Deloitte.

Information Assurance (IA) – Organize for Success

April 2009

Agenda

- Overview of IA Policy
- Roles & Responsibilities
- Implication of FISMA
- Risk Management Framework
- Recommendation

DoD Policy for IA

- Security Integrated into Life Cycle Development
- Organize and Manage Systems in Categories
- Incorporated into Investment Portfolios
- Monitor, Report, & Evaluate as an Element of Mission Readiness
- Assign Systems a Mission Assurance Category
- Systems will be Certified & Accredited
- Detect, Isolate, & React to Intrusions, Disruption of Services, or other Incidents
- Train & Certify All Personnel
- Appoint a DAA

Organizational Responsibilities for IA

- DARPA to Coordinate all DoD IA Research and Technology Initiatives with NSA (in coordinate with DDR&E)
- Develop & implement an IA program
- Collect & Report IA Management, Financial, and Readiness Data to Meet DoD Internal or External Reporting Requirements
- Formally Establish a DAA
- Identify & Include IA Requirements in the Design, Acquisition, Installation, Operation, Upgrade or Replacement
- Ensure Awareness, Training, Education, & Professionalization
- Comply with Established Accreditation & Connection Approval Processes

Roles & Responsibilities

- Designated Certification & Accreditation
- Authorizing Official
- Chief Information Officer
- Senior Information Security Officer (CISO)
- Information System Owner
- Information Owner
- Information System Security Officer (ISSO)
- Privileged Users with IA Responsibilities
- Authorized Users

Other Responsibilities

- Lead for Program, Plan, & Budget
- Conducting Risk Management
- Formulizing Decisions and Authority for Risk Acceptance
- Making Security Decisions Based on Mission Assurance and Resiliency
- Implementing a Governance Structure
- System and Information Owners
- Business and Functional Owners
- Complying and Reporting in Accordance with FISMA

Basic Requirements of FISMA

Establish Roles & Responsibilities

- Agency Head
- CIO
- Agency Security Officer

Define Security Program

1. Risk assessments
2. C&A assessments
3. System services & acquisition
4. Security plans
5. Configuration Mgt.
6. Systems & Communications Protection
7. Personnel Security
8. Awareness Training
9. Physical & Environmental Protection
10. Media Protections
11. Contingency Planning
12. Maintenance
13. System & Information Integrity
14. Incident Response
15. Identification & Authentication
16. Access Control
17. Accountability & Audit

Perform Annual Security Reviews

- Determine sufficiency of security program
- Independent Evaluation (e.g., IG)
- Safeguard evaluation data

Provide Annual Reporting

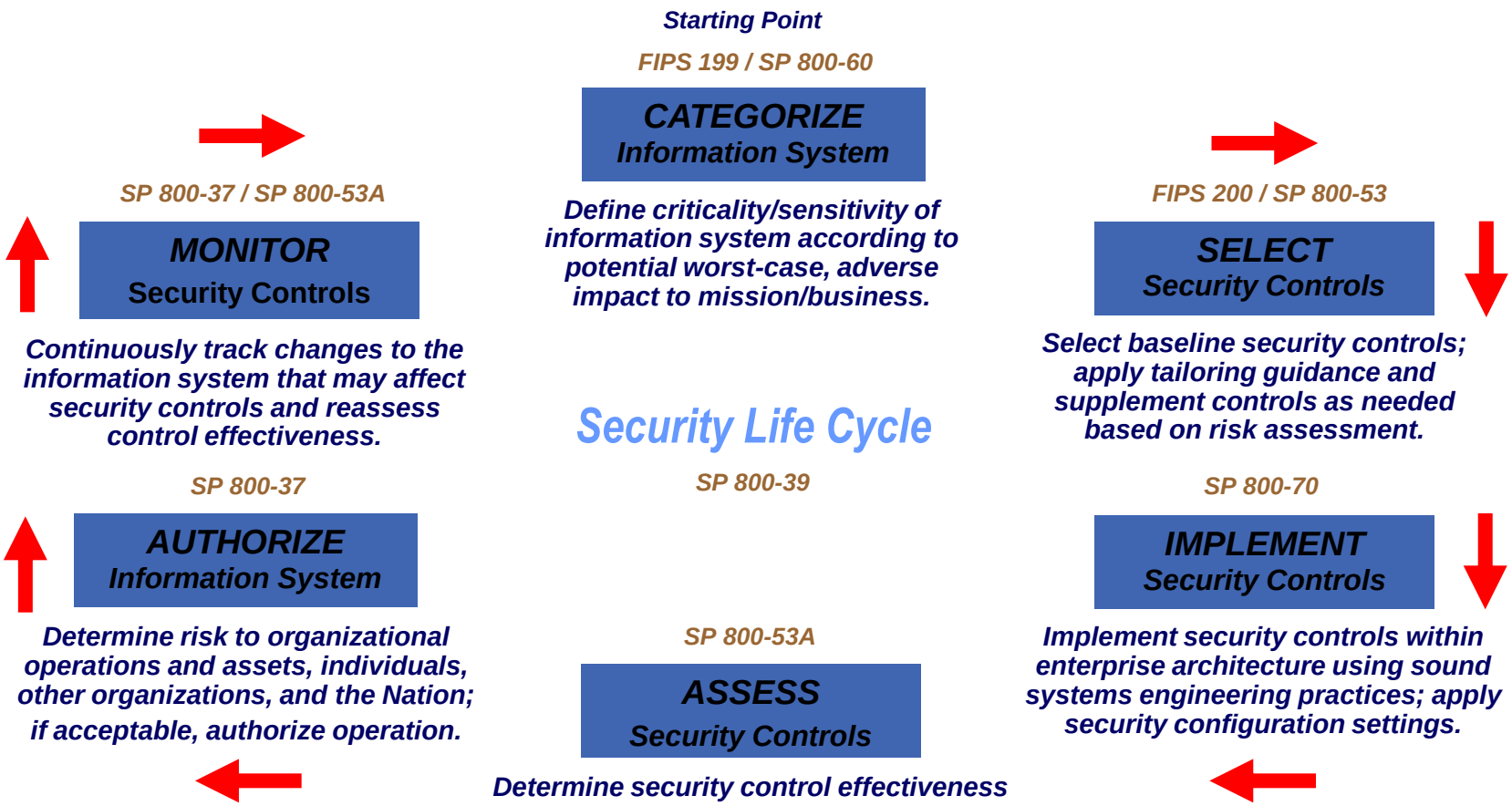
- Reports from CIO & IG
- Report material weaknesses
- Provide performance plans

Compliance

An Effective Information Security Program will:

- Conduct periodic assessments of risk from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems
- Contain policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level
- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate
- Perform security awareness training to inform personnel (including contractors) of information security risks associated with their activities and their responsibilities in complying with organizational policies
- Conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually
- Establish a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization
- Implement procedures for detecting, reporting, and responding to security incidents
- Provide plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the organization

Risk Management Framework*



*National Institute of Standards and Technology

Organize to Manage

- **Agency Executive Leadership**
  - **Commitment**
  - **Assigning Responsibility**
  - **Budget**

- **CIO**
  - **Key Executive Sponsor for IA**
  - **Program Oversight and Assessment**
  - **Advisor to Agency Executive Team on IA**

- **CISO**
  - **Designated by CIO and Key Leadership**
  - **Works with Stakeholders on Cross-Cutting IA issues**
  - **Single Point of Accountability for IA**
  - **Coordinates the Risk Management Program**
  - **Establishes and Maintains Intuitional IA Framework**
  - **Tracks and Develops Compliance**

Options for Governance Structure

Centralized

- CIO/CISO has budget control
- Manages all Security Practitioners in the orgs
- Implement & monitor throughout organization

Decentralized

- CIO/CISO are policy & oversight
- Budget control for program but not operations
- Security Practitioners throughout orgs implement & monitor

Governance Challenges

- **De-Conflicting Priorities**
- **Balancing Requirements From Multiple Bodies**
- **Determining Policy – Who, How Stringent**
- **Maintaining Currency**
- **Funding Decisions**
- **Ownership of Issues**
- **Incident Management & Response**
- **Responsibilities for FISMA & Other Reports**

Recommendation

- **Initiative an IA Organization Review**
  - **Reference Policy and Mandates**
  - **Appoint a Lead**
- **State Goals of the Initiative**
  - **Make short term**
  - **No boundaries**
- **Focus On Key Drivers**
  - **Governance**
  - **Mission Support**
  - **Integrate element of mission**
- **Identify Risk to Business**
  - Identify Gaps
- **Define Program of Record**
  - Plan of Action & Milestone (POA&M)

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Copyright © 2009 Deloitte Development LLC. All rights reserved.

Member of
Deloitte Touche Tohmatsu