US TREASURY - BUREAU OF THE FISCAL SERVICE

Risk Based Information Security Continuous Monitoring (ISCM)

August 2014

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

Agenda

- 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

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

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

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

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**

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

ISCM Approach – Assessment

- 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

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

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

Individual Control Risk Determination

Likelihood	Level of Impact				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

ISCM Approach – Assessment

Determining risk on a control by control basis

NIST Ref #	FS ID Ref #	Requirements	O-ISCM Activities	Likelihood of Change	Likelihood of Failure or Compromise	Overall Likelihood	Impact	Overall Risk	Assessment Frequency
AC-1	AC-1_N_00	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	Y	Moderate	Low	Low	Very Low	Very Low	Once Every Five Years

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

ISCM Approach – Assessment

Defining a frequency based on control risk and FIPS 199

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

FIPS 199	Control Risk				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
High	Once every 4 yrs.	Once every 3 yrs.	Once every 2 yrs.	Annually	Annually
Moderate	Once every 5 yrs.	Once every 4 yrs.	Once every 3 yrs.	Annually	Annually
Low	Once every 6 yrs.	Once every 6 yrs.	Once every 4 yrs.	Once every 2 yrs.	Annually

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

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

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

ISCM Approach – Operational

Sample Continuous Monitoring Plan

NIST Ref #	FS ID Ref #	Requirements	Control Allocation	CC Provider	Control Status	Control Implementation	O-ISCM Technique	O-ISCM Evidence	O-ISCM Frequency
AC-2	AC-2_N_13	j. Reviews accounts for compliance with account management requirements [of users annually; privileged users semi-annually (TRE)]; and [NOTE: The term "annually" is interpreted in this context by Fiscal Service as "365 days" or possibly 366 days factoring in leap year. For example, if testing was conducted on March 1, 2011, testing must happen again on or before March 1, 2012. (FS)] [NOTE: The term "semi-annually" is interpreted in this context by Fiscal Service as "at least once within each calendar half year (Jan - Jun, Jul - Dec)." (FS)] [NOTE: Privileged user is any user who has access to system control, monitoring, or administration functions (e.g., system administrator, system ISSO, maintainers, system programmers, etc.). (FS)]	SS	N/A	Implemented	Application accounts are reviewed quarterly following Recert SOP X.	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.	Quarterly Recert Statement saved to local share.	Quarterly
PL-2	PL-2_N_10	c. Reviews the security plan for the information system [annually or as a result of a significant change (TRE)]; [NOTE: The term "annually" is interpreted in this context by Fiscal Service as "365 days" or possibly 366 days factoring in leap year. For example, if testing was conducted on March 1, 2011, testing must happen again on or before March 1, 2012. (FS)]	SS	N/A	Implemented	The application SSP is reviewed at least annually, but updated as changes occur.	Review and update the SSP as system changes occur, but no less than monthly.	SSP Change Log	Monthly

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

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

Incorporating ERM

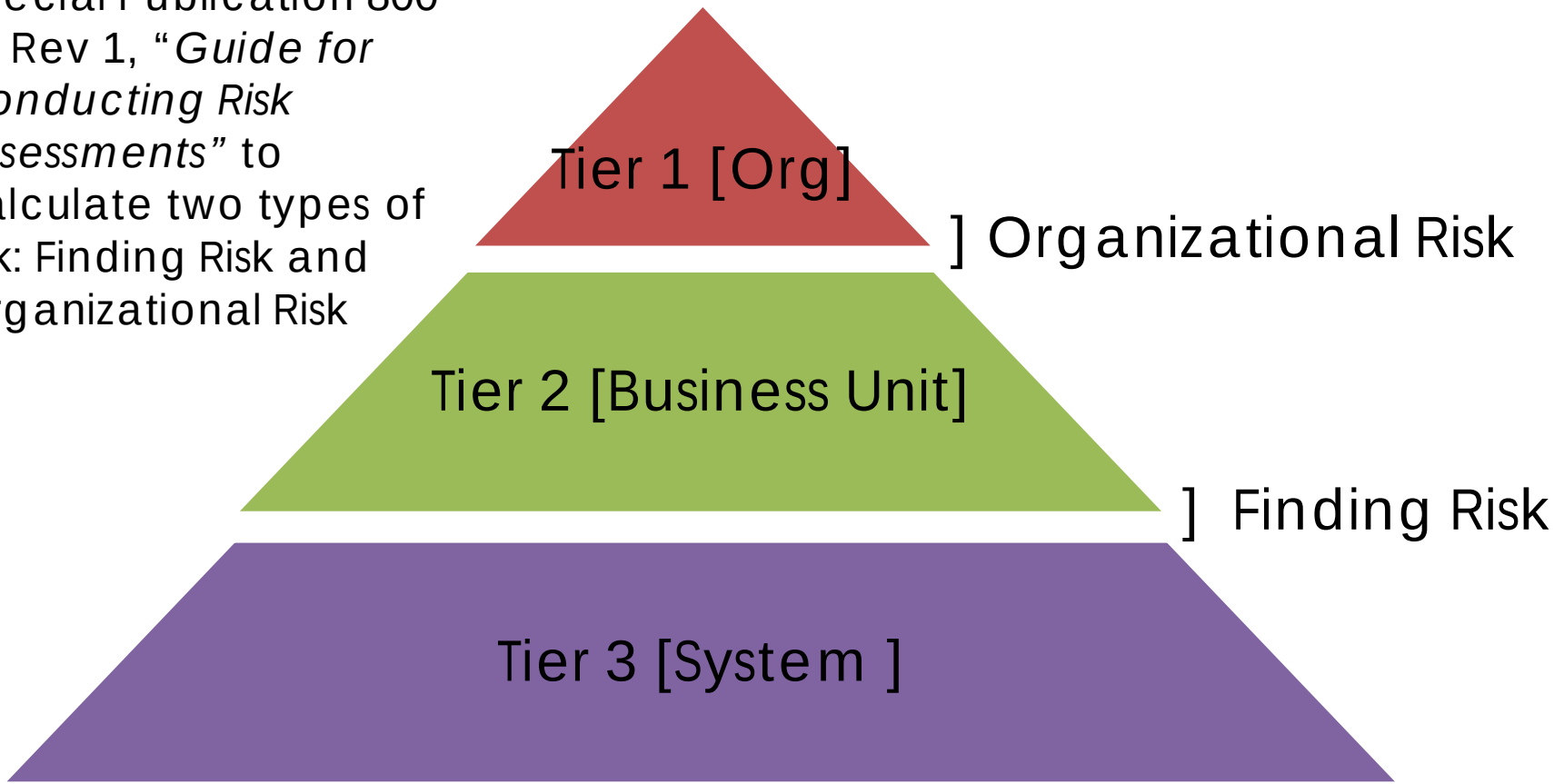
- Historic Approach
  - Risk Determination – Defined at two levels between Tiers 3-2 and Tiers 2-1: Finding Risk and Organizational Risk
  - Prioritization – Determined from Organizational Risk
  - Remediation – Driven historically by Finding Risk, changing to Organizational Risk focus

- 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

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

Applying the Tiered approach

Fiscal Service applies NIST Special Publication 800-30 Rev 1, "*Guide for Conducting Risk Assessments*" to calculate two types of risk: Finding Risk and Organizational Risk

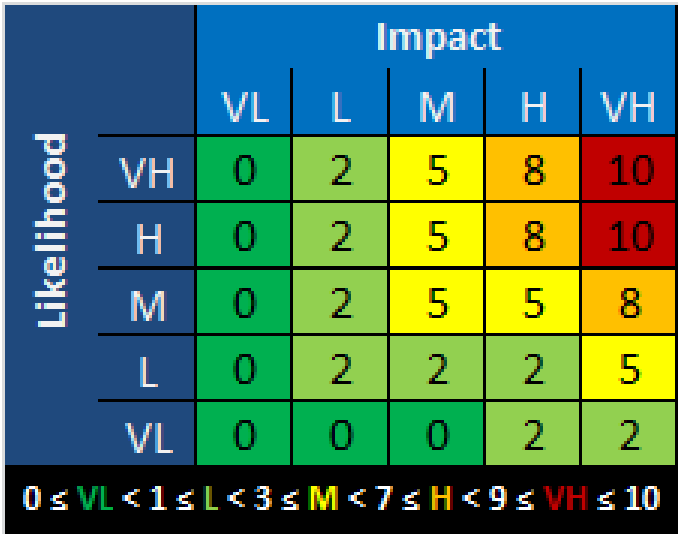


BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

Finding Risk

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.



Likelihood	Impact				
	VL	L	M	H	VH
VH	0	2	5	8	10
H	0	2	5	8	10
M	0	2	5	5	8
L	0	2	2	2	5
VL	0	0	0	2	2

0 ≤ VL < 1 ≤ L < 3 ≤ M < 7 ≤ H < 9 ≤ VH ≤ 10

VL = Very Low
L = Low
M = Moderate
H = High
VH = Very High

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

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

Organizational Risk

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.

Finding Risk Level	Security Categorization				
	NS	L	M	H	CIP
VH	0	2	5	8	10
H	0	2	5	8	10
M	0	2	5	5	8
L	0	2	2	2	5
VL	0	0	0	2	2

0 ≤ VL < 1 ≤ L < 3 ≤ M < 7 ≤ H < 9 ≤ VH ≤ 10

- 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 in the High Risk rating range of greater than or equal to 7 and less than 9.

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

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

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

What it looks like

Vulnerability Assessment - Issue Resolution (FIPS 199 Moderate System)							Control Risk (Tier 3)		
VUL #	Vul Grouping	FS REF#	Vulnerability Description	Scope / Affected Area	Status	Existing Controls	Likelihood	Impact	Risk Level
1	1	AC-1_N_00	Something is wrong and so on and so forth and more ~~		R		High	Very High	Very High

Assessor Risk (Tier 3)				Finding Risk (Tiers 3 & 2)				Org Risk (Tier 1)
Likelihood	Impact	Risk Level	Justification	Likelihood	Impact	Risk Level	Justification	Risk Level
High	Very High	Very High		Moderate	Very High	High	Internal controls ~ ~~~~~~~	Moderate

	Issue Resolution			
Recommendation(s)	Disposition	Disposition Explanation	Responsible Official	Status
FIX IT	Risk Accepted			

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)

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

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)

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

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)

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.

Questions

BUREAU OF THE
Fiscal Service
LEAD. TRANSFORM. DELIVER.

Contact Information

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

BUREAU OF THE Fiscal Service
LEAD. TRANSFORM. DELIVER.