# Automated Assessment Practicals

NIST/DHS Workshop

April 10th, 2014

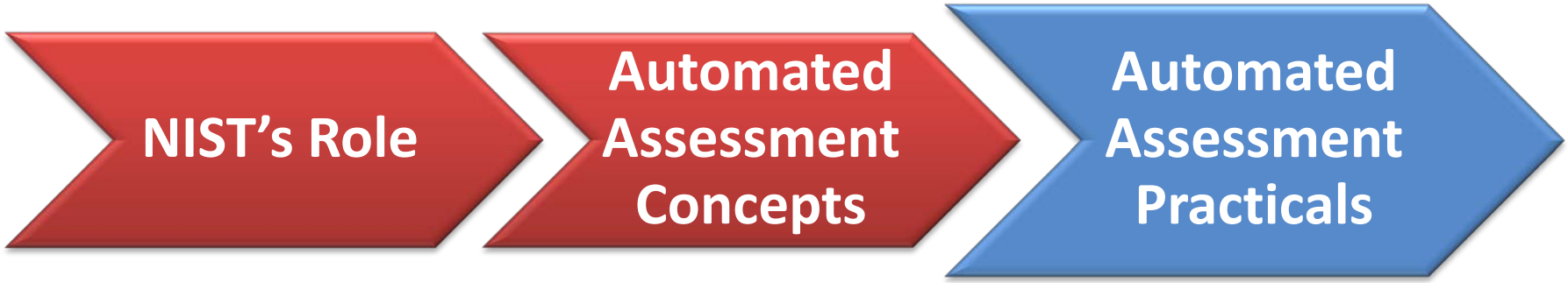
Kelley Dempsey
Dr. George Moore

NIST

Homeland Security

# *Module 3: Automated Assessment Practicals*

- Where in the training sequence does this module fit?




**Module 1**
**1 hour**

**Module 2**
**2 hours**

**Module 3**
**1 hour**

# *Overview*

- ❑ **Learning Objectives**
- ❑ **Automating the Security Lifecycle**

# *Learning Objectives*

- **At the conclusion of this module, the participants will be able to:**
  - Identify how CDM can be used to automate the security lifecycle promoted by the NIST Risk Management Framework (RMF).

# *Automating the Security Life Cycle (800-37)*

Pertinent RMF Step 4: Assess Security Controls

- *Task 4-1 Assessment Preparation*
  - Develop, review and approve a plan to assess the security controls.
- *Task 4-2 Security Control Assessment*
  - Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.
- *Task 4-3 Security Assessment Report*
  - Prepare the security assessment report documenting the issues, findings, and recommendations.
- *Task 4-4 Remediation Actions*
  - Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate

# *Automating the Security Life Cycle (800-37)*

## RMF Step 4, Task 4-1: Assessment Preparation

### Traditional Approach

*TASK 4-1: Develop, review, and approve a plan to assess the security controls.*

- Primary Responsibility:
  - Security Control Assessor.
- Supporting Roles:
  - Authorizing Official or Designated Representative; Chief Information Officer; Senior Information Security Officer; Information System Owner or Common Control Provider; Information Owner/Steward; Information System Security Officer.
- System Development Life Cycle Phase: Development/Acquisition; Implementation.
- Supplemental Guidance: The *security assessment plan provides the objectives for the security control assessment, a* detailed roadmap of how to conduct such an assessment, and assessment procedures. The assessment plan reflects the type of assessment the organization is conducting (e.g., developmental testing and evaluation, independent verification and validation, assessments supporting security authorizations or reauthorizations, audits, continuous monitoring, assessments subsequent to remediation actions).

### Continuous Diagnostics & Mitigation

*TASK 4-1: Develop, review, and approve a plan to assess the security controls.*

- Follow standard NIST guidance (on left)
- Use the Security Assessment Plan Template provided in each NISTIR appendix as you chose
  - Adopt the template as is
  - Customize the template
    - Customize to D/A roles
    - Decide which local checks to implement
    - Focus on controls that match the system's impact level
    - Other.
  - Write an organization specific plan

# *Automating the Security Life Cycle (800-37)*

## RMF Step 4, Task 4-2: Security Control Assessment

### Traditional Approach

TASK 4-2: Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.

- Primary Responsibility:
  - Security Control Assessor.
- Supporting Roles:
  - Information System Owner or Common Control Provider; Information Owner/Steward; Information System Security Officer.
- System Development Life Cycle Phase: Development/Acquisition; Implementation.
- Supplemental Guidance: Security control assessments determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Security control assessments occur as early as practicable in the system development life cycle, preferably during the development phase of the information system.

### Continuous Diagnostics & Mitigation

TASK 4-2: Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.

- Follow standard NIST guidance (on left)
- Use CDM to implement the automated defect checks called for in the security assessment plan.
- Use manual procedure to test controls that either cannot be automated or that the organization choses not to automate.

# *Automating the Security Life Cycle (800-37)*

## RMF Step 4, Task 4-3: Security Assessment Report

### Traditional Approach

TASK 4-3: Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.

- **Primary Responsibility:**
  - Security Control Assessor.
- **Supporting Roles:**
  - Information System Owner or Common Control Provider; Information System Security Officer.
- **System Development Life Cycle Phase:**
  - Development/Acquisition; Implementation.
- **Supplemental Guidance:**

  The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the *security assessment report. The security assessment* report is one of three key documents in the security authorization package developed for authorizing officials. The assessment report includes information from the assessor necessary to determine the effectiveness of the security controls employed within or inherited by the information system based upon the assessor's findings.

### Continuous Diagnostics & Mitigation

TASK 4-3: Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.

- Follow standard NIST guidance (on left)
- Configure the dashboard to show risks by defect check and "system" by including the following in the "system's" report:
  - Objects in the system's authorization boundary
  - Objects/Defect checks related to inherited controls
  - Objects that impose risk on the system from outside the two areas listed above. (Advanced.)
- Set control limits on risk from each relevant defect check to know when risk is within acceptable limits.
- Document levels of risk from automated controls (summary level, generated by the dashboard) and manual testing (detailed level) in the report.

# *Automating the Security Life Cycle (800-37)*

## RMF Step 4, Task 4-4: Remediation Actions

### Traditional Approach

**TASK 4-4: Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.**

- **Primary Responsibility:** Information System Owner or Common Control Provider; Security Control Assessor.
- **Supporting Roles:** Authorizing Official or Designated Representative; Chief Information Officer; Senior Information Security Officer; Information Owner/Steward; Information System Security Officer; Information System Security Engineer; Security Control Assessor.
- **System Development Life Cycle Phase:** Development/Acquisition; Implementation.
- **Supplemental Guidance:** The security assessment report provides visibility into specific weaknesses and deficiencies **in** the security controls employed within or inherited by the information system that could not reasonably be resolved during system development. The findings generated during the security control assessment facilitate a disciplined and structured approach to mitigating risks in accordance with organizational priorities. Information system owners and common control providers, in collaboration with selected organizational officials (e.g., information system security engineer, authorizing official designated representative, chief information officer, senior information security officer, information owner/steward), may decide that certain findings are inconsequential and present no significant risk to the organization.

### Continuous Diagnostics & Mitigation

**TASK 4-4: Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate**.

- Follow standard NIST guidance (on left)
- The organization uses the CDM dashboard to find the **highest risk** problems to remediate first, until risk is acceptable.
- Mitigation is not done by CDM, but by the D/A
- The following are tracked in the CDM dashboard to meet the intent of the POA&M for all controls tested under CDM
  - Prioritized list of *actions/milestones*
  - *When first found.*
  - *(Removed when fixed)*
  - *Progress being made (risk level time series data)*

# *Recap*

- ❑ **Learning Objectives**
- ❑ **Automating the Security Lifecycle**