NIST Special Publication 800-137

Information Security Continuous Monitoring for Federal Information Systems and Organizations

FISSEA 27th Annual Conference
Partners in Performance: Shaping the Future of Cybersecurity Awareness, Education, and Training

March 19th, 2014

Kelley Dempsey

Computer Security Division
Information Technology Laboratory

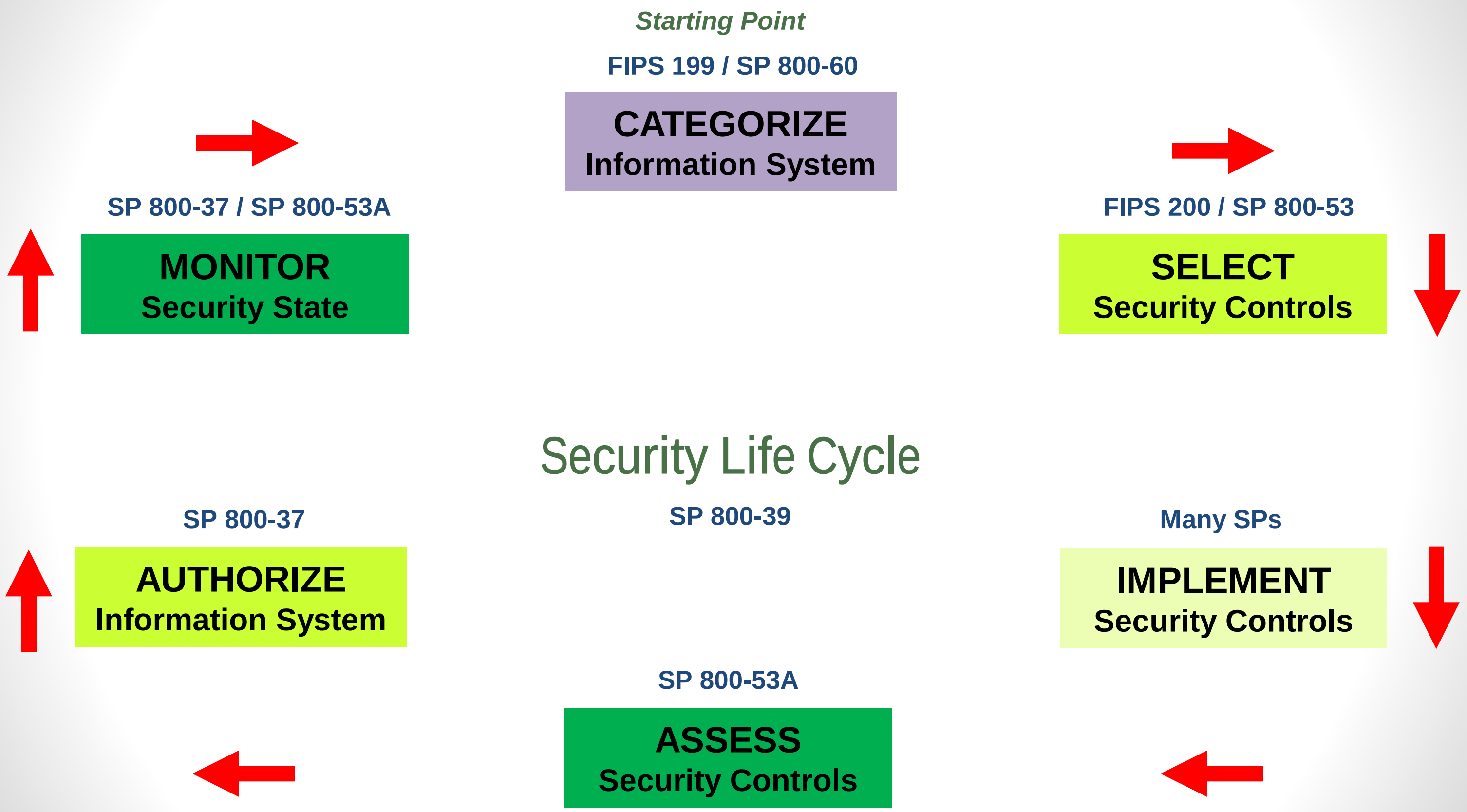
Why Monitor Continuously?

- Monitoring is required by FISMA and OMB A-130
- Continuous Monitoring was identified by the Administration as one of three Cross-Agency Priorities for Cybersecurity (95% by end of FY14)
- **Continuous Monitoring is the only way to maintain situational awareness of organizational and system security posture in support of risk management**

Objectives of Information Security Continuous Monitoring (ISCM)

- Conduct ongoing monitoring of security
- Determine if security controls continue to be effective over time
- Respond to risk as situations change
- Ensure monitoring and reporting frequencies remain aligned with organizational threats and risk tolerance

Risk Management Framework



Starting Point

FIPS 199 / SP 800-60

CATEGORIZE
Information System

FIPS 200 / SP 800-53

SELECT
Security Controls

Many SPs

IMPLEMENT
Security Controls

SP 800-53A

ASSESS
Security Controls

SP 800-37

AUTHORIZE
Information System

SP 800-37 / SP 800-53A

MONITOR
Security State

Security Life Cycle

SP 800-39

OMB Policy Change

OMB 2013 FISMA Reporting Guidance, *Memorandum-14-04*

http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-04.pdf, question #34

- "34. Is a security reauthorization still required every 3 years or when an information system has undergone significant change as stated in OMB Circular A-130? No. Rather than enforcing a static, three-year reauthorization process, agencies are expected to make ongoing authorization decisions for information systems by leveraging security-related information gathered through the implementation of ISCM programs. Implementation of ISCM and ongoing authorization thus fulfill the three year security reauthorization requirement, so a separate reauthorization process is not necessary."
- Follow guidance in NIST Special Publications 800-37 Revision 1 and 800-137

Bottom Line: Use security-related information from ISCM to support ongoing authorization

Term Confusion?

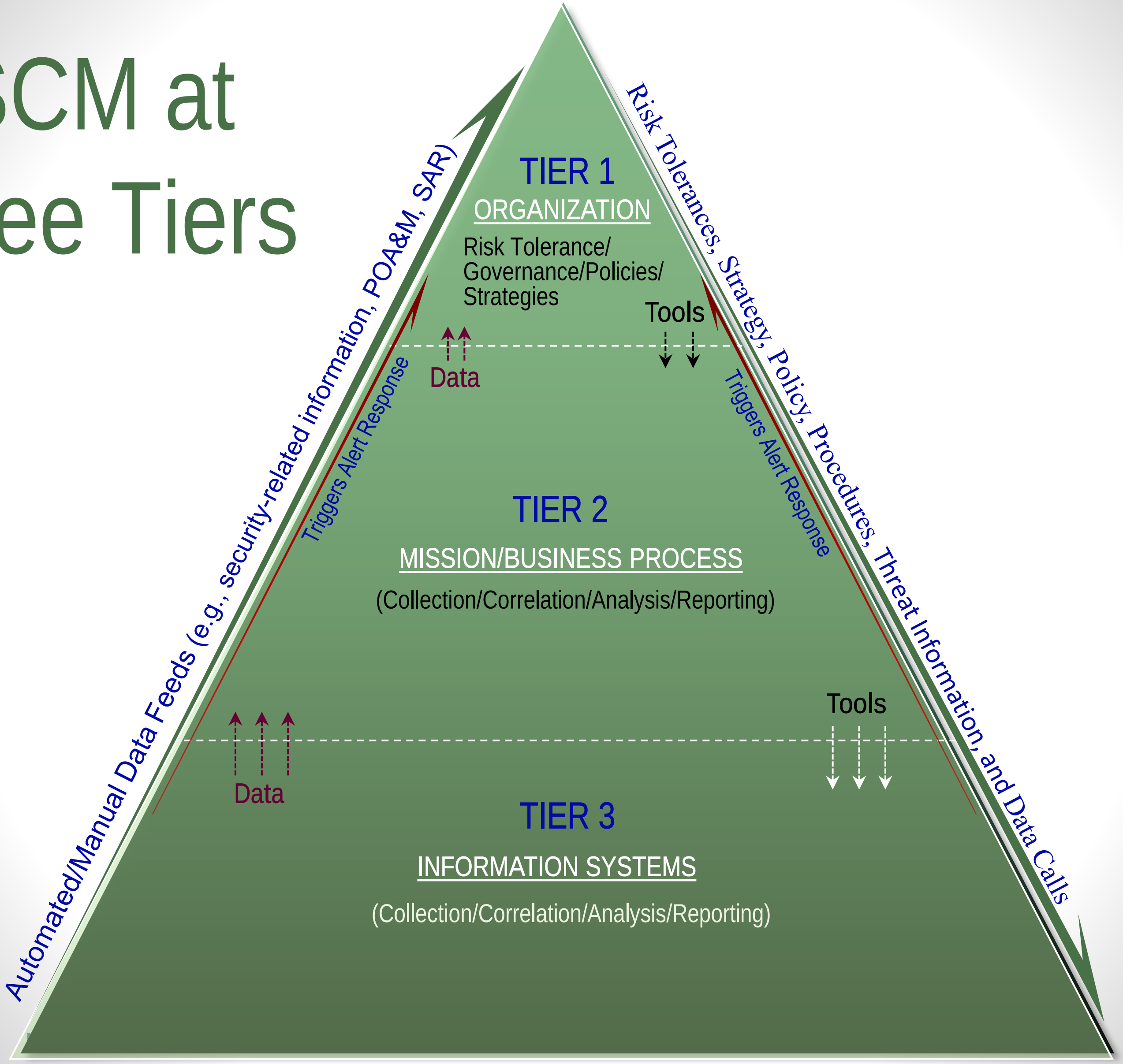
- Information Security Continuous Monitoring
- Reauthorization (to operate)
- Ongoing Authorization (to operate)
- Ongoing Assessment
- Continuous Diagnostics and Monitoring

NIST SP 800-137 Definition

Information security continuous[*] monitoring (ISCM) 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. Data collection, no matter how frequent, is performed at discrete intervals.

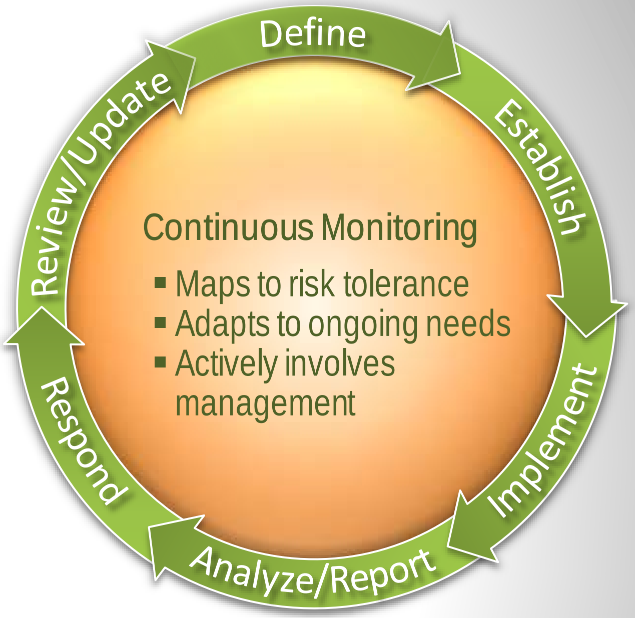
ISCM at Three Tiers



TIER 1
ORGANIZATION
Risk Tolerance/ Governance/Policies/ Strategies
Tools
Data
TIER 2
MISSION/BUSINESS PROCESS
(Collection/Correlation/Analysis/Reporting)
Tools
Data
TIER 3
INFORMATION SYSTEMS
(Collection/Correlation/Analysis/Reporting)
Triggers Alert Response
Triggers Alert Response
Automated/Manual Data Feeds (e.g., security-related information, POA&M, SAR)
Risk Tolerances, Strategy, Policy, Procedures, Threat Information, and Data Calls

NIST

ISCM Process Steps



1. **Define** continous monitoring **strategy**
2. **Establish** continuous monitoring **program**
   a) Determine **metrics**
   b) Determine monitoring **frequencies**
   c) Develop ISCM **architecture**
3. **Implement** the monitoring program
4. **Analyze** security-related information (data) and **report** findings
5. **Respond** to findings
6. **Review** and **update** monitoring strategy and program

Step 1: Define the ISCM Strategy

- Tier 1 - Organization:
  - Define the organization-wide 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 – Mission/Business Process:
  - Assist/provide input to Tier 1 on strategy and policies
  - Develop procedures/templates to support Tier 1 strategy and fill in gaps
- Tier 3 – Information System:
  - Assist/provide input to Tier 2 on procedures
  - Establish information system-level procedures

Step 2: Establish the ISCM Program

Three parts:

a) Determine metrics

b) Determine monitoring frequencies

c) Develop technical architecture

Step 2a: Determine Metrics

- Metrics - **All** the security-related information from assessments and monitoring (manually **and** automatically generated) **organized** into meaningful statistics that support decision making
- Security-related information from multiple sources may support a single metric
- Metrics should **have a meaningful purpose** that is mapped or tied to a specific objective that helps maintain or improve the security posture of the system/organization

Step 2b: Establish Monitoring and Assessment Frequencies

- Monitor metrics and <u>each</u> control with varying frequencies
- Multiple requirements within a control may have to be monitored with differing/varying frequencies

Frequency Determination Criteria

- Control volatility
- Organizational and system risk tolerance
- Current threat and vulnerability information
- System categorization/impact levels
- Controls with identified weaknesses
- Controls/components providing critical security functions
- Risk assessment results
- Output of monitoring strategy reviews
- Reporting requirements

Frequency Determination Example: Volatility

- MA-5a – The organization establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel
- Is volatility the only criterion to consider?

Step 2c: Develop ISCM Architecture

- Continuous monitoring architecture uses standard protocols and specifications
- Organizations seek to leverage existing tools/applications and infrastructure for continuous monitoring architecture
- NISTIRs 7756, 7799, & 7800 describe a technical architecture that support ISCM

Step 3: Implement the ISCM Program

- **All** controls and metrics are monitored and/or assessed (common, system, and hybrid controls) at the frequency identified in step three

- 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 pull at least some 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

Step 4: Analyze Data and Report Findings

- Analyze Data in the context of:
  - Stated organizational risk tolerance
  - Potential impact of vulnerabilities on organizational and mission/business processes
  - Potential impact/costs of mitigation options (vs. other response actions)
- Report on Assessments
- Report on Security Status Monitoring

Step 5: Respond to Findings

- Determine if the organization will:
  - Take remediation action
  - Accept the risk
  - Reject the risk
  - Transfer/Share the risk
- Specific response actions will vary by Tier
- May need to prioritize remediation actions

Step 6: Review/Update the ISCM Strategy

- Organizations establish a process for reviewing and modifying the strategy
- Various factors may precipitate changes to the strategy

Step 6: Strategy Review Considerations

- Is the strategy an accurate reflection of organizational risk tolerance?
- Applicability of metrics
- Applicability/appropriateness of:
  - Monitoring frequencies
  - Reporting requirements

Step 6: Strategy Update Factors

- Changes to missions/business processes
- Changes in enterprise and/or security architecture
- Changes in risk tolerance
- Revised threat or vulnerability information
- Increase or decrease in POA&Ms for specific controls or metrics
- Trend analyses of status reporting output

Automating Continuous Monitoring

SP 800-137 Appendix D

ISCM Processes Supported by Technology

- Ongoing assessments of security control effectiveness
- Reporting of security status
- Management of risk and verification and assessment of mitigation activities
- Assurance of compliance with internal and external requirements
- Analysis of the security impact of changes to the operational environment

Technologies for Enabling ISCM

- Direct Data Gathering
- Aggregation and Analysis
- Automation Data Sources

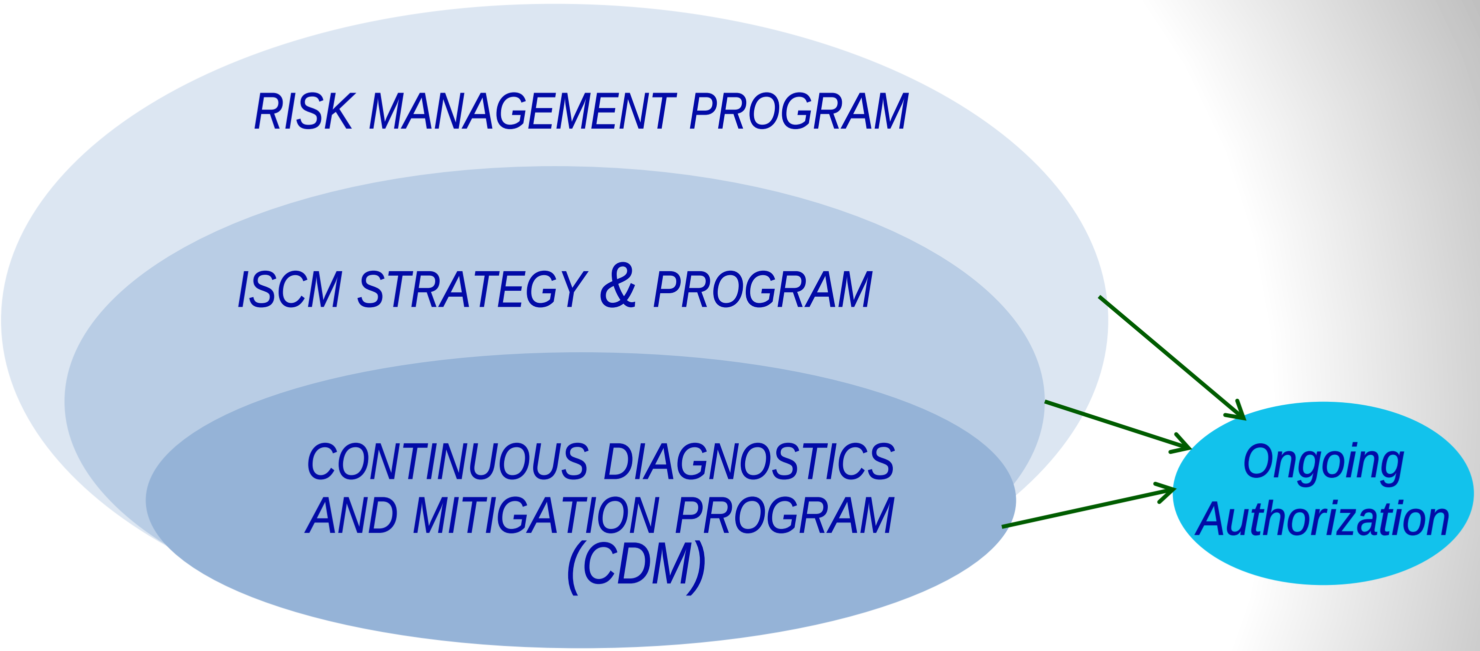
Automation Data Sources

- National Vulnerability Database (NVD)
  - http://nvd.nist.gov
  - More than 50,000 CVEs
  - CPE dictionary
  - Data available via Web, XML feeds, and RSS Feeds
  - iAssurance iPhone app
- National Checklist Program (NCP)
  - http://checklists.nist.gov
  - More than 230 checklists
  - Created by Government, academia, industry, product vendors
  - Prose and SCAP-expressed format
- SCAP validated tools use these data sources!

Security Content Automation Protocol (SCAP)

- Standardized format for communicating security information
- Open specifications, community driven
- Creates interoperability across disparate products
- Languages – XCCDF, OVAL, OCIL
- Reporting formats – ARF, AI
- Enumerations – CPE, CCE, CVE
- Measurement and scoring – CVSS, CCSS

RM, ISCM, and the DHS CDM Program



ISCM is a subset of a comprehensive risk management program and CDM is a subset of a holistic ISCM program

ISCM Automation: The Need for Caution

- Automated tools may lead to a false sense of security
  - A complete picture of overall security posture may not be provided
  - May not provide information on nontechnical security controls
  - May not be possible to automate monitoring the effectiveness of policies and procedures
  - May not be able to monitor all assets/all platforms
- The tools must be monitored for accuracy and integrity
- The tools may generate a quantity of data too large for adequate analysis and response
- The tools must be interoperable

OMB Memo 14-03

- Mandates dates for agencies to complete specific ISCM-related tasks:
  - Develop ISCM strategy by 2-28-14 ☺
  - Inventory staff/resources for ISCM by 4-30-14
  - Begin procurement of ISCM products by 2-28-14
  - Begin to deploy ISCM products by 5-20-14
  - Install dashboard and begin submitting data feeds within six months of its availability (DHS to provide dashboard)
  - Implement phase 1 CDM focus areas upon dashboard activation
    - HW & SW asset management
    - Configuration setting management
    - Common vulnerability management
  - NIST to provide guidance on OA by 3-31-13

http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf

Contact Information

NIST FISMA Project Leader

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

NIST *Administrative Support*

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

NIST Senior Information Security Researchers and Technical Support

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

Kevin Stine
(301) 975-4483
kevin.stine@nist.gov

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

Comments: **sec-cert@nist.gov**

Web: **csrc.nist.gov/sec-cert**