

Developing a Better Finding Tracking Mousetrap

What is a Finding?

A finding is a potential IT security vulnerability that is reported, and that must be addressed in some way. For example, if it was noted during certification and accreditation that passwords do not automatically expire after a certain time period, that observation would be formally reported as a finding.

Note that findings are also called observations, reportable items, action items, and various other names. For consistency, we will refer to all of these as “findings.”

The Need

Quarterly report that must be sent to OMB re: findings. Big Ed creates the report; FSA validates report by system. There will soon be a standardized web-based data entry form for generating this report.

The Solution

We propose creating a comprehensive database that contains all findings, from all sources. Such a database not only will this ensure one centralized location for all findings, but also will provide robust reporting capabilities. For example, one could generate a report on all open findings, a report listing only “nonconcur” findings, a report listing all findings for one particular system—the types of reports are essentially limited only by the data fields we include in the database.

The next section lists the data fields we propose to include in the finding database.

Tracking System for Findings: Data Categories to Include in the Database

System

Priority

High

Medium

Low

Finding ID (this is a unique identifying number)

Recurring?

Yes

No

Tracking System for Findings: Data Categories to Include

Document Number

Finding Description

Recommended Action

CAP

SP Reviewed and Provided Comments

Target Closure Date

Regression Test Item

Yes

No

Actual Closure Date

Status

On track

CAP implemented

CAP validated

Finding closed

Finding Originator:

IG Observation

IG Scan

GAO

Ed CIO

FSA Assessor

Type of Review:

Risk Assessment

Precert Review

C&A

Self-Assessment

Audit

Security Control Area

Management

Operational

Technical

NIST Control Area

Risk Management

Tracking System for Findings: Data Categories to Include

Review of Security Controls
Life Cycle
Authorize Processing (C&A)
System Security Plan
Personnel Security
Physical Security
Production I/O Controls
Contingency Planning
HW/SW Maintenance
Data Integrity
Documentation
Awareness/Training
Incident Response
Identification/Authentication
Logical Access Controls
Audit Trails

Resources Required

High
Medium
Low

Date Finding Reported

Validated

Yes
No