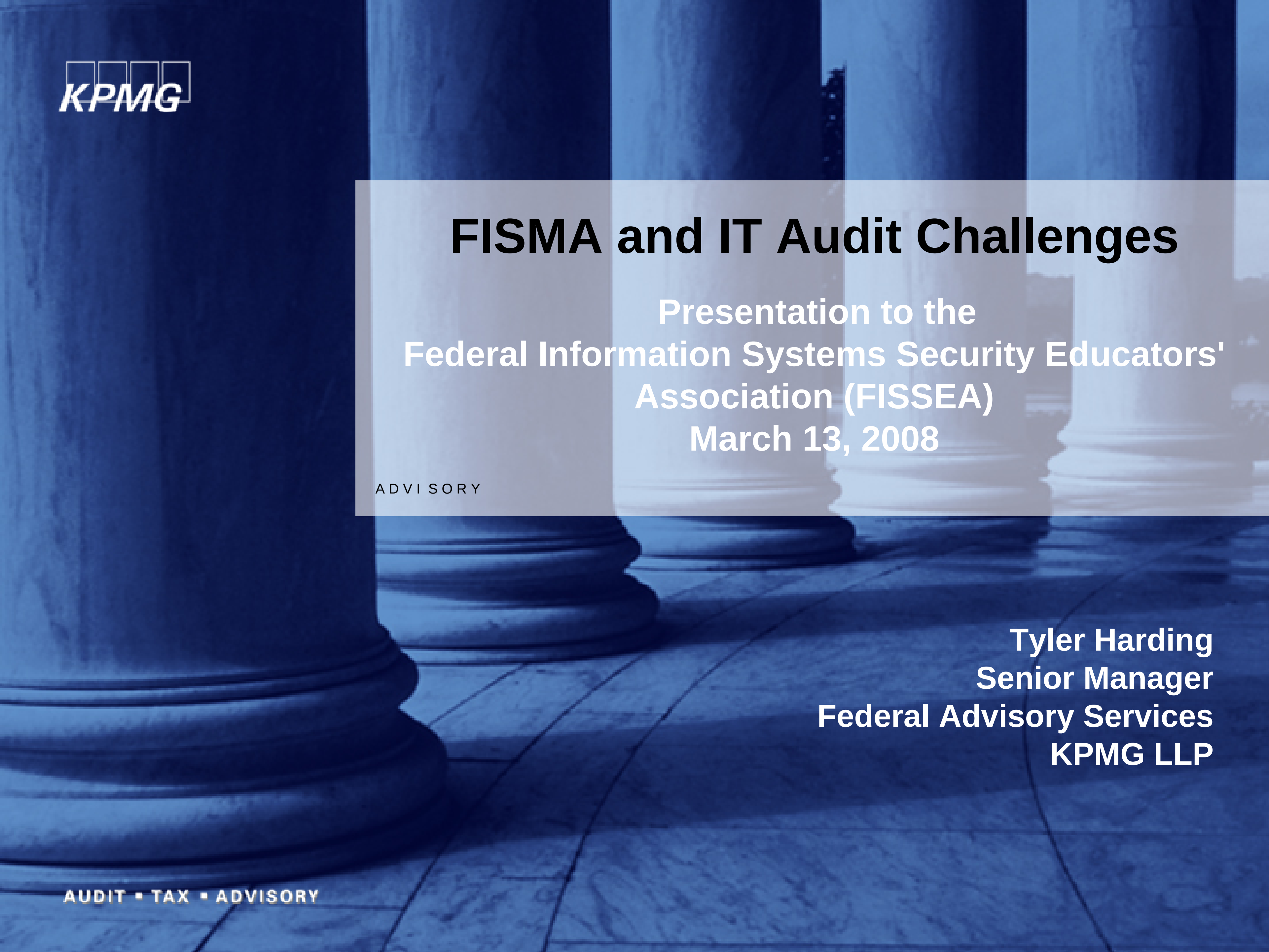


KPMG

FISMA and IT Audit Challenges

Presentation to the Federal Information Systems Security Educators' Association (FISSEA)

March 13, 2008

ADVISORY

Tyler Harding
Senior Manager
Federal Advisory Services
KPMG LLP

AUDIT ▪ TAX ▪ ADVISORY

Topics

- Current IT Environment
- Mission Impact of Security Failures
- FISMA Update
- Lessons Learned
- FISMA Next Steps
- Appendix I
  - Discussion Topic # 1 – C&A Dilemma
  - Discussion Topic # 2 – OIG FISMA Audit

Current Environment

- Continuing serious attacks, targeting key federal operations and assets.
- Attacks are organized, disciplined, aggressive, and well resourced; many are extremely sophisticated.
- Adversaries: Nation states, terrorist groups, hackers, criminals, and any individuals or groups with intentions of compromising a federal information system.
- “The threat to US Government systems is shifting from opportunistic hacking to targeted, dynamically adapting attacks.” (OMB 2007 FISMA Report)
- Increasing number of trusted employees taking dangerous and imprudent actions with respect to organizational information systems.
- Greater reliance on contractor support of IT management

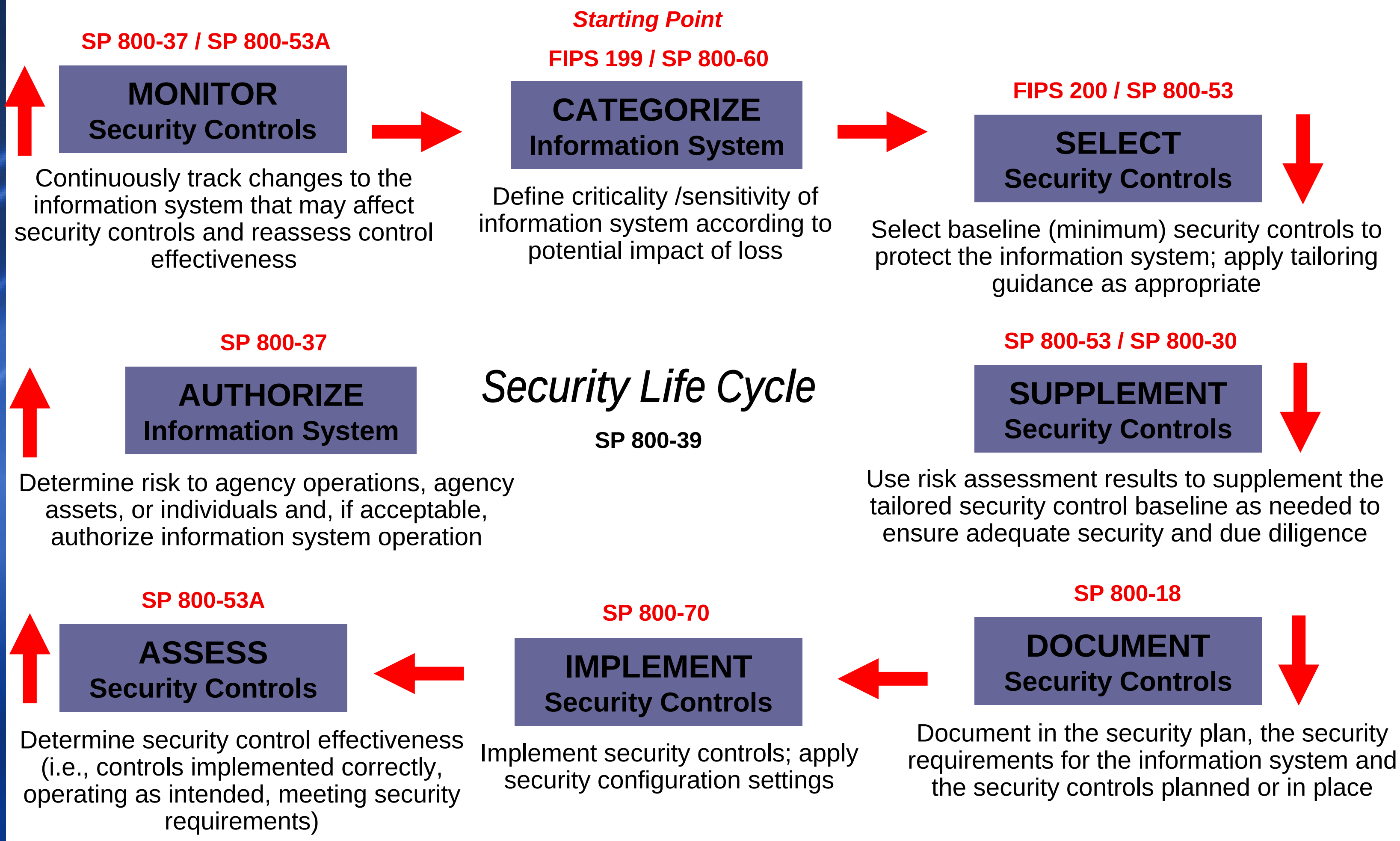
Security Impacts

- Energy (electrical, nuclear, gas and oil, dams)
- Transportation (air, road, rail, port, waterways)
- Public Health Systems/Emergency Services
- Information and Telecommunications
- Defense Industry
- Banking and Finance
- Postal and Shipping
- Agriculture/Food/Water
- Chemical

Challenging Technology Environment

- **Large, complex information technology infrastructures; many information systems to manage**
- **Cross-platform distributed computing**
- **Dynamic operational environments with changing threats, vulnerabilities, and technologies**
- **Recruiting and retaining IT personnel (management and audit) with requisite information security skills and expertise**

NIST Risk Management Framework



Starting Point

FIPS 199 / SP 800-60

CATEGORIZE
Information System

Define criticality /sensitivity of information system according to potential impact of loss

FIPS 200 / SP 800-53

SELECT
Security Controls

Select baseline (minimum) security controls to protect the information system; apply tailoring guidance as appropriate

SP 800-53 / SP 800-30

SUPPLEMENT
Security Controls

Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

SP 800-18

DOCUMENT
Security Controls

Document in the security plan, the security requirements for the information system and the security controls planned or in place

SP 800-70

IMPLEMENT
Security Controls

Implement security controls; apply security configuration settings

SP 800-53A

ASSESS
Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

SP 800-37

AUTHORIZE
Information System

Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

SP 800-37 / SP 800-53A

MONITOR
Security Controls

Continuously track changes to the information system that may affect security controls and reassess control effectiveness

Security Life Cycle

SP 800-39

FISMA Update

July 2007: ***Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*** **(GAO 07-837)**

- **Information security weaknesses at nearly all major agencies in each area of security control**
- **Weaknesses in access controls, segregation of duties and continuity of operations, configuration management and information security program**
- **GAO recommends that OMB:**
  - **Develop additional performance metrics measuring the effectiveness of FISMA activities**
  - **Require OIGs to report on the quality of additional agency security processes (ST&E, Risk Categorization, Security Training, Incident Reporting)**
  - **Require agencies to report on agency patch management**

FISMA Update (cont.)

- OMB release of baseline security configurations for Microsoft’s Windows XP and Vista operating systems
- OMB release of FY 2007 FISMA reporting guidelines
  - Increased emphasis on privacy and PII breach notification.
  - New question for OIG's to rate the adequacy of an agency's privacy program
  - Growing emphasis on Privacy

Staying Green in FY 2008

To maintain a “Green Rating” Agencies must meet the following security & privacy criteria:

1. 100% of systems Certified and Accredited;
2. Systems installed and maintained in accordance with security configurations;
3. Demonstrated 90% of applicable systems have completed a PIA and the results are publically posted.
4. Demonstrated 90% of applicable systems with PII and covered by the Privacy Act have developed, published and maintained a current SORN.
5. Established a COOP and COG.

Source: *OMB 2007 FISMA Report to Congress.*

FISMA Lessons Learned

- Too much emphasis on paperwork vs. real security controls testing
- Too much emphasis on “inspecting quality” into operations, rather than building security and control processes into the system
- The quality of ST&E and C&A packages generally continue to be weak
- C&A process does not sufficiently involve the business owner
- A solid security management program is a must
- System inventories continue to be a challenge

FISMA Lessons Learned (cont.)

- Proper identification of boundaries:
  - Are all interconnections identified and assessed?
  - Is all cross-agency and contractor support identified (including sub service providers)?
  - Are all components of an information system included?
- Globalization (offshoring/outsourcing) who has access to information and assets?
- Consideration to mission and infrastructure impacts

FISMA Next Steps

- Greater emphasis on Performance Measures related to security
  - *What gets measured gets done.*
  - Challenge: How to measure safety or risk avoidance?
- Changes to the Audit Function
  - Increased emphasis on Program Controls and Performance Measures
- Need improved Risk Management techniques
  - Need quantitative results to determine appropriate investment.
  - Need to align strategic goals of agency programs to a successful security program

FISMA Next Steps - Risk Management Shift

From: Policy-based compliance

- Policy dictates discrete, pre-defined information security requirements and associated safeguards/countermeasures
- Minimal flexibility in implementation
- Little emphasis on explicit acceptance of mission risk

To: Risk-based protection

- Enterprise missions and business functions drive security requirements and associated safeguards/countermeasures
- Highly flexible in implementation
- Focuses on acknowledgement and acceptance of mission risk

In Closing…

A computer lets you make more mistakes faster than any invention in human history - with the possible exceptions of handguns and tequila. — Mitch Radcliffe

Contact Information

Tyler Harding
Senior Manager
KPMG Federal Advisory Services
tylerharding@kpmg.com
(202) 533-8039 (office)
(703) 244-8137 (cell)

All information provided is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

Appendix I

Discussion Topics

- Instructions: Break into teams / tables of 5-8 individuals and elect a team spokesman for the following two discussion topics.
  1. C&A Dilemma
  2. OIG FISMA Audit

Developments to Watch in FY 2008

- New OMB Guidance
- Updated NIST Guidance

Discussion Topic # 1 – C&A Dilemma

Situation # 1 – Consider for a moment that you reside within an Agency's Information Security / Information Risk Management office. Your team is responsible for performing independent Risk Assessments and independent System Test and Evaluations (ST&E) for Agency Program Offices. Your security team is one of several that report to the Chief Information Security Officer.

An Agency Program representative comes to your Information Risk Management office with a last minute request to evaluate a new, distributed system that replaces several mainframe applications. The Program Offices indicated that the CIO and Program Office want to see a successful, on-time launch of this new Line of Business application. This new application is critically important as it replaces several legacy applications residing on the Agency's mainframe, which is scheduled to be retired in the next 3 months.

Discussion Topic # 1 – C&A Dilemma

Hence there is significant schedule pressure and management desire to get off the mainframe. The new application has completed User Integration and User Acceptance Testing and is deemed ready to “Go Live” in 2 months by the Program Office. The Information System owner has completed a FIPS 199 Sensitivity Analysis and determined the impact rating was **Moderate** for Confidentiality, Integrity and Availability. However, you realize that Information System Owner has not prepared a Risk Assessment, System Security Plan, Disaster Recovery Plan, or other artifacts necessary for the C&A effort to begin.

Discussion:

- What do you do next?
- How do you handle this sticky situation and still be “Team Player?”

Discussion Topic # 2 – FISMA Audit

Situation: As the team lead for your Agency's Information Security Risk Management office, you have observed the annual OIG FISMA audit for the past 5 years. Your conclusion is that the OIG focuses too much on "policies and procedures," [you fill in the blank] and [blank]. Overall, you think the FISMA Audit could be more valuable to the Agency if the OIG redirected its efforts by taking the following three steps.

Discussion: Identify three short-comings of the current FISMA audit process and suggest three steps that the Agency's OIG could take to make the audit more effective and beneficial to the Agency.

Developments to Watch in FY 2008

- **OMB Memorandums**
  - M-07-18: Ensuring New Acquisition Include Common Security Configurations, 6/1/2007 effective 2/1/2008
  - M0-08-09: New FISMA Privacy Reporting Requirements for FY 2008 – Three New Elements to Report
- **NIST – Updated FISMA Guidance**
  - SP 800-53 Rev 2 - *Recommended Security Controls for Federal Information Systems* (Dec 2007)
  - SP 800-53 A - *DRAFT Guide for Assessing the Security Controls in Federal Information Systems (Dec 2007)*
  - NIST SP 800-39: *DRAFT Managing Risk from Information Systems – An Organizational Perspective (Oct 25, 2007)*

Developments to Watch in FY 2008

NIST – Significant Updates

- SP 800-60 *Rev 1 - DRAFT Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories Volume 2: Appendices (Nov 8, 2007)*
- SP 800-115 *DRAFT Technical Guide to Information Security Testing* (Nov 13, 2007)
- SP 800 – 55 Rev 1 - *DRAFT Performance Measurement Guide for Information Security (*Sept 28, 2007)
- NIST Interagency Report (IR) 7328: *DRAFT Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment Credentialing Program for Federal Information Systems (Sept 29 2007)*