BUREAU OF THE
Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

Security Assessment Finding Risk Reviews

Jim McLaughlin
Ralph Jones
5/16/2018

If you want to drive an expensive sports car as fast as you can do so (safely), should you focus forward at road ahead or backward using rear-view mirror ?

Traditional Audit and Security Assessments: Focus Backward – PAST

Risk Management: Focus Forward – FUTURE, while learning from past

Agenda

- Overview
- **What** is a Finding Risk Review?
- **Why** Do We Do Finding Risk Reviews?
- Finding Risk Review **Process**
- Risk Management **Outcomes**
- Assessment Analysis **(How)**
- Conclusion **(So What – why it matters)**
- Questions

Overview - WHAT

Fiscal Service “Finding Risk Review” process:

- **Review** assessor findings
- **Create** (Fiscal Service declared) values for likelihood, impact, and risk ratings
- No longer making risk-based decisions using the risk ratings assigned by assessors

Overview - WHY

- Assessor declared risk ratings for the **same finding** can differ from one assessment to another:

different assessment = different ratings

- Effective risk management needs same risk rating for same finding.

Overview - HOW

- Assessor findings summarized on Issue Resolution Spreadsheet (IR)

- Risk Management staff **analyze & (normalize)**

  Assessor findings → Finding Risk ratings

  – FR(Likelihood) x FR(Impact) = FR(RISK)

- Finding Risk ratings used to make risk disposition decisions

Overview – SO WHAT

- Better risk management

same finding = same risk rating

$$$

Detailed Overview

- Security assessments require accurate and consistent risk ratings in order to make good authorization decisions.
- Collection and analysis of risk ratings assigned by multiple security control assessors across various system FIPS 199 impact ratings, operating environments, and various other factors, enable “normalized” finding risk ratings.
- Normalized consistent risk ratings are essential for effective continuous monitoring and risk management programs.

What is a Finding Risk Review?

- Finding risk reviews are critical examinations of security assessments to determine:
  - Whether the assessor applied appropriate context in assessing a finding.
  - Whether the risk rating assigned is appropriate – is the rating consistent with precedent for similar findings on similar systems in similar situations?

- Finding risk reviews are conducted by Fiscal Service Policy & Risk Management staff.

Why Do We Do Finding Risk Reviews?

Normalize risk values

- Finding risks should be consistent across assessors and across similar systems in similar environments of operation

Consistently interpret policy

- Policy should be interpreted consistently across various assessors and assessments

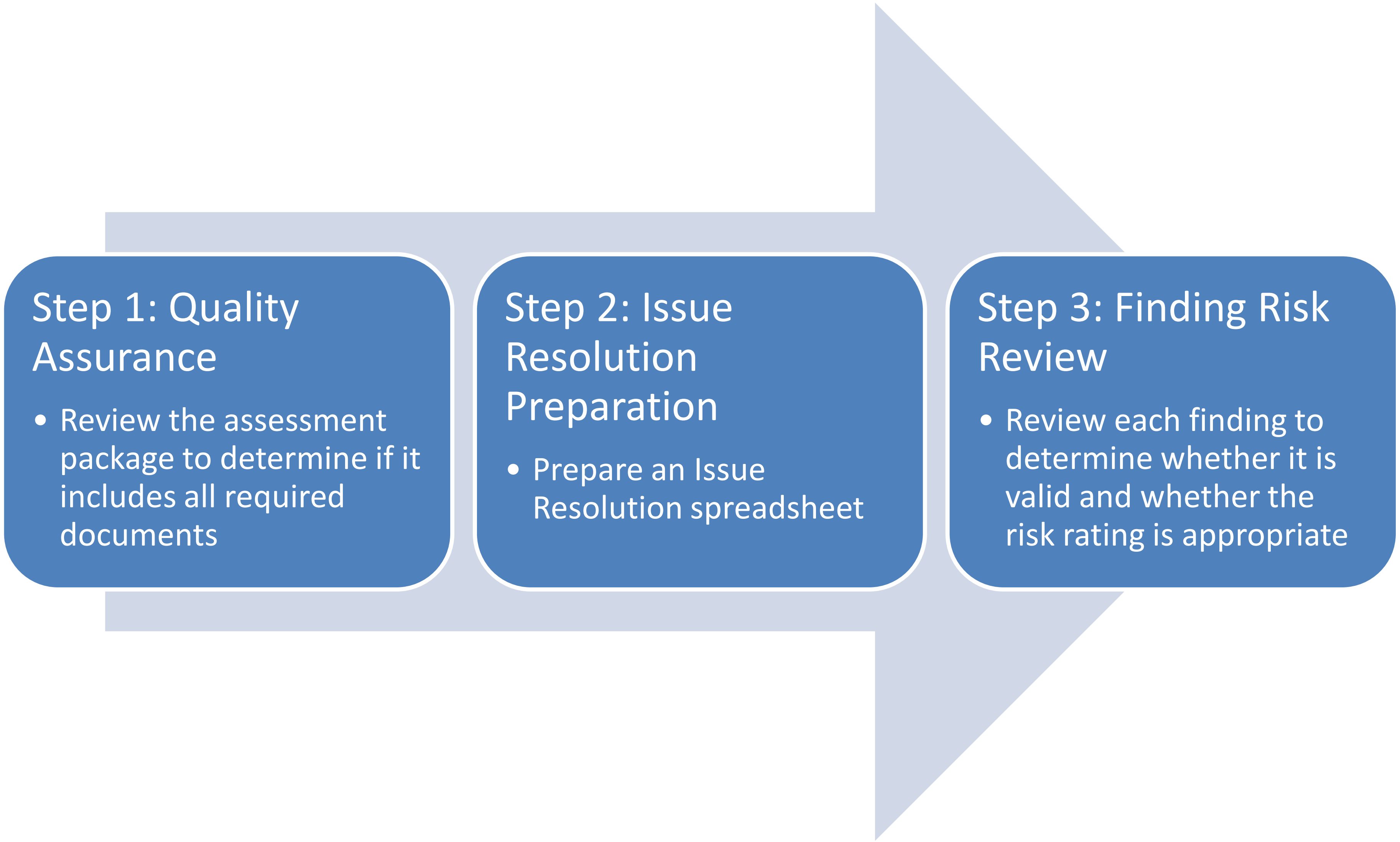
Effectively prioritize risks

- Consistent risk ratings ensure Fiscal Service prioritizes limited resources effectively to address the most significant risks

Improve decision-making

- Precedent analysis allows Fiscal Service decision-makers, including AOs, the ability to make better more consistent (risk-based) authorization decisions

Finding Risk Review Process



Step 1: Quality Assurance

- Review the assessment package to determine if it includes all required documents

Step 2: Issue Resolution Preparation

- Prepare an Issue Resolution spreadsheet

Step 3: Finding Risk Review

- Review each finding to determine whether it is valid and whether the risk rating is appropriate

Step 1: Quality Assurance

- The assessment package is reviewed for completeness
- Some possible issues identified in this step:
  - The assessors did not indicate an impact or likelihood for a finding
  - The assessors did not provide recommendations
  - The Issue Resolution information is provided in a format other than Excel or IR is not filled out

Step 2: Issue Resolution Preparation

- The Issue Resolution spreadsheet contains the findings included in the Security Assessment Report.
- The spreadsheet allows for identification of findings, recommendations, mitigations, risk ratings, and dispositions.
- Some possible issues identified in this step:
  - The findings in the IR do not match the findings in the SAR or in a PDF or other version of the IR
  - Mitigations are missing from all of the findings

Step 3: Finding Risk Review

Analyst reviews each finding to determine:

Validity –

- Is the control in effect for the given system's baseline? Is the control applied correctly to the situation?

Scope –

- Is the finding applied to the correct system/component?

Risk –

- Is the risk rating adjusted to reflect the mitigations in place, the context of the system and extent of control implementation, similar system ratings, etc.?

Risk Management Outcomes

Finding risk reviews result in several key risk management outcomes:

- Consistent finding risk ratings and organizational risk ratings (that take into account the criticality of the system)
- Plan of Action & Milestones (POA&M) prioritization based upon finding and organizational risk ratings
- Risk Acceptance decisions based upon the context of the finding in system security posture

Assessment Analysis

- The policy & risk management program collects data from finding risk reviews in a risk register database.
- The database permits ongoing analysis of precedent, trends, and outliers.

Conclusion

- Finding risk reviews are an integral part of the risk management program
- The reviews enable validity checks on findings and ensure consistency in approach to risk ratings
- Successfully implementing this process requires collaboration throughout the assessment lifecycle
- Ongoing data collected from this process will be used to improve risk management decisions going forward

Questions

Contact Information

Jim McLaughlin
(304) 480-6149
jim.mclaughlin@fiscal.treasury.gov

Ralph Jones
(202) 874-5057
ralph.m.jones@fiscal.treasury.gov