System Focus Product Assurance

Security Perspective

Software Assurance Forum

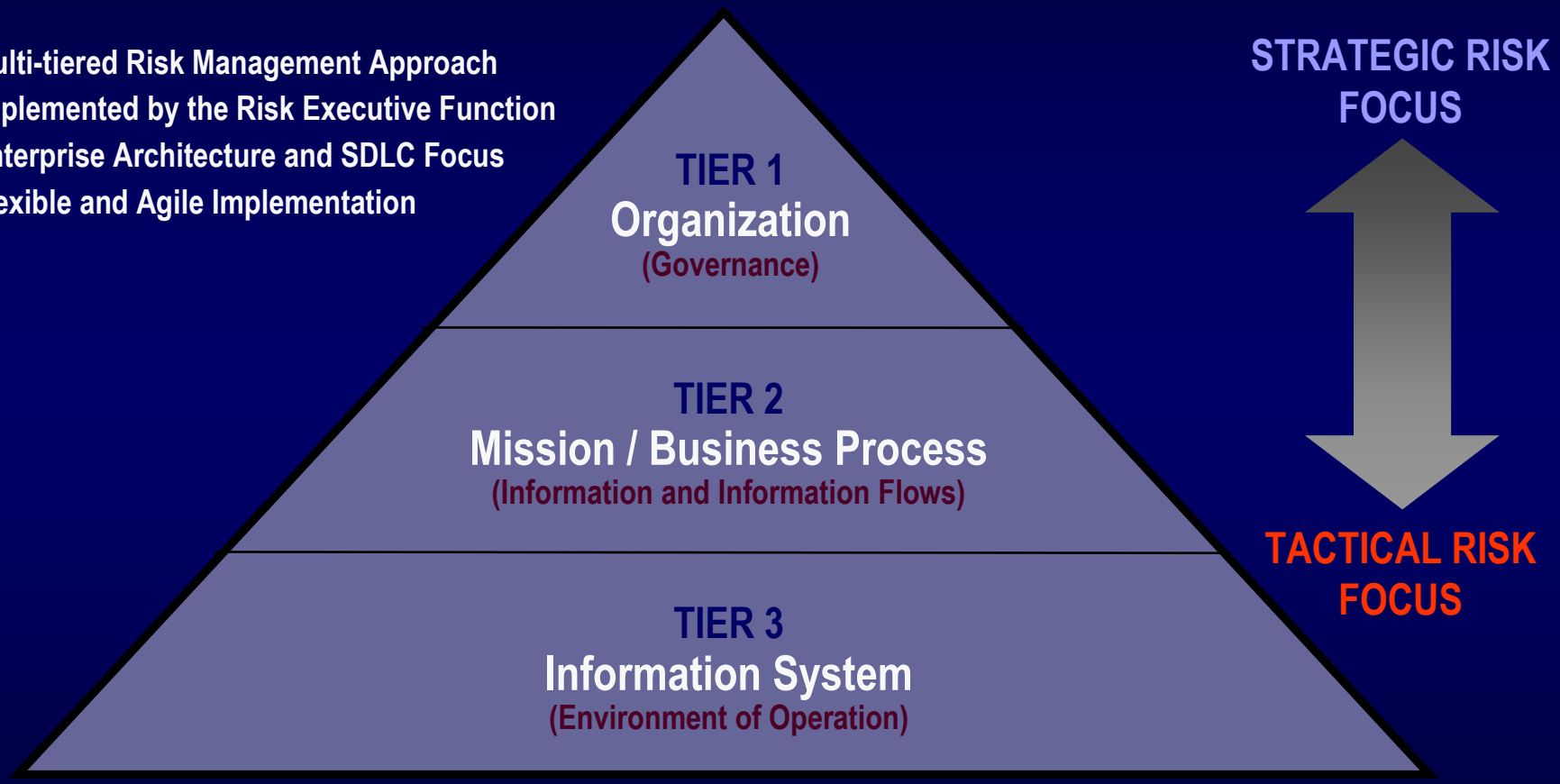
June 23, 2010

L. Arnold Johnson

Computer Security Division
Information Technology Laboratory

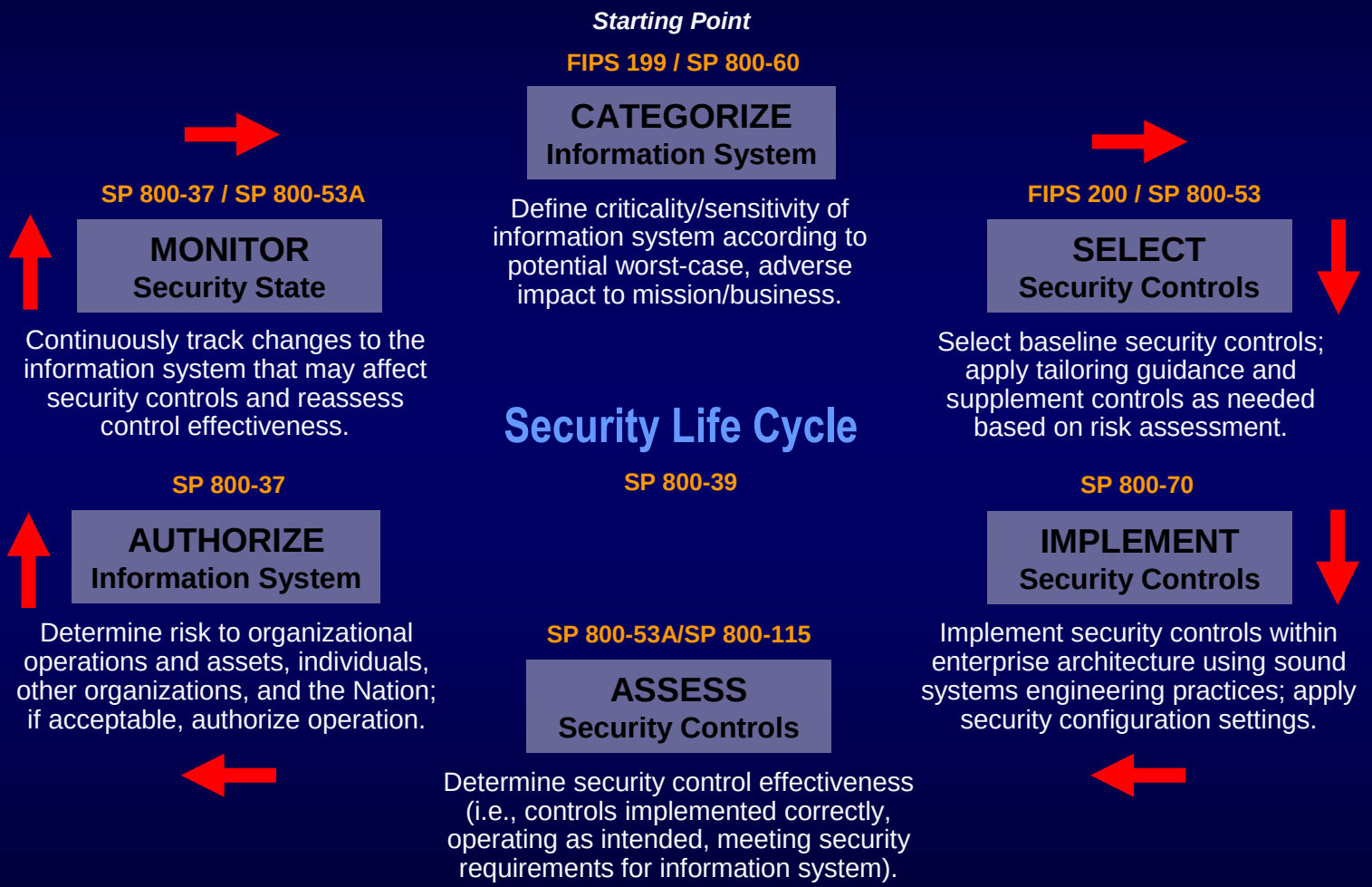
Enterprise-Wide Risk Management

- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Flexible and Agile Implementation



Risk Management Framework

System Perspective



Security Control Implementation

- Security controls (management, operational and technical) include:
  - Policies, Plans and Procedures;
  - Processes and Activities;
  - Mechanisms (hardware, software, firmware); and
  - Products and Services.
- Adequate information system security depends on security controls functioning as claimed when configured, integrated, and used in the end-user operational environment.

FISMA Implementation Project Initiatives

- Product and Service Supplier Assurance Initiative
- Support Tools, Techniques, Reference Materials, Practices and Processes Initiative

Assurance

- *Product assurance* is the grounds for confidence that the security functionality and quality of the product performs as claimed, and when employed within an information system or its supporting infrastructure, is effective in its application.

- An *assurance case* is a body of evidence organized into an argument demonstrating that some claim about an information security product holds (i.e., is assured).

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/assurance/643.html

Product Assurance

- ***Functionality***
  - Security-related functions or features of the system, for example, identification and authentication mechanisms, access control mechanisms, auditing mechanisms, and encryption mechanisms.
- ***Quality*** of the design, development, implementation, and operation
  - Degree to which the functionality is correct, always invoked, non bypassable, and resistant to tampering.
  - Achieved by employing well-defined security policy models, structured, disciplined, and rigorous hardware and secure software development techniques, and recommended system/security engineering principles and concepts when building an information system from information technology component products.
- ***Evidence***
  - Grounds for confidence that the claims made about the functionality and quality of the product are being met.
  - Achieved through a variety of sources including post-development evidence brought forward regarding the design and implementation of the information system and the results of independent assessments (e.g., analyses, testing, evaluation, inspections, and audits) of the system conducted by qualified assessors using a common set of techniques and tools.

Goals

- Build product assurance case throughout the SDLC
- Emphasis – Functional testing and assurance
- Leverage existing testing programs and assurance process (e.g., IT supplier security development methodology, SCAP, CMVP, CCEVS)
- Emphasis on use of automated tools to validate IT product functionality
- Supplier claims traceable to standards and guidelines and FISMA (e.g., FIPS 200 security requirements, SP 800-53 security controls, SP 800-115)

Security Control Assessment

- Emphasis on assessing security controls in the information system operational environment.
- Rigor of security assessments based on FIPS 199 information system impact level (i.e., low, moderate or high).

Approach to Assessing IT Products

- Security assurance case built from:
  - Suppliers (products) [1st party] (i.e., developmental test environment).
  - Product Evaluation [3rd party] (i.e., laboratory test environment).
  - Customers [2nd party] (i.e., operational test environment).
- Product assessment
  - Test laboratory (generically configured and detailed).
  - Operational environment (specifically configured and integrated).
  - Leverage common set of techniques and tools to produce assurance evidence to support the security claims.
- Emphasis on providing assurance results that can be readily used, confirmed, repeated and enhanced in the end-user operational (system) environment.

Product Supplier Information

- 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
- Security claims specified in terms of:
  - SP 800-53 functional requirements
  - SP 800-53 assurance requirements
- Evidence provided to support claims drawing on 800-53A assessment procedures and other assurance processes.
- Use of common S-CAP based protocols & automated tools

Functional Security Control (example)

Supporting Software Assurance

- Configuration Management (Operational)
  - Configuration Change Control
  - Security Impact Analysis
  - Access Restrictions for Change
  - Configuration Settings
  - Least Functionality
- System and Information Integrity (Operational)
  - Security Functionality Verification
  - Software and Information Integrity
  - Information Input Validation
  - Error Handling
  - Predictable Failure Prevention

Functional Security Control (example)

Supporting Software Assurance

- System and Services Acquisition (Management)
  - Resource Allocation
  - Acquisition and Life Cycle Support
  - Security Engineering Principles
  - Developer Configuration Management and Testing
  - Trustworthiness and Critical Information System Components
  - Supply Chain
- System and Communications Protection (Technical)
  - Application Partitioning
  - Security Function Isolation
  - Information Shared Resources
  - Trusted Path
  - Transmission of Security Attributes
  - Fail in Known State
  - Thin Nodes

Assurance Requirements (example)

Special Publication 800-53

- The security control is in effect and meets explicitly identified functional requirements in the control statement.
- The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control.

Supplier Claims Statement Uses

- Form of assurances that *supplier's* can readily provide with each product release.
- Base information for including in offers to *customers*.
- Base information *customers* can use for assessing product/service acceptance or for conducting supplemental assessments in the operational environment as needed.

Supplier Claims Statement Uses

- Base information that can be provided to *third party evaluators* (e.g., validation laboratories) for acquiring additional assurances.
- Base information for system security *assessment providers*.
- Information for *security plans* and *security assessment plans*.

Product Supplier Claims Statement

- Description of security features.
- Identification of 800-53 security controls product/service supported.
- Description of how product or service meets identified security control functional requirements.

Product Supplier Claims Statement

- Potential evidence to support claims.
  - Internal assessments reports.
  - External assessments reports (e.g., third party).
  - Use of SCAP validated products.
  - Results from configuration checklist testing.
- How evidence can be used or tailored to support SP 800-53A and system specific assessment procedures and processes.

Common Assessment Support Tools/References

- National Checklist Program (NCP)
- Security Content Automation Protocol (SCAP)
- Cryptographic Module Validation Program (CMVP)
- SCAP Validated Tools
- SP 800-115 Technical Guide to IS Testing
- Personal Identity Verification Program (NPIVP)
- Virtualization to verify supplier product claims (i.e., configuration / checklist / FDCC
- Others

Guidelines

- Product Supplier guide for product assurance claims submission – define minimum criteria, structure, form, etc. to support system security control implementation, and assessment.
- Test Laboratory guide for evaluating supplier product assurance claims.
- Customer guide on using supplier (1st party), test lab (3rd party, e.g., CMVP, CCEVS, other?) and customer (2nd party) assurances for building assurance cases for products operating in customer- specific system environments.

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Information and Feedback
Web: csrc.nist.gov/sec-cert
Comments: sec-cert@nist.gov