Risk Based Information Security
Continuous Monitoring (ISCM)

August 2014
Purpose

- Present a universal “Risk Based” approach to ISCM

Approach

- Define Risk Based Approach to ISCM
- Discuss implementation
- Present monitoring techniques

Expected Results

- Attendees will be familiar with Fiscal Service's risk based approach to ISCM
ISCM Approach

- Define ISCM
  - Assessment – Validation of security control effectiveness and compliance based on risk
  - Operational Security – Day to day security monitoring (manual and/or automated)

- Assessment types supporting Ongoing Authorization:
  - Full – Initial assessment required for new systems or major change – all controls
  - Annual – Partial assessment of controls based on POA&M closures, new controls, and control risk
  - Delta (Ad Hoc) – Focused assessment of controls impacted by a significant change – Triggered by a Security Impact Analysis (SIA)
  - IV&V (Independent Verification and Validation) – Independent review of assessment or audit closure evidence
Background

- **Historic Control Selection:**
  - Volatility
  - Closed POA&Ms
  - New Controls
  - Controls not previously assessed within authorization cycle (spread out over 3 years)

- **Risk Based Control Selection:**
  - **Likelihood** – Measure of how often a control may change (volatility) and probability of failure or compromise over time
  - **Impact** – Effect of control failure or non-implementation
  - **Control Risk** = Likelihood X Impact
Establishing a Risk Based approach to ISCM:

- Document tier 3 (system level) risk for each control per system:
  - Determine overall Likelihood
  - Evaluate impact (CIA)
  - Calculate the risk rating

- Derive an assessment frequency based on control risk rating and FIPS 199 Security Categorization
Control Risk Determination

- Determined during System Security Plan (SSP) development and updates
- Approved by System Owner/ISSO
- Input from Enterprise Security Risk Management (ESRM) –
  - Evolving threat landscape
  - Control failures

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Very Low</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
<th>Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>Very Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>High</td>
<td>Very Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Moderate</td>
<td>Very Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>Low</td>
<td>Very Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
</tr>
<tr>
<td>Very Low</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>
ISCM Approach – Assessment

Determining risk on a control by control basis

<table>
<thead>
<tr>
<th>NIST Ref #</th>
<th>FS ID Ref #</th>
<th>Requirements</th>
<th>O-ISCM Activities</th>
<th>Likelihood of Change</th>
<th>Likelihood of Failure or Compromise</th>
<th>Overall Likelihood</th>
<th>Impact</th>
<th>Overall Risk</th>
<th>Assessment Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-1</td>
<td>AC-1_N_00</td>
<td>ACCESS CONTROL POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Fiscal Service personnel (FS)]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</td>
<td>Y</td>
<td>Moderate</td>
<td>Low</td>
<td>Low</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Once Every Five Years</td>
</tr>
</tbody>
</table>
ISCM Approach – Assessment

Defining a frequency based on control risk and FIPS 199

Minimum Control Assessment Frequency Schedule (Control Risk by FIPS 199 Rating)

<table>
<thead>
<tr>
<th>FIPS 199</th>
<th>Very Low</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
<th>Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Once every 4 yrs.</td>
<td>Once every 3 yrs.</td>
<td>Once every 2 yrs.</td>
<td>Annually</td>
<td>Annually</td>
</tr>
<tr>
<td>Moderate</td>
<td>Once every 5 yrs.</td>
<td>Once every 4 yrs.</td>
<td>Once every 3 yrs.</td>
<td>Annually</td>
<td>Annually</td>
</tr>
<tr>
<td>Low</td>
<td>Once every 6 yrs.</td>
<td>Once every 6 yrs.</td>
<td>Once every 4 yrs.</td>
<td>Once every 2 yrs.</td>
<td>Annually</td>
</tr>
</tbody>
</table>
ISCM Approach – Operational

- Day to day security monitoring (manual & automated)
  - Identified during SSP development (RMF Step 2)
  - Recorded and tracked in the SSP
  - Results in an ISSO Checklist

- Continuous Diagnostics and Mitigation (CDM) should be part of Operational ISCM

- Benefits:
  - Provides more consistent & reproducible method of ensuring operational tasks are performed
  - Assists in the retention and transfer of knowledge
  - Supports assessment and audit activities
# ISCM Approach – Operational

## Sample Continuous Monitoring Plan

<table>
<thead>
<tr>
<th>NIST Ref #</th>
<th>FS ID Ref #</th>
<th>Requirements</th>
<th>Control Allocation</th>
<th>Control Implementation</th>
<th>O-ISCM Technique</th>
<th>O-ISCM Evidence</th>
<th>O-ISCM Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-2</td>
<td>AC-2_N_13</td>
<td>j. Reviews accounts for compliance with account management requirements of users annually; privileged users semi-annually (TRE); and</td>
<td>N/A</td>
<td>Implemented</td>
<td>Application accounts are reviewed quarterly following Recert SOP X.</td>
<td>Follow Recert SOP X. Specifically, ISSO or designee runs a report of active accounts (all types), and sends to supervisor to determine (1) account validity and (2) accuracy of permissions based on group assignment. Removals and changes are initiated based on supervisor response.</td>
<td>Quarterly</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PL-2</td>
<td>PL-2_N_10</td>
<td>c. Reviews the security plan for the information system annually or as a result of a significant change (TRE);</td>
<td>N/A</td>
<td>Implemented</td>
<td>The application SSP is reviewed at least annually, but updated as changes occur.</td>
<td>Review and update the SSP as system changes occur, but no less than monthly.</td>
<td>SSP Change Log</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Ongoing Authorization

Fiscal Service systems will receive an initial Authorization to Operate (ATO) that is reviewed on an ongoing basis:

› Full Assessment – Initial ATO
› Annual Assessment – ATO Renewal
› Delta Assessment – Continued ATO
› Operational ISCM – Monitoring in support of ongoing authorization
Incorporating ERM

- **Historic Approach**
  - Risk Determination – Defined at two levels between Tiers 3-2 and Tiers 2-1: Finding Risk and Organizational Risk
  - Prioritization – Determined from Organizational Risk
  - Remediation – Driven historically by Finding Risk, changing to Organizational Risk focus

- **Risk Based Approach**
  - Risk Determination – Includes all 3 Tiers
  - Prioritization – Determined from Aggregate Risk rating
  - Remediation – Driven from prioritization across Fiscal Service
  - Further integration with Enterprise Risk Management
Applying the Tiered approach

A **Finding** Risk level is calculated using the likelihood and impact rating of the finding. A number and word based risk rating are derived from the risk table.

The **Finding Risk** level represents the risk posed to a system, and the business unit the system supports.

**Example:**
High Likelihood X Moderate Impact = Risk rating of 5

This is a Moderate Risk because 5 is within in the Moderate Risk rating range of greater than or equal to 3 and less than 7
Organizational Risk is calculated using the finding risk and the security impact categorization level of the information.

Fiscal Service applied two categorization levels (non-sensitive and CIP) in addition to the three FIPS 199 levels (Low, Moderate, and High).

Organizational Risk represents risk that the finding poses to Fiscal Service and the business unit.

- NS = non-sensitive
- L = Low
- M = Moderate
- H = High
- CIP = Critical Infrastructure Protection

**Example:**
Moderate Finding Risk X CIP Security Categorization = Risk rating of 8
This is a High Organizational Risk because 8 is within the High Risk rating range of greater than or equal to 7 and less than 9.
Putting it all together

- Sequentially defined risk → Moving up the multi-tiered risk triad
- Initial control risk ratings are auto populated for the assessor risk
- Incorporate / apply risk methodology to derive findings risk (Tiers 2-3)
- Determine organizational risk (Tier 1) using the defined methodology
## Vulnerability Assessment - Issue Resolution (FIPS 199 Moderate System)

<table>
<thead>
<tr>
<th>VUL #</th>
<th>Vul Grouping</th>
<th>FS REF#</th>
<th>Vulnerability Description</th>
<th>Scope / Affected Area</th>
<th>Status</th>
<th>Existing Controls</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>AC-1_N_00</td>
<td>Something is wrong and so on and so forth and more ~ ~</td>
<td></td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Assessor Risk (Tier 3)

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk Level</th>
<th>Justification</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk Level</th>
<th>Justification</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
<td>Moderate</td>
<td>Very High</td>
<td>High</td>
<td>Internal controls ~</td>
<td>Moderate</td>
<td></td>
</tr>
</tbody>
</table>

### Finding Risk (Tiers 3 & 2)

### Org Risk (Tier 1)

### Issue Resolution

<table>
<thead>
<tr>
<th>Recommendation(s)</th>
<th>Disposition</th>
<th>Disposition Explanation</th>
<th>Responsible Official</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIX IT</td>
<td>Risk Accepted</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Implementation

- Establish robust change and configuration management, incorporating SIA
- Update SA&A templates
- Train key personnel
- Assign risk to controls and establish assessment and monitoring frequencies
- Transition from traditional assessment cycles
  Adjust frequencies based on policy changes and risk (enterprise or per system basis)
Monitoring

- Leverage existing metrics and reporting mechanisms where possible:
  - FISMA reporting via TFIMS
  - Monthly Consolidated Data Call
  - Cyberscope Data Feeds
  - Fiscal Service Security Risk Management Report

- Establish additional monitoring mechanisms as needed (system or enterprise)
Benefits

- Meets intent and mandate for risk-based ongoing authorization
- Bridges gap between full automation vs. traditional SA&A
- Assessment and monitoring frequencies are based on control risk
- Allows for the aggregation and proactive use of data:
  - Remediation can be prioritized based on defined system and enterprise risk
  - Provides a mechanism for assessing impact and prioritizing incident response
  - Provides data for budgetary purposes (ROI)
Questions
Stacy Cahill
Chief Information Security Officer
Acting Director, Enterprise Information Assurance Division (EIAD)

Ron Hall
Division of Security Services (DSS)
Manager, Fiscal Services Branch
(304) 480-6326
ronald.hall@fiscal.treasury.gov

Michael Merrill
Enterprise Information Assurance Division (EIAD)
Manager, IT Security Oversight and Compliance (ITSOC)
(304) 480-6213
michael.merrill@fiscal.treasury.gov

Jim McLaughlin
Enterprise Information Assurance Division (EIAD)
Manager, Security Policy & Risk Management
(304) 480-6149
jim.mclaughlin@fiscal.treasury.gov

John Hairl
Division of Security Services (DSS)
Manager, Franchise Services Branch
(304) 480-6868
john.hairl@fiscal.treasury.gov