NIST's Role in Ongoing Assessments

NIST/DHS Workshop

April 10th, 2014

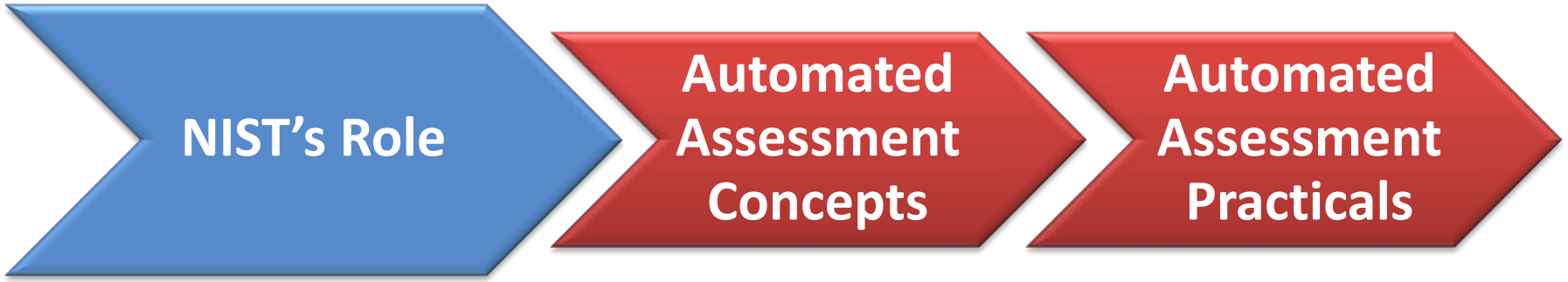
Kelley Dempsey
Dr. George Moore

NIST

Homeland Security

Module 1: NIST's Role

- Where in the training sequence does this module fit?



Module 1
1 hour

Module 2
2 hours

Module 3
1 hour

Overview

- Learning Objectives
- NIST and Cybersecurity
- Steps of the RMF
- Purpose of Continuous Monitoring
- Role of an Organizational Information Security Continuous Monitoring (ISCM) Program
- Continuous Monitoring and Ongoing Assessments
- NIST's View on Automation
- ISCM Roles and Responsibilities
- Defining an ISCM Strategy
- Building an ISCM Program
- Analyzing Data
- Responding to Findings / Defects
- Updating the ISCM

Learning Objectives

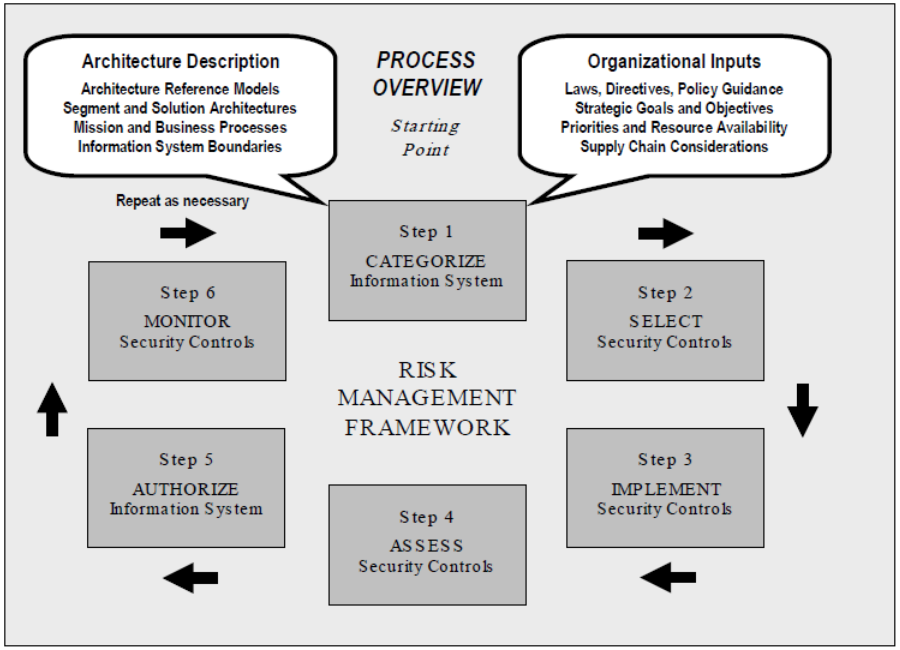
- **At the conclusion of this module, the participants will be able to:**
  - Describe the role that NIST plays in cybersecurity.
  - Understand the role of the Risk Management Framework.
  - Define the six steps with the Risk Management Framework.
  - Identify the purpose that Continuous Monitoring plays.
  - Understand the role of the organizational ISCM program.
  - Define how continuous monitoring promotes ongoing assessments.
  - Define NIST's view on the role of automation within an ISCM.
  - Understand how to develop an ISCM strategy.
  - Learn about how to build and implement an ISCM program.
  - Understand the role of analyzing data within an ISCM program.
  - Describe how to respond to findings with an ISCM.
  - Identify the need to monitor and update the ISCM based upon situational awareness.

NIST and Cybersecurity

- NIST Defines
  - Information security standards
  - Information security guidelines
  - Minimum security requirements for federal information systems
- Important Information Security Publications
  - Special Publication 800-30
  - Special Publication 800-37
  - Special Publications 800-53/53A
  - Special Publication 800-39
  - Special Publication 800-137

Steps of the RMF

- Risk Management Framework
  - Broken into 6 steps
    - Step 1 – Categorize
    - Step 2 – Select Controls
    - Step 3 – Implement Controls
    - Step 4 – Assess Controls
    - Step 5 – Authorize Controls
    - Step 6 - Monitor

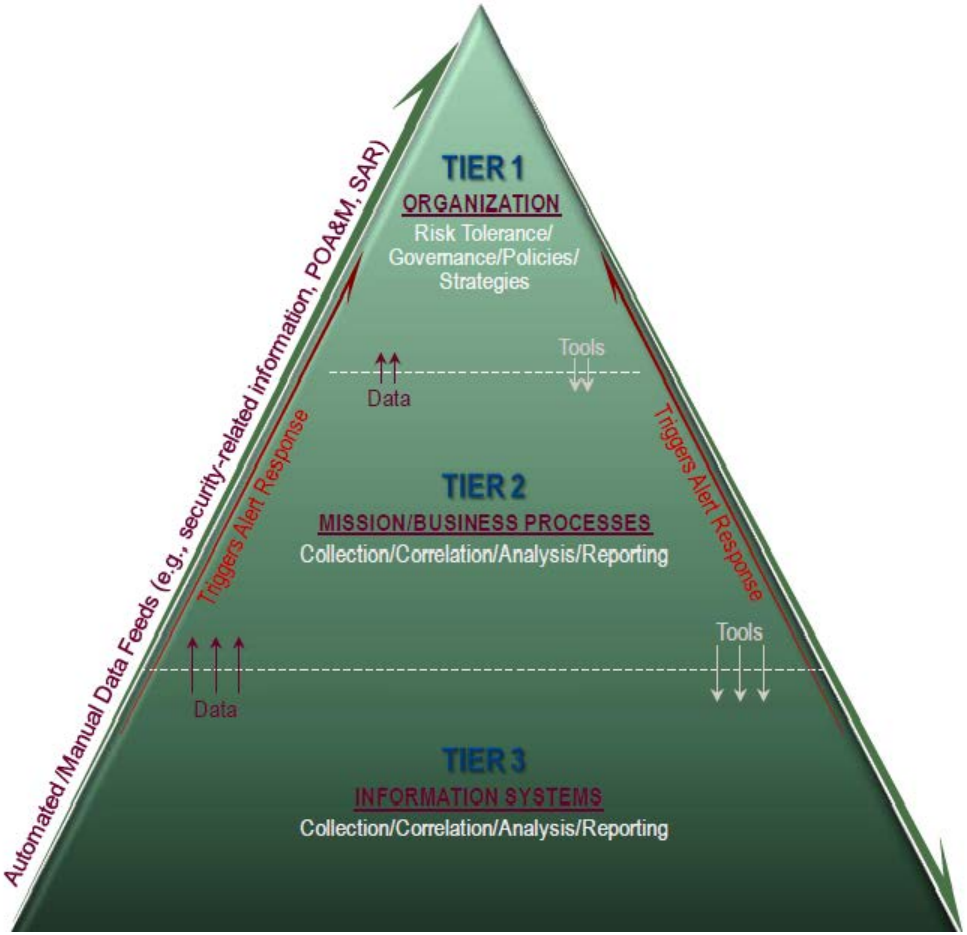


Purpose of Continuous Monitoring

- Definition: maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions
  - necessitates
    - maintaining situational awareness of all systems across the organization;
    - maintaining an understanding of threats and threat activities;
    - assessing all security controls;
    - collecting, correlating, and analyzing security-related information;
    - providing actionable communication of security status across all tiers of the organization; and
    - active management of risk by organizational officials
  - gives organizational officials access to security-related information on demand, enabling timely risk management decisions, including authorization decisions.

Role of an Organizational Information Security Continuous Monitoring (ISCM) Program

- An organization-wide approach to continuous monitoring of information and information system security supports risk-related decision making at the *organization level (Tier 1), the mission/business processes level (Tier 2), and the information systems level (Tier 3).*



Continuous Monitoring and Ongoing Assessments

- Focus is on Steps 4 and 6 of the RMF (but begins in Step 2)
- Ongoing assessment of security control effectiveness supports a system's security authorization over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes.
- New threat or vulnerability information is evaluated as it becomes available, permitting organizations to make adjustments to security requirements or individual controls as needed to maintain authorization decisions.
- A security control assessment and risk determination process, otherwise static between authorizations, is thus transformed into a dynamic process that supports timely risk response actions and cost-effective, ongoing authorizations.

NIST's View on Automation

- When possible, organizations look for automated solutions to lower costs, enhance efficiency, and improve the reliability of monitoring security-related information.
- The automation of information security deals primarily with automating aspects of security that require little human interaction.
  - Benefits
    - able to recognize patterns and relationships that may escape the notice of human analysts.
    - augment the security processes conducted by security professionals within an organization and may reduce the amount of time a security professional must spend on doing redundant tasks.

NIST's View on Automation

- When determining the extent to which the organization automates ISCM, organizations consider potential efficiencies of process standardization that may be gained with automation, and the potential value (or lack of value) of the automated security-related information from a risk management perspective.
- Cautionary note:
  - Watch out for false sense of security!
  - Be aware of the scope of any automated tools

ISCM Roles and Responsibilities

- Head of Agency
- Risk Executive (Function)
- Chief Information Officer (CIO)
- Senior Information Security Officer (SISO)
- Authorizing Official (AO)
- Information System Officer/Information Owner/Steward
- Common Control Provider
- Information System Security Officer (ISSO)
- Security Control Assessor

ISCM Roles and Responsibilities

- Head of Agency
  - The agency head is likely to participate in the organization's ISCM program within the context of the risk executive (function).

ISCM Roles and Responsibilities

- Risk Executive (Function)
  - The risk executive (function) oversees the organization's ISCM strategy and program. The risk executive (function) reviews status reports from the ISCM process as input to information security risk posture and risk tolerance decisions and provides input to mission/business process and information systems tier entities on ISCM strategy and requirements; promotes collaboration and cooperation among organizational entities; facilitates sharing of security-related information; provides an organization-wide forum to consider all sources of risk; and ensures that risk information is considered for continuous monitoring decisions.

ISCM Roles and Responsibilities

- Chief Information Officer (CIO)
  - The CIO leads the organization's ISCM program. The CIO ensures that an effective ISCM program is established and implemented for the organization by establishing expectations and requirements for the organization's ISCM program; working closely with authorizing officials to provide funding, personnel, and other resources to support ISCM; and maintaining high-level communications and working group relationships among organizational entities.

ISCM Roles and Responsibilities

- Senior Information Security Officer (SISO)
  - The SISO establishes, implements, and maintains the organization's ISCM program; develops organizational program guidance (i.e., policies/procedures) for continuous monitoring of the security program and information systems; develops configuration management guidance for the organization; consolidates and analyzes POA&Ms to determine organizational security weaknesses and deficiencies; acquires or develops and maintains automated tools to support ISCM and ongoing authorizations; provides training on the organization's ISCM program and process; and provides support to information owners/information system owners and common control providers on how to implement ISCM for their information systems.
  - Also known as the SAISO or CISO
    - SAISO = Senior Agency Information Security Officer
    - CISO = Chief Information Security Officer

ISCM Roles and Responsibilities

- Authorizing Official (AO)
  - The AO assumes responsibility for ensuring the organization's ISCM program is applied with respect to a given information system. The AO ensures the security posture of the information system is maintained, reviews security status reports and critical security documents and determines if the risk to the organization from operation of the information system remains acceptable.

ISCM Roles and Responsibilities

- Information System Officer/Information Owner/Steward
  - The ISO establishes processes and procedures in support of system-level implementation of the organization's ISCM program.

ISCM Roles and Responsibilities

- Common Control Provider
  - The common control provider establishes processes and procedures in support of ongoing monitoring of common controls.

ISCM Roles and Responsibilities

- Information System Security Officer (ISSO)
  - The ISSO supports the organization's ISCM program by assisting the ISO in completing ISCM responsibilities and by participating in the configuration management process.

ISCM Roles and Responsibilities

- Security Control Assessor
  - The security control assessor provides input into the types of security-related information gathered as part of ISCM and assesses information system or program management security controls for the organization's ISCM program.

Defining an ISCM Strategy

- A well-designed ISCM strategy encompasses security control assessment, security status monitoring, and security status reporting in support of timely risk-based decision making throughout the organization.
  - The ISCM strategy is based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.

Building an ISCM Program

- Two steps
  - Establish the ISCM by
    - determining metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture.
  - Implement the ISCM by
    - collecting the security-related information required for metrics, assessments, and reporting.
      - Automate collection, analysis, and reporting of data where possible.

Analyzing Data

- Analyze the data collected and Report findings, determining the appropriate response. It may be necessary to collect additional information to clarify or supplement existing monitoring data.

Responding to Findings / Defects

- Respond to findings with technical, management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.

Updating the ISCM

- Review and Update the monitoring program, adjusting the ISCM strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities, further enable data-driven control of the security of an organization’s information infrastructure, and increase organizational resilience.

Recap

- Learning Objectives
- NIST and Cybersecurity
- Steps of the RMF
- Purpose of Continuous Monitoring
- Role of an Organizational Information Security Continuous Monitoring (ISCM) Program
- Continuous Monitoring and Ongoing Assessments
- NIST's View on Automation
- ISCM Roles and Responsibilities
- Defining an ISCM Strategy
- Building an ISCM Program
- Analyzing Data
- Responding to Findings / Defects
- Updating the ISCM