Information Security Continuous Monitoring

(Ongoing Monitoring in Support of Organizational Risk Management)

NIST SP 800-137

December 14th, 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

TIER 1
Organization
(Governance)

TIER 2
Mission / Business Process
(Information Assets and Information Flows)

TIER 3
Information System
(Environment of Operation)

STRATEGIC RISK FOCUS

TACTICAL RISK FOCUS

Characteristics of Risk-Based Approaches

(1 of 2)

- Integrates information security more closely into the enterprise architecture and system life cycle.
- Promotes near real-time risk management and ongoing system authorization through the implementation of robust continuous monitoring processes.
- Provides senior leaders with necessary information to make risk-based decisions regarding information systems supporting their core missions and business functions.

Characteristics of Risk-Based Approaches

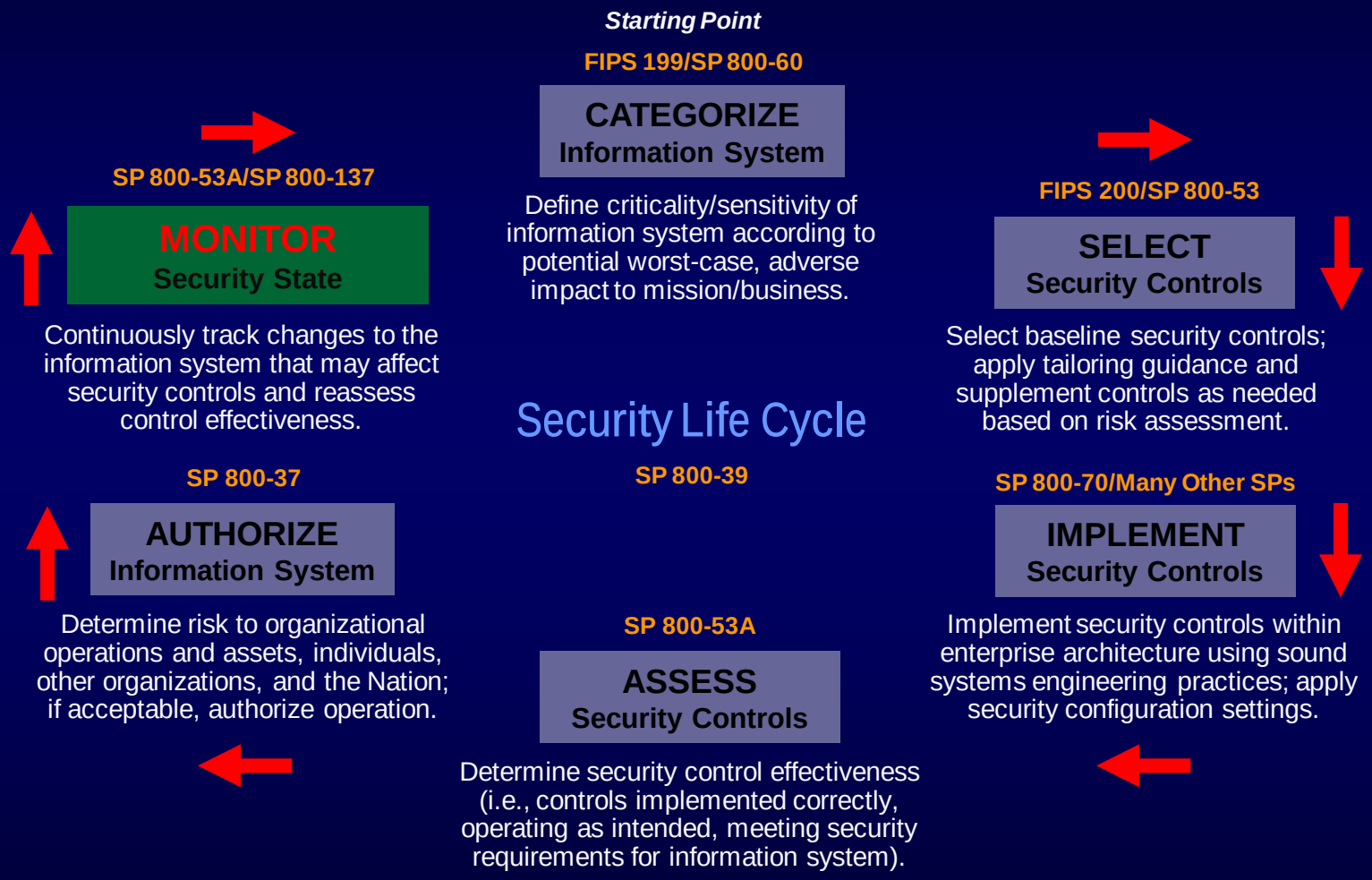
(2 of 2)

- Links risk management activities at the organization, mission, and information system levels through a risk executive (function).
- Establishes responsibility and accountability for security controls deployed within information systems.
- Encourages the use of automation to increase consistency, effectiveness, and timeliness of security control implementation.

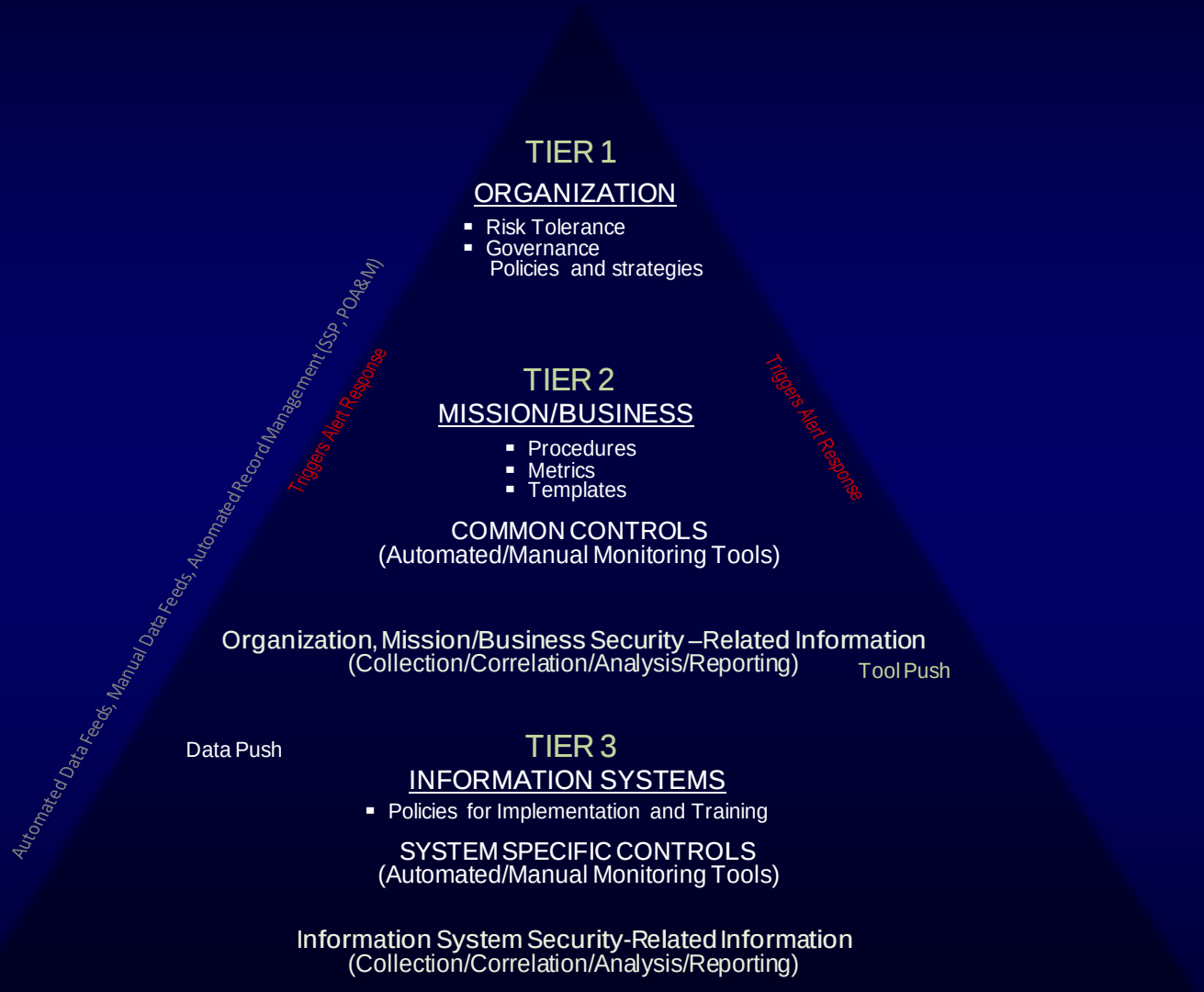
Monitoring History

- Not a totally new concept!
- Initially introduced in NIST SP 800-12 in 1995
- Expanded upon in OMB Circular A-130 Appendix III
- FISMA 2002
- NIST SP 800-37 in 2004 (Continuous Monitoring, 4th Step in system authorization)
- NIST SP 800-37 Rev. 1 (Continuous Monitoring a formal step in the RMF with organization-wide implications)

Continuous Monitoring & the RMF



Organization-wide Continuous Monitoring



Continuous Monitoring Working Definition (1 of 2)

- Continuous* monitoring (generic) is maintaining ongoing awareness to support organizational risk decisions.
- Information security continuous* monitoring is maintaining ongoing* awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

* The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed, analyzed and reported at a frequency sufficient to support risk-based security decisions as needed to adequately protect organization information.

Continuous Monitoring Working Definition (2 of 2)

- Objective: to conduct ongoing monitoring of the security of an organization's information, applications, networks, and systems, and respond to RISK accepting, avoiding/rejecting, transferring/sharing, or mitigating risk as situations change.

- Objective: to determine if the complete set of selected security controls implemented within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur.

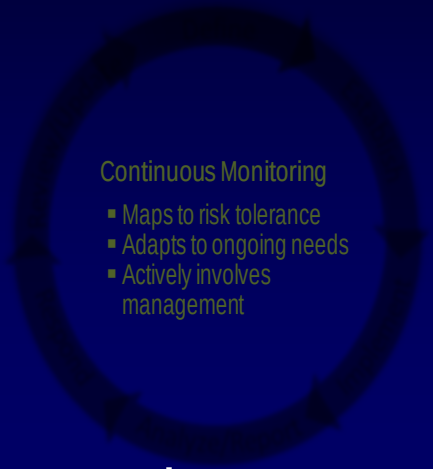
Continuous Monitoring Process (1 of 2)

The Continuous Monitoring Process, as described in NIST SP 800-137, is consistent with and an expansion of:

- Step Six of the Risk Management Framework (NIST SP 800-37 Revision 1)
- Appendix G of NIST SP 800-37 Revision 1
- Control CA-7 from NIST SP 800-53 Revision 3

Continuous Monitoring Process (2 of 2)

The Continuous Monitoring process steps, as described in NIST SP 800-137, consists of:



- Define Strategy
- Establish measures and metrics
- Establish monitoring and assessment frequencies
- Implement the monitoring program
- Analyze security-related information (data) and report findings
- Respond with mitigation actions OR reject/avoid, transfer, or accept risk
- Review and update monitoring strategy and program

Continuous Monitoring Process Step One

Define the Continuous Monitoring Strategy

- Tier 1:
  - Define the strategy in accordance with organizational risk tolerance (developed at Tier 1 based on guidance in NIST SP 800-39)
  - Develop policies to enforce the strategy
- Tier 2:
  - Assist/provide input to Tier 1 on strategy and policies
  - Develop procedures and templates to support the Tier 1 strategy and policies
- Tier 3:
  - Assist/provide input to Tier 2 on procedures
  - Establish information system-level strategy and procedures based on drivers from all three Tiers

Continuous Monitoring Strategy (1 of 2)

- Develop strategy focused on situational awareness for:
  - Risk management decisions
    - On-going authorization decisions
  - Asset and configuration management
  - Federal and organizational reporting requirements
- In addition to the original objective of monitoring for control effectiveness, the monitoring strategy also supports security posture monitoring (e.g., risk scoring tools like CAESARS)
- The continuous monitoring strategy itself is also monitored to ensure monitoring and reporting frequencies remain aligned with threats and organizational risk tolerance

Continuous Monitoring Strategy (2 of 2)

The Continuous Monitoring Strategy:

- Is grounded in a clear expression of organizational risk tolerance
- Includes measures and metrics that provide meaningful indications of security status at all organizational tiers
- Ensures continued effectiveness of all system defined security controls
- Is informed by and helps maintain visibility into organizational IT assets
- Ensures knowledge/control of changes via configuration management
- Facilitates proactive management of the security impact of changes
- Maintains awareness of threats and vulnerabilities
- Helps officials set priorities and manage risk within organizational risk tolerance levels

Continuous Monitoring Process Step Two

Establish Measures and Metrics

- Measures = all the security-related information from assessments and monitoring (manually **and** automatically generated)
- Metrics = measures organized into meaningful information that supports decision making
- Multiple measures may support one metric
- Example: A organization wants to monitor status of authorized and unauthorized components on a network.
  - The organization defines the metric as the % of unauthorized components connected to the network at a specified frequency (hourly, daily, weekly, etc.)
  - Measures to support this metric may include security-related information regarding physical asset locations, logical asset locations (subnets/IP addresses), MAC addresses, system association, policies/procedures for network connectivity, etc.

Continuous Monitoring Process Step Three

Establish Monitoring and Assessment Frequencies

- Monitor metrics/measures and each control with varying frequencies based on:
  - Control volatility
  - Organizational and system risk tolerance
  - Current threat and vulnerability information
  - System categorization/impact levels
  - Controls with identified weaknesses
  - Controls or system components providing critical security functions
  - Risk assessment results
  - Output of monitoring strategy reviews
  - Reporting requirements
- Multiple requirements within a control may have to be monitored with differing/varying frequencies.

Continuous Monitoring Process Step Four

Implement the Continuous Monitoring Program

- All controls are monitored and/or assessed (common, system, and hybrid controls)
- Tier 2 - Implement tools and processes associated with common controls and organization-wide monitoring (IDPS, vulnerability scanning, configuration management, asset management, etc.)
  - Organization-wide monitoring will likely pull security-related information from the system level
- Tier 3 – Implement tools and processes pushed down from Tier 2 and fill in any gaps at the system level
- Tiers 2 and 3 – Organize/prepare data for analysis

Continuous Monitoring Process Step Five

Analyze Data and Report Findings

- Data is analyzed in the context of:
  - Stated organizational risk tolerance
  - Potential impact of vulnerabilities on organizational and mission/business processes
  - Potential impact/costs of mitigation options
- Tier 3
  - Conducts initial analysis
  - Reports findings/provides recommendations to Tiers 2 and/or 1
- Tiers 1 and 2
  - Determine aggregate security status of effectiveness of controls (including common controls) for all systems in meeting organizational information security requirements
- Granularity of data varies with report recipient and frequency of report

Continuous Monitoring Process Step Six

Respond to Findings

- Determine if the organization will take remediation action, accept the risk, avoid/reject the risk, or transfer the risk (all tiers)
- Tier 1 Specific Response - Changes to strategy or policies
- Tier 2 Specific Response
  - Request additional information
  - Changes in procedures
  - Changes in common control implementations
- Tier 3 Specific Response
  - Implementation of additional controls/changes in existing control implementations
  - Additional/more detailed analysis of security-related information
  - Suspension or removal of authorization to operation

Continuous Monitoring Process Step Seven

Review/Update the Monitoring Strategy/Program

- Organizations establish a process for reviewing and modifying the strategy
  - Accuracy in reflecting organizational risk tolerance
  - Accuracy of measurements
  - Applicability of metrics
  - Applicability of monitoring frequencies and reporting requirements
- Factors precipitating changes to the strategy may include:
  - Changes to core missions or business processes
  - Significant changes in the enterprise architecture
  - Changes in organizational risk tolerance
  - Changes in threat and/or vulnerability information
  - Increase/decrease in POA&Ms related to specific controls or metrics
  - Trend analyses of status reporting output

Technologies for Enabling Continuous Monitoring

- Security engineering and direct data gathering
  - Security domains
- Aggregation and analysis
  - Security information and event management (SIEM)
  - Management dashboards
- Automation and Data Sources
  - Security content automation protocol (SCAP)
  - Data sources

Other Automation Enablers

- Leverage existing security status information and reporting available from security and security enabled products
- Leverage reference architectures for supporting such functions as tool integration, and gathering, collecting, and presentation of security system status information

Continuous Monitoring Automation

- Potential limitations
  - All controls may be not taken into account thus presenting a incomplete picture of overall organization security status and risk
  - Risk scores may not be comprehensive, i.e., it cannot score risks about which it has no information
  - Risk scoring is often based largely on automation of technical controls and not a substitute for monitoring other essential operational and management controls nor can it determine how security failures will affect organization functions and mission
  - Controls that do not lend themselves to automated monitoring must still be monitored/assessed and included for consideration in making organizational risk decisions
  - Automated tools can lead to a false sense of security

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

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

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

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

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov

Extra Slides

A Unified Framework

For Information Security

The Generalized Model

Unique Information Security Requirements

Intelligence Community	Department of Defense	Federal Civil Agencies	Private Sector State and Local Govt

Common Information Security Requirements

Foundational Set of Information Security Standards and Guidance

- Standardized risk management process
- Standardized security categorization (criticality/sensitivity)
- Standardized security controls (safeguards/countermeasures)
- Standardized security assessment procedures
- Standardized security authorization process

National security and non national security information systems

Joint Task Force Transformation Initiative

Core Risk Management Publications

- NIST Special Publication 800-53, Revision 3

  Recommended Security Controls for Federal Information Systems and Organizations

Completed

- NIST Special Publication 800-53A, Revision 1

  Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans

Completed

- NIST Special Publication 800-37, Revision 1

  Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach

Completed

Joint Task Force Transformation Initiative

Core Risk Management Publications

- NIST Special Publication 800-53, Revision 3

  Recommended Security Controls for Federal Information Systems and Organizations

Completed

- NIST Special Publication 800-53A, Revision 1

  Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans

Completed

- NIST Special Publication 800-37, Revision 1

  Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach

Completed

Joint Task Force Transformation Initiative

Core Risk Management Publications

- NIST Special Publication 800-39

  Enterprise-Wide Risk Management: Organization, Mission, and Information Systems View

  Final Projected: March 2011 (Final Public Draft projected for December 2010)

- NIST Special Publication 800-30, Revision 1

  Guide for Conducting Risk Assessments

  Final Projected: June 2011 (Initial Public Draft projected for January 2011)