Role-Based
Risk Management Framework

Process integration for the NIST RMF and NICE Framework

Jeff Monroe
Department of The Interior

Role-Based RMF Goal

Leverage the NIST RMF Process to inform your Information Security Program of workforce resource needs and changes.

NIST Frameworks Overview

1. NIST Risk Management Framework (RMF)
   - Applicable law – *Federal Information Security Modernization Act (FISMA)*
   - Process-centric
2. NIST National Initiative for Cybersecurity Education Framework (NICE)
   - Applicable law - *Federal Cybersecurity Workforce Assessment Act*
   - Supports implementation of *PM-13 Information Security Workforce*
   - Not Process-centric

PM-13 Information Security Workforce

PM-13 Information Security Workforce

- Control: The organization establishes an information security workforce development and improvement program.
- Supplemental Guidance: Information security workforce development and improvement programs include, for example: (i) defining the knowledge and skill levels needed to perform information security duties and tasks; (ii) developing role-based training programs for individuals assigned information security roles and responsibilities; and (iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions. Such workforce programs can also include associated information security career paths to encourage: (i) information security professionals to advance in the field and fill positions with greater responsibility; and (ii) organizations to fill information security-related positions with qualified personnel. Information security workforce development and improvement programs are complementary to organizational security awareness and training programs. Information security workforce development and improvement programs focus on developing and institutionalizing core information security capabilities of selected personnel needed to protect organizational operations, assets, and individuals. Related controls: AT-2, AT-3.

RMF Process – Security Control Taxonomy

NIST 800-53 & 53A

- Security Control Family
  - Security Control
    - Security Control Assessment Objective
      - Determination Statement

NICE Framework Taxonomy

NIST 800-181

- Category: a high-level grouping of security functions
  - Specialty Area: represent an area of concentrated work, or function, within cybersecurity and related work
    - Work Roles: most detailed groupings of cybersecurity and related work
      - Tasks: specific work activities
      - KSA: attributes required to perform tasks

Rhetorical Claims

1. Claim – RMF Determination Statements can be directly correlated to NICE Framework Tasks therefore;
2. Claim – NICE Framework Roles/Tasks/KSAs can be defined and monitored through applicable RMF Program and Information System security controls

Rhetorical Claim #1 + Evidence

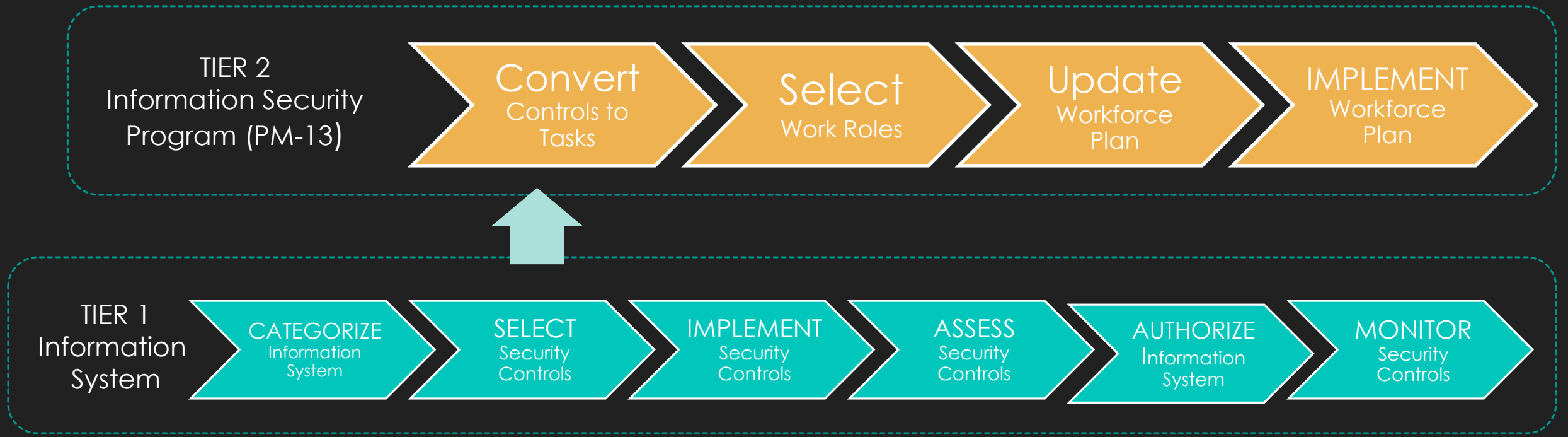
- Claim #1 – RMF Determination Statements can be directly correlated to NICE Framework Tasks therefore;
  - Evidence – examples of RMF *AC-2 Account Management* Determination Statements
    - AC-2(f)[1][a] create information system accounts;
    - AC-2(f)[1][b] enable information system accounts;
    - AC-2(f)[1][c] modify information system accounts;
    - AC-2(f)[1][d] disable information system accounts;
    - AC-2(f)[1][e] remove information system accounts;
  - Evidence – current corresponding NICE Framework Role and Task
    - System Administrator – Manage accounts, network rights, and access to systems and equipment

Rhetorical Claim #2 + Evidence

- Claim #2 – NICE Framework Roles/Tasks/KSAs can be defined and monitored through applicable RMF Program and information system security controls

Applicable Security Controls	Responsible NICE Work Role
CA-6	Authorizing Official
??	System Owner *
CA-5, CA-7, PL-2, PL-2(3), RA-1, RA-2, RA-3	Information System Security Manager *
AC-2, AC-2(1), AC-3, AC-5, AC-6, AC-6(1), AC-6(2), AC-6(5), AC-6(10), AU-1, AU-6, CM-1, CP-1, CP-2, CP-2(1), CP-2(3), CP-2(8), CP-3, CP-4, CP-4(1), IA-1, IA-5(3), IA-5(11), IR-1, IR-8, MP-1, SA-1, SC-1	System Administrator
CA-2, CA-2(1)	Security Control Assessor
Total Controls = 38	**Total Roles = 5**

Role-Based RMF Process Diagram



Role-Based RMF Benefits

1. Process integration w/ the RMF ensures the workforce plan is automagically:
   - Defined
   - Customized
   - Monitored
   - Updated

NICE Framework/Workforce Plan Benefits

1. Workforce Identification, Tracking, & Reporting
2. Qualifications Requirements
3. Human Capital Planning
4. Standardized Development of Position Descriptions
5. Training Requirements and Standards
6. Career Progression
7. CDM Role-Based Dashboard Planning

Recommendations

- Map NIST 800-53A Determination Statements, using a RACI Matrix, to NICE Framework:
  - Tasks
  - KSA's
- Align 800-37 Roles to NICE Framework Roles
  - System Owner (does not exist)
  - ISSM to ISSO
  - Etc.

Questions/Comments?

Jeffrey_Monroe@ios.doi.gov