NIST Special Publication 800-137

Information Security Continuous Monitoring for Federal Information Systems and Organizations

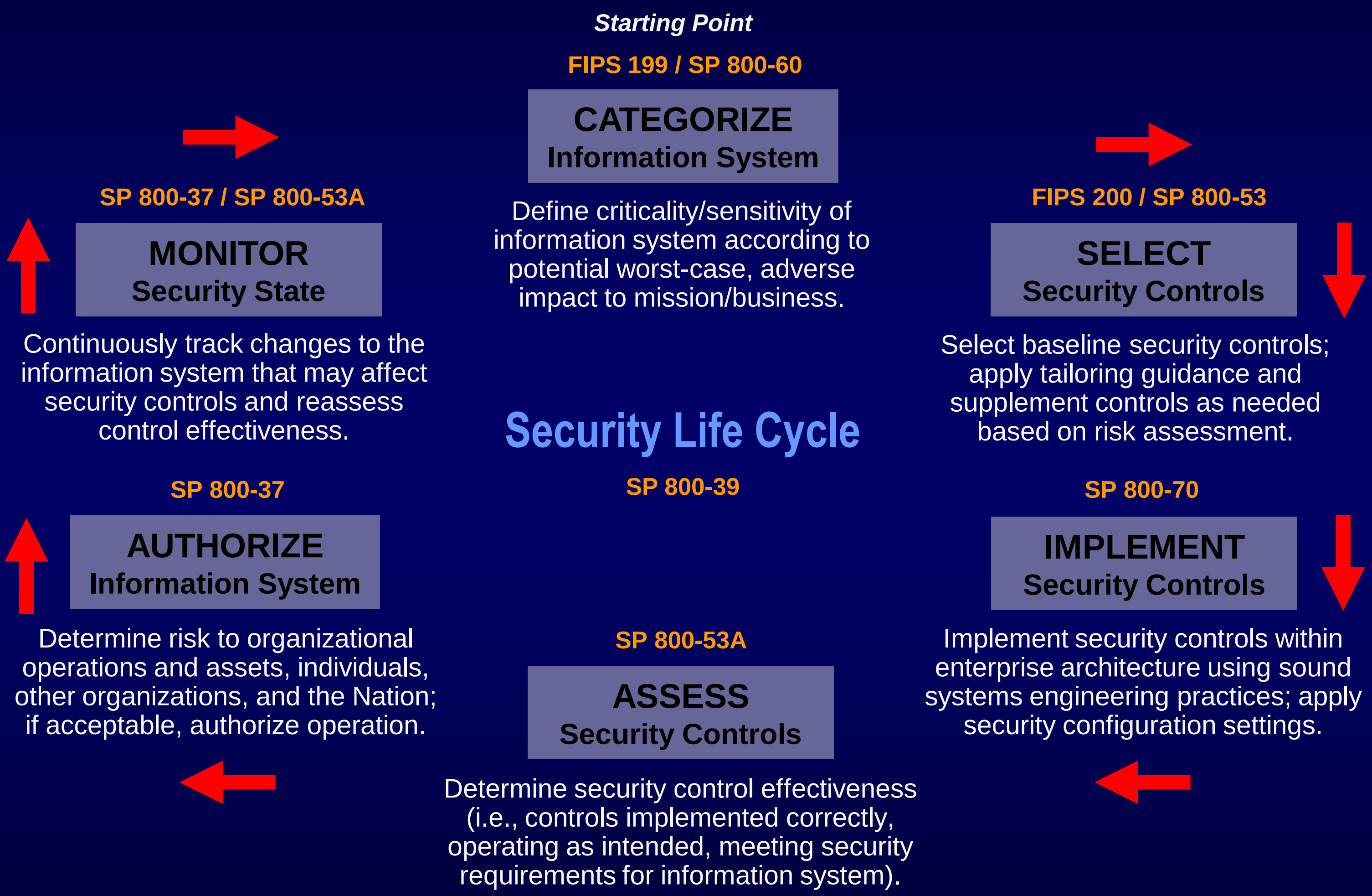
Security Automation Conference

November 1, 2011

Kevin Stine and Kelley Dempsey

Computer Security Division
Information Technology Laboratory

Risk Management Framework



Starting Point

FIPS 199 / SP 800-60

CATEGORIZE
Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

FIPS 200 / SP 800-53

SELECT
Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

SP 800-70

IMPLEMENT
Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-53A

ASSESS
Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

SP 800-37

AUTHORIZE
Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

SP 800-37 / SP 800-53A

MONITOR
Security State

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Security Life Cycle

SP 800-39

Policy Changes (Authorize & Monitor)

OMB 2011 FISMA Reporting Guidance, *Memorandum-11-33*

http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf, question #28

- "28. 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 conduct ongoing authorizations of information systems through the implementation of continuous monitoring programs. Continuous monitoring programs thus fulfill the three year security reauthorization requirement, so a separate reauthorization process is not necessary**………"
- Follow guidance consistent with NIST Special Publication 800-37, Revision 1

Bottom Line: Rather than enforcing a static, three-year reauthorization process, agencies are expected to conduct ongoing authorizations of Information systems through the implementation of continuous monitoring programs.

Objectives of Information Securty Continuous Monitoring (ISCM)

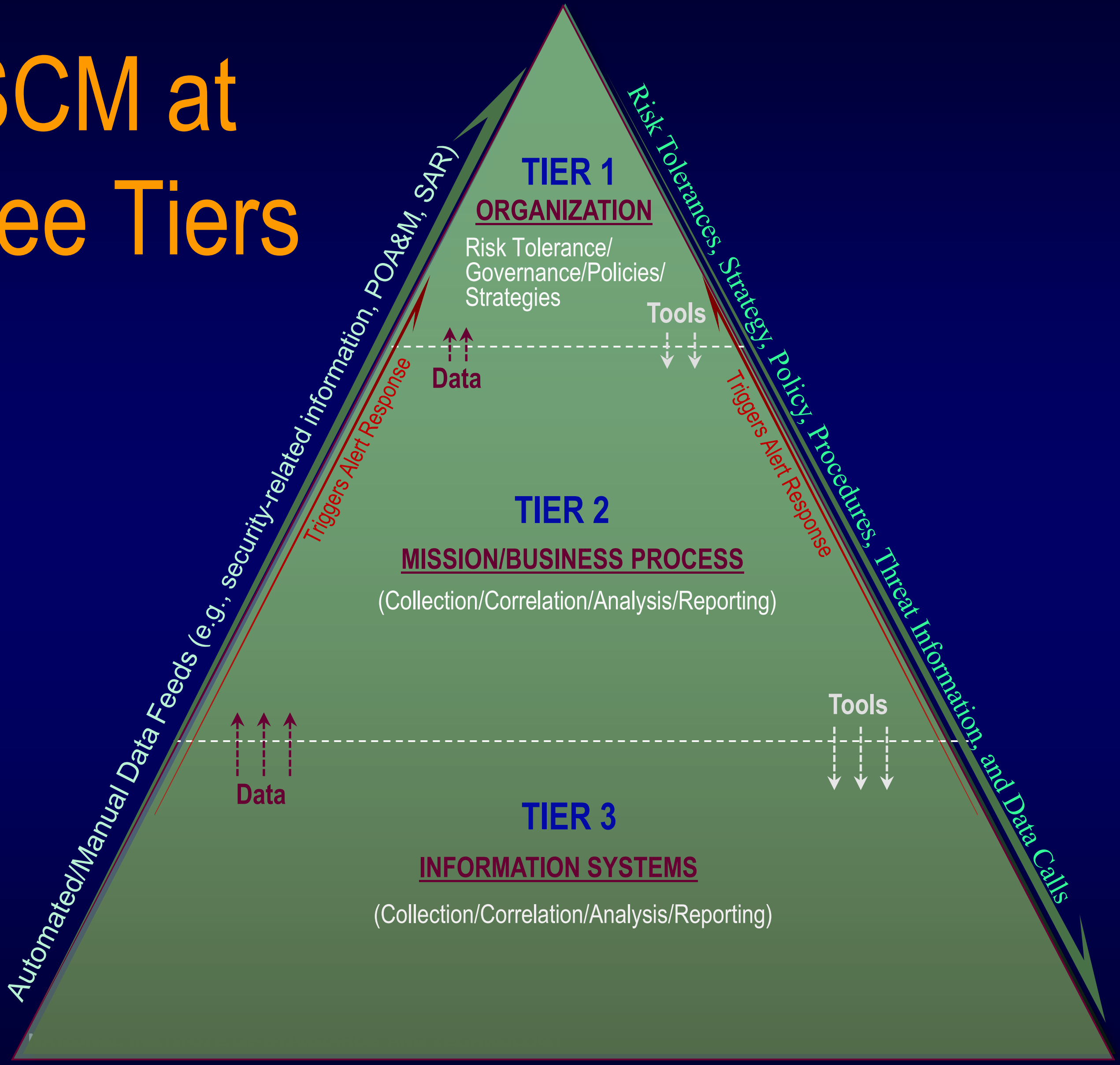
- Conduct ongoing monitoring of security
- Determine if security controls continue to be effective over time
- Respond to risk as situations change
- Ensure monitoring and reporting frequencies remain aligned with threats and organizational risk tolerance by monitoring the monitoring strategy itself

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

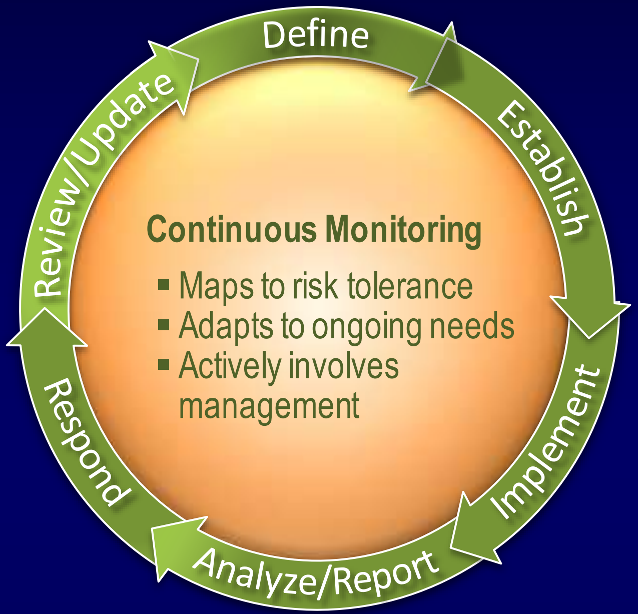
* The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed, analyzed and reported at a frequency sufficient to support risk-based security decisions as needed to adequately protect organization information. Data collection, no matter how frequent, is performed at discrete intervals.

ISCM at Three Tiers


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

ISCM Process Steps

The Continuous Monitoring process, as described in NIST SP 800–137, consists of six 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 with mitigation actions OR reject/avoid, transfer, or accept risk
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 information that supports 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

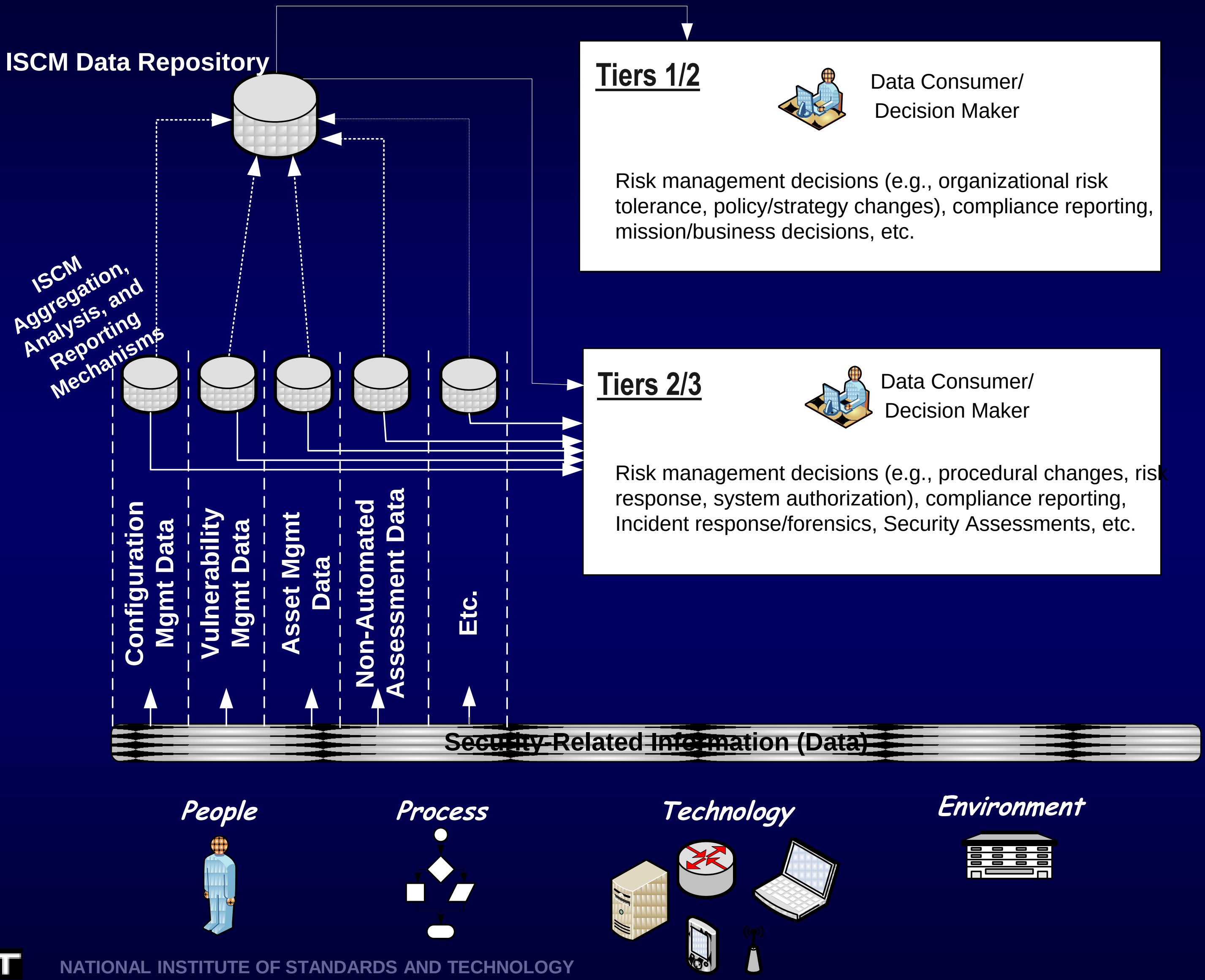
Step 2b: Establish Monitoring and Assessment Frequencies

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

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

High-Level Architecture Example


ISCM Data Repository
ISCM Aggregation, Analysis, and Reporting Mechanisms
Configuration Mgmt Data
Vulnerability Mgmt Data
Asset Mgmt Data
Non-Automated Assessment Data
Etc.
Security-Related Information (Data)
People
Process
Technology
Environment
Tiers 1/2
Data Consumer/ Decision Maker
Tiers 2/3
Data Consumer/ Decision Maker

Tiers 1/2 – Data Consumer/ Decision Maker

Risk management decisions (e.g., organizational risk tolerance, policy/strategy changes), compliance reporting, mission/business decisions, etc.

Tiers 2/3 – Data Consumer/ Decision Maker

Risk management decisions (e.g., procedural changes, risk response, system authorization), compliance reporting, Incident response/forensics, Security Assessments, etc.

Step 3: Implement the ISCM Program

- All controls 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 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

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
- Report on Assessments
- Report on Security Status Monitoring

Step 5: Respond to Findings

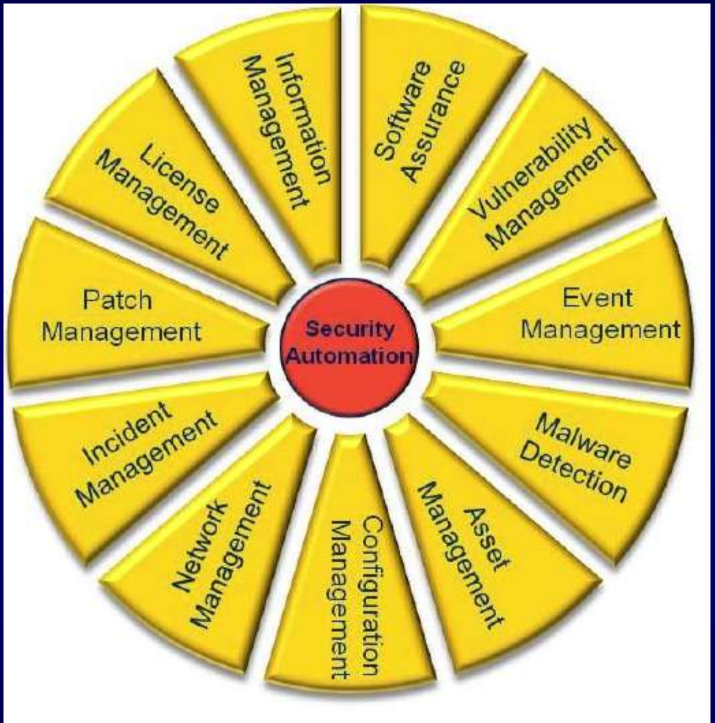
- Determine if the organization will:
  - Take remediation action
  - Accept the risk
  - Reject the risk
  - Transfer/Share the risk
- Specific response actions will vary by Tier

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

Technologies for Enabling ISCM

- Direct data gathering
  - 11 security domains
- Aggregation and analysis
  - Security information and event management (SIEM)
  - Management dashboards
- Automation and Data Sources
  - Security content automation protocol (SCAP), XML, etc.
  - Data sources



Continuous Monitoring Domains

ISCM Automation: The Need for Caution

- Automated tools may lead to a false sense of security by not providing a complete picture of the overall security posture
- The tools must be monitored for accuracy and integrity
- Interoperability

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

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

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov