NIST
National Institute of
Standards and Technology

Government Initiatives / Deliverables Related to Software Assurance and Supply Chain Risk Management

Michael Kass
Computer Scientist
Software and Systems Division
Information Technology Laboratory
National Institute of Standards and Technology
michael.kass@nist.gov

FISMA 2010 and Beyond

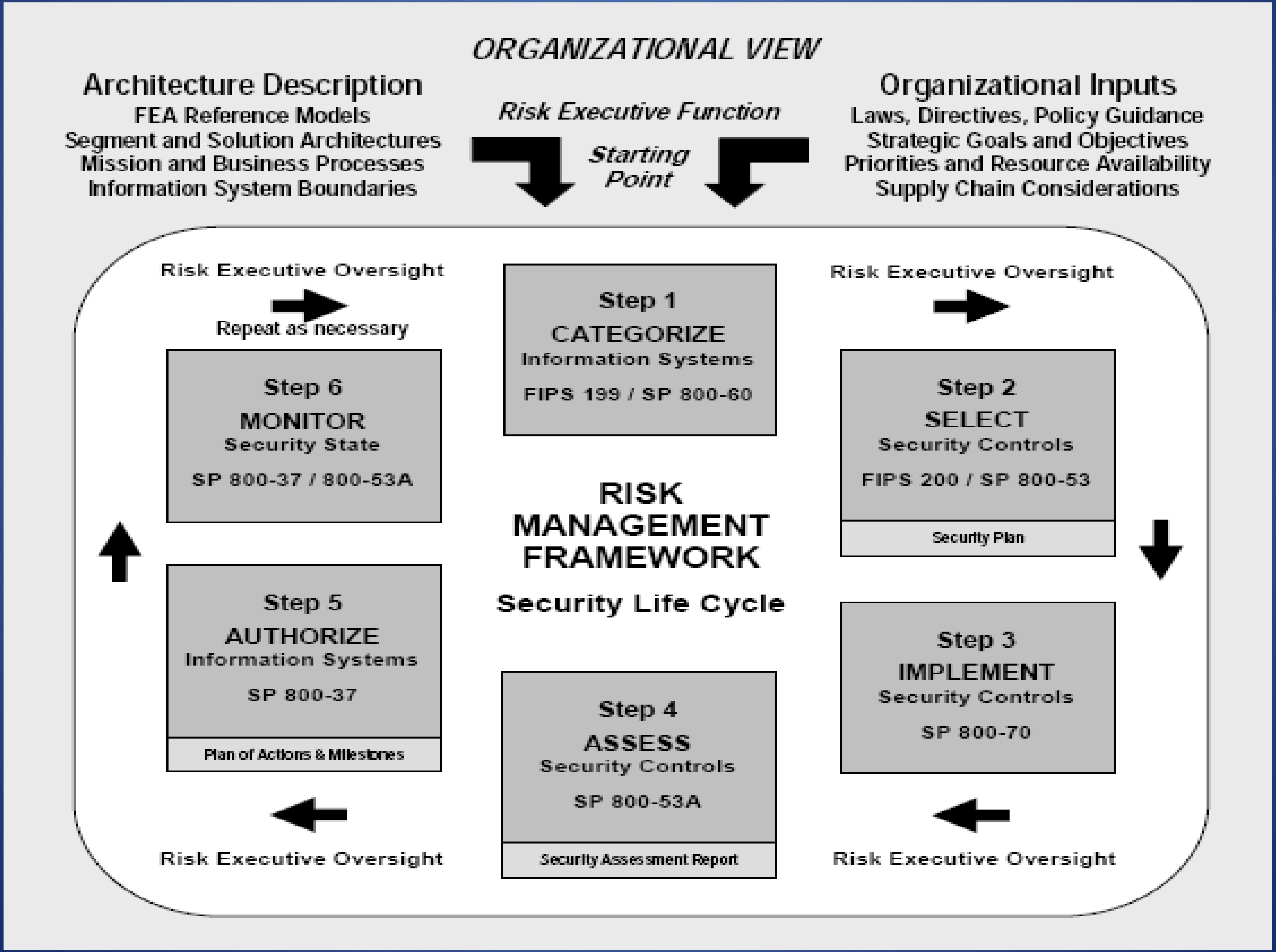
Strategic and Tactical Risk Management and the Role of Software Assurance

Dr. Ron Ross, NIST

- Over 35 pieces of legislation have been introduced in Congress to address Cybersecurity.
- Ron Ross is the NIST project manager responsible for the implementation of the Federal Information Security Act (FISMA) which has set the tone and direction of Federal Cybersecurity since 2002.
- Ron Ross is at the focal point of much of the activity to promote the development of key security standards and guidelines to support the implementation of and compliance with FISMA.

National Institute of Standards and Technology

Managing Risk from Information Systems: an Organizational Perspective



ORGANIZATIONAL VIEW

Architecture Description

FEA Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

Risk Executive Function

Starting Point

Organizational Inputs

Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations

Step 1
CATEGORIZE
Information Systems
FIPS 199 / SP 800-60

Step 2
SELECT
Security Controls
FIPS 200 / SP 800-53
Security Plan

Step 3
IMPLEMENT
Security Controls
SP 800-70

Step 4
ASSESS
Security Controls
SP 800-53A
Security Assessment Report

Step 5
AUTHORIZE
Information Systems
SP 800-37
Plan of Actions & Milestones

Step 6
MONITOR
Security State
SP 800-37 / 800-53A

RISK MANAGEMENT FRAMEWORK

Security Life Cycle

Risk Executive Oversight

Repeat as necessary

Risk Executive Oversight

Risk Executive Oversight

Risk Executive Oversight

FISMA 2010 and Beyond

- The federal government is undergoing a transformation with regard to information security and risk management.
- The DOD, Intelligence Community, and NIST are building a unified information security framework consolidating current standards and guidance.
- Software assurance is a critical component to achieving a robust enterprise-wide information security program.
- Security requirements traceability from legislation and policy to information systems and component products is important.
- Many security control families in NIST Special Publication 800-53 support software assurance.
- Advanced persistent threats require new strategies for protecting core missions and business processes.

Panel: Software Assurance Automation

Stephen Quinn, NIST   Sean Barnum, MITRE

- Discussion follows background presentations on status of and possible contribution to a software assurance automation protocol:
  - CWE – Common Weakness Enumeration
  - CAPEC – Common Attack Pattern Enumeration and Classification
  - MAEC – Malware Enumeration and Classification
  - Structured Assurance Case
  - OMG SAEM - Software Assurance Evidence Metamodel
  - OMG ARM – Software Assurance Argumentation Metamodel
  - ISO 15026 - Systems and Software Assurance Pt 2: Assurance Case
  - SAFES - Software Assurance Findings Expression Schema
  - SCAP – Secure Content Automation Protocol
- Stephen provides a NIST/Standards view of SwAAP

Emerging Software Assurance and Supply Chain Risk Management Efforts

Rama Moorthy, Hatha Systems

- A status report on the NIST-led efforts in Supply Chain Risk Management and System Assurance.
- NIST, in coordination with DoD, DHS, and Department of State will be issuing for public review draft NISTIR 7622, *Supply Chain Risk Management Practices for Federal Information Systems.*
- Based on the foundation Supply Chain Risk Management guidance work by the DoD (as part of the Working Group 2 interagency efforts)
- Refined to address the Federal market requirements
- Targeted at stakeholders critical to the all Federal efforts and thus engaging the broader Federal sector as well as industry Sectors

Emerging Software Assurance and Supply Chain Risk Management Efforts

Rama Moorthy, Hatha Systems

- NISTIR 7622 discusses the following topics:
  - Determining procurements that are vulnerable to supply chain risk;
  - Understanding procurement strategies and working with the procurement office to help mitigate supply chain risk;
  - Mitigating residual supply chain risk by requiring either the contractor or the organization to implement additional applicable practices contained in the planned document and augmenting the baseline of security controls (NIST SP 800- 53)
  - Describing the roles and responsibilities within the organization as it relates to supply chain risk management.

System Focused Product Assurance

Arnold Johnson, NIST

- Supplier Claims in the context of a information system framework -- e.g., Risk Management Framework, SP 800-53 Management, Operational, and Technical Security Control Catalog
- Build a product assurance case throughout the SDLC that is transferable, adaptable, repeatable, and extensible
- Product assurance primary elements include functional testing (product features), quality (practices/processes/methodology), and evidence (grounds for confidence) from development, implementation, assessment, and operational sources.
- Based on readily available assurance evidence to include 1st party (supplier - developmental testing), 3rd party (independent/laboratory testing), and 2nd party (end-user/customer integrated & operational system environment assessment).
- Use of common S-CAP based protocols & automated tools