Program Review for Information Security Management Assistance

PRISMA

Keith Watson, CISSP-ISSAP, CISA
IA Research Engineer, CERIAS

Overview

- Disclaimer and Purpose
- PRISMA, FISMA, and NIST, oh my!
- PRISMA versus an Assessment
- Topic Areas
- Maturity Levels
- Review Options

PRISMA, FISMA, and NIST Oh My!

- Federal Information Security Management Act of 2002 (FISMA; 44 U.S.C. § 3541, et seq.)
  - Requires Agencies, Contractors to develop, document, implement an infosec program to protect information and information systems
  - "risk-based policy for cost-effective security"
  - NIST and OMB assigned responsibilities

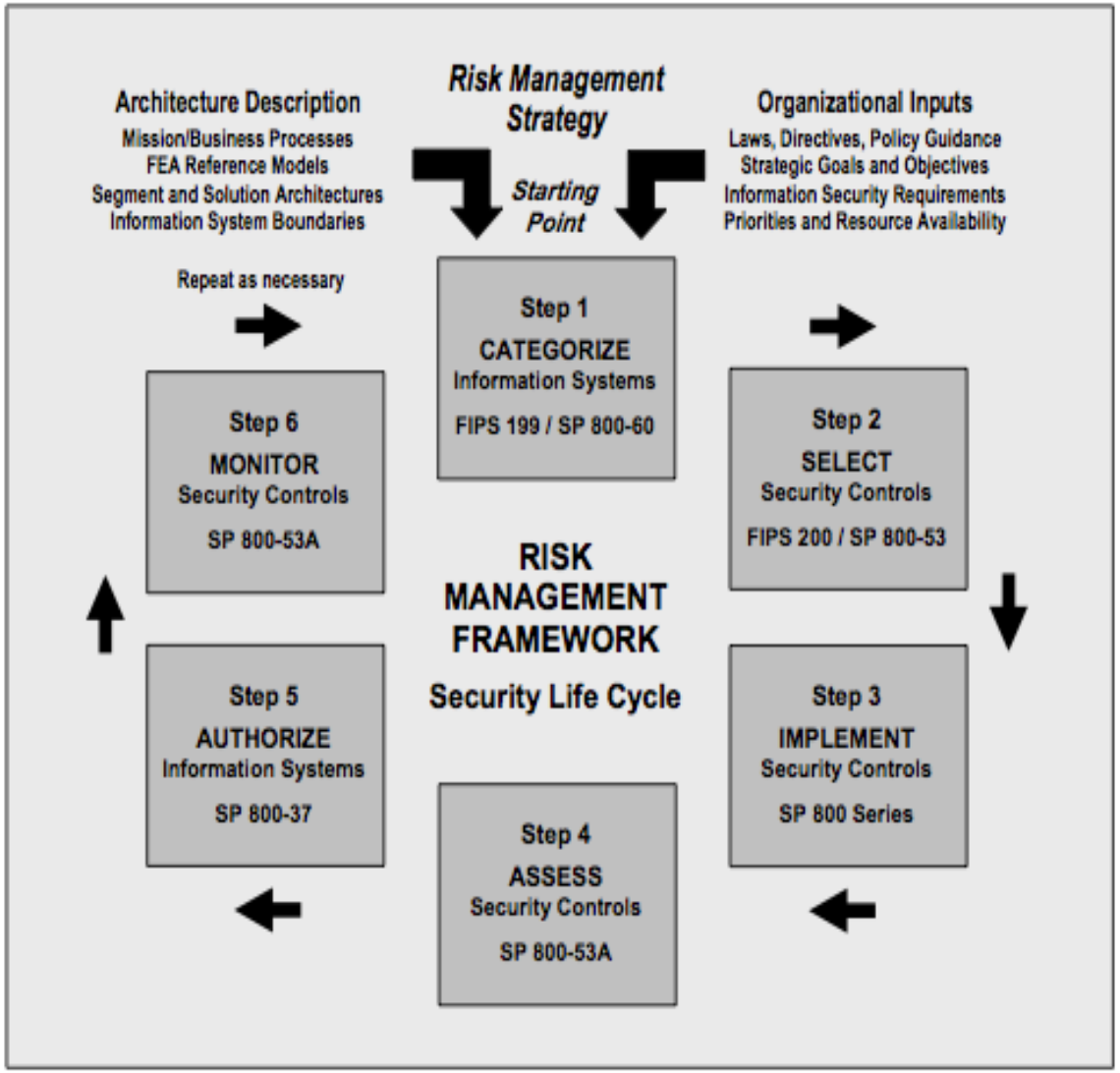
NIST

- National Institute of Science and Technology
- The CSD publishes Special Publications, Interagency Reports, Federal Information Processing Standards, etc
- FISMA requires NIST to develop standards, guidelines, methods, techniques to assist agencies in meeting requirements
- Created the FISMA Implementation Project

FISMA Implementation Overview

- Risk-based approach to implementation
  - Risk Management Framework (RMF)
- Independent review of information security maturity
  - PRISMA

Risk Management Framework



PRISMA

- Program Review for Information Security Management Assistance
  - Uses maturity levels based on SEI's Capability Maturity Model (CMM)
  - Provides a methodology for conducting a review
  - Has the same issues as a standard assessment

PRISMA versus an Assessment

- Looks like an assessment
  - NIST SP-800-30, section 3
- Uses maturity levels to evaluate
  - No High, Medium, Low levels (not qualitative)
  - No 65%, 0.65 measures (not quantitative)
- Still a snapshot in time
- Uses information provided by system owners, interviews, limited samples
- Management level review, not technical

PRISMA Approach

- Topic Areas
  - Focus of review efforts
- Maturity Levels
  - Measurement of sophistication of security controls
  - Higher level attained only if previous level attained
- Preparation
  - Usual scope definition, planning, kickoff
- Execution
  - Usual interviews, doc review, report draft, final

PRISMA Topic Areas

1. Information Security Management and Culture
2. Information Security Planning
3. Security Awareness, Training, and Education
4. Budget and Resources
5. Life Cycle Management
6. Certification and Accreditation
7. Critical Infrastructure Protection
8. Incident and Emergency Response, and
9. Security Controls

PRISMA Maturity Levels

1. Policies
2. Procedures
3. Implementation
4. Test
5. Integration

Maturity Level 1: Policies

- Formal, up-to-date, documented policies
- Continuous risk management
- Cover all facilities, operations, assets
- Proper approvals
- Define information security management structure, assign responsibilities
- Identify penalties and disciplinary actions

Maturity Level 2: Procedures

- Formal, up-to-date, documented procedures
- Clarify where, how, when, by whom, and on what the procedure is to be performed
- Define responsibilities for asset owners/users, IS management, management, infosec
- Lists appropriate contacts
- Document implementation and rigor of the control

Maturity Level 3: Implementation

- Procedures communicated
- Implementation of controls is consistent and reinforced with training
- Ad hoc approaches are discouraged
- Initial testing of controls

Maturity Level 4: Test

- Tests routinely conducted
- Ensure policies, procedures, controls ensure appropriate security level
- Effective corrective actions are performed
- Self-assessments are used
- Independent audits are used
- Security incidents/alerts used in test creation
- Evaluation requirements are documented
- Frequency and rigor of tests are risk-based

Maturity Level 5: Integration

- Implementation of controls is second nature
- Improvements made to controls, policies, etc.
- Security integrated into budgeting, planning
- Comprehensive information security part of the culture of the organization; pervasive
- Decision-making based on cost, risk, mission
- Program achieves cost-effective security
- Vulnerabilities understood and managed
- Threats continually re-evaluated; controls adapted
- Additional or more cost-effective alternatives identified
- Metrics for program and investments are met

Compliance Indicators

- Compliant
- Noncompliant
- Partially Compliant

- Overall Maturity Scores
  - All Maturity Levels Compliant: Complaint
  - Some Maturity Levels Compliant: Partially Compliant
  - All Maturity Levels Noncompliant: Non-compliant

Compliance Aggregation

Subtopic Area Policy Questions	Document 1	Document 2	Policy Maturity Score
Criterion 1 Policy Question	Noncompliant	Noncompliant	Noncompliant
Criterion 2 Policy Question	Compliant	Noncompliant	Partially Compliant
Criterion 3 Policy Question	Noncompliant	Partially Compliant	Partially Compliant
Criterion 4 Policy Question	Partially Compliant [requirement part 1 of 2]	Partially Compliant [requirement part 2 of 2]	Partially Compliant

Compliance Aggregation

STA 3.1 Criteria	Maturity Level Evaluation Questions				
	Policy	Procedures	Implementation	Test	Integration
Criterion 3.1.1	Does documented policy require employees and contractors to receive adequate training to fulfill their security responsibilities prior to access of the system?	Are procedures documented for employees and contractors to receive adequate training to fulfill their security responsibilities prior to access of the system?	Have employees and contractors received adequate training to fulfill their security responsibilities prior to access of the system?	Are employees' and contractors' understanding of their information and information system security responsibilities periodically assessed?	Is information and information system security an integral part of the duties of employees and contractors?
Criterion 3.1.2	Does documented policy require information security training and professional development for personnel recorded and monitored?	Are procedures documented on information security training and professional development for personnel?	Is information security training and professional development for personnel documented and monitored?	Is the information security knowledge of personnel periodically evaluated?	Is information security training and professional development for personnel an integral part of doing business?
Criteria 3.1.3 thru 3.1.4	⋮	⋮	⋮	⋮	⋮
Aggregate Scores >>>	Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Noncompliant

PRISMA Toolkit

- A "database" is available from NIST
  - Series of templates and a MS Access Database
  - Contains most documents needed for standard assessment methodology
  - Automates collection and report creation
  - Provides questions to be asked during document review and interviews

Review Options

- PRISMA has multiple review options
- Option 1
  - Strategic aspects of the information security program
- Option 2
  - Strategic and technical aspects of the program

Review Option 1

- Information Security Management and Culture
- Information Security Planning
- Security Awareness, Training, and Education
- Budget and Resources
- Life Cycle Management
- Certification and Accreditation
- Critical Infrastructure Protection
- Incident Response

Review Option 2

- Same list from Option 1
- Also includes Security Controls
  - Physical and Environmental Program
  - Hardware and Software Maintenance
  - System and Information Integrity
  - Media Protection
  - Identification and Authentication
  - Logical Access Control
  - Accountability (including Audit Trails)
  - System and Communications Protection

Summary

- PRISMA is for FISMA but useful assessment framework
- Is aligned with most risk assessment methodologies
- The toolkit may be useful as a source for standard assessments with customization

References

- NIST Interagency Report 7358
- http://csrc.nist.gov/groups/SMA/prisma/