Automated Security Self-Assessment Evaluation Tool (ASSET) Training
Administration

• Target Audience
  – Individuals who have self-assessment data collection responsibilities

• Length of training session
  – 9:00 - 12:30  ASSET System
  – 12:30 - 1:30  Lunch
  – 1:30 - 5:00  ASSET Manager
ASSET System Objectives

• Upon completion of today’s training, you will be able to describe:
  – The purpose of ASSET System
  – ASSET System roles and responsibilities
  – How to enter data into ASSET System
  – How to import assessments into ASSET System
  – How to export assessments from ASSET System
Morning Agenda

• Introduction to ASSET System
• Assessment Process
• ASSET Description
• ASSET System Installation
• Information Security Considerations
• ASSET System Demonstration
Introduction to ASSET System

• Upon completion of this module, you will be able to describe:
  – ASSET’s role in the assessment process
  – Roles and responsibilities of key assessment individuals
  – The main components of ASSET
IT Security Self-Assessment

Background

• Federal IT Security Assessment Framework
• Government Information Security Reform Act
• NIST Special Publication 800-26, “Self-Assessment Guide for IT Systems”
Federal IT Security Assessment Framework

- Five levels of IT security program effectiveness
- Each level contains criteria to determine whether the level is adequately implemented
- The degree of sensitivity of information must first be determined
- The asset owner determines whether the measurement criteria are being met
Framework Benefits

• Identifies a standard way of performing self assessments
• Provides flexibility in assessments based on the size and complexity of the asset
• Built on collaboration among the Federal CIO Council, OMB, GAO, NIST, the Congress, and Industry
Security Self-Assessment Guide for IT Systems

- Introduction
- Questionnaire structure
Self-Assessment Guide

Introduction

• Questions directed at the system
• Specific control objectives that a system can be measured against
• Blending requirements and guidance from GAO’s FISCAM and NIST documents
Questionnaire Structure

Cover Sheet
- Control of completed questionnaire
- System identification
- Assessor information
- Criticality of system

Questions
- Critical elements
- Subordinate elements
The purpose of ASSET is to assist managers in gathering system data and creating reports in support of NIST Special Publication 800-26 IT security self-assessment questionnaire.
Assessment Process
Assessment

The entire process of collecting and analyzing system data
Assessment Process Steps

Data Collection

– The process of gathering and entering system data
Assessment Process Steps

Reporting
– Creating aggregate data so that it can be analyzed
Assessment Process Steps

Analysis

– The process of understanding, evaluating, and making judgments upon a set of system data
ASSET Role

• Asset facilitates data collection and reporting and thus supports assessment process
Roles and Responsibilities 1 of 6

Manager

Assessor

Information Flow

Reporter

Subject Matter Expert
Roles and Responsibilities 2 of 6

Manager
  – Individual(s) with the responsibility for the assessment
  – Responsible for analysis of the results
Roles and Responsibilities 3 of 6

Reporter

- Must understand deployment, installation, and execution of ASSET
- Responsible for importing multiple system data into ASSET
- Ensures that all questions are answered for all systems
- Aggregates results from all systems within an agency or enterprise
- Generates reports
Roles and Responsibilities 4 of 6

Primary Assessor

– Ensures that all questions are answered for each system under a assessor’s review
– Interacts with the SME or secondary assessor to gather system information
– Responsible for conferring with SME(s) for clarification where necessary
– Enters individual system data into ASSET
Secondary Assessor

- Interacts with the SME to gather system information
- May be assigned responsibility for conferring with SME(s) for clarification where necessary
- May be listed as person who answered the question, if in fact, they did
Roles and Responsibilities 6 of 6

Subject Matter Expert

- Knowledgeable about the system being assessed
- Provides specific responses to assessment questions
- Interacts with the Assessor on an as-needed basis
- Will be listed as secondary assessor for questions they specifically answered
A typical assessment will have multiple ‘Assessors’ and one ‘Reporter’
ASSET Introduction Summary

• Based on existing requirements
• Designed to automate data collection and reporting requirements
• Managers, reporters, and assessors have specific roles and responsibilities
ASSET Description
ASSET is comprised of two separate host-based applications.
ASSET – Manager

Individual system data

ASSET – Manager

Unique answers
System types
Before assessment begins

Aggregated system reports
After assessment
ASSET – System

Individual system information
Common answer set

ASSET – System

Individual system reports
System data
After system assessment
ASSET System

• Provides for data entry and storage of individual system data
• Generates single system summary reports providing immediate picture of single system assessment results
• Reports are intended for the user who completes the questionnaire
ASSET System

- Reports can be exported to any popular spreadsheet or charting program
- Reports
  - Summary of topic areas by levels of effectiveness
  - List on N/A questions
  - List of risk-based decisions
  - System summary
ASSET Manager

- Aggregates data from multiple systems so that organization-wide reports can be developed
- Tracks all system operators and SMEs who provide answers to ASSET questions
ASSET Manager

• Intended to generate reports (exportable to any spreadsheet application) that are interpreted by the managers who request an assessment

• Reports
  – Summary of all systems
  – Summary of system types
  – Summary by system sensitivities
  – Summary by organization
ASSET Scope

- It assists in gathering data and reporting results for IT systems.
- It is a stand-alone java-based software application
- It is the first of a number of modules that will assist IT security managers in providing for effective security
ASSET Limitations

• It does not
  – Establish new security requirements
  – Analyze report results
  – Assess system or program risk
• It is not web-based (client:server)
• Users are responsible for security of data (host-based security)
ASSET Considerations

- Implementation of an assessment
- Other people answering questions
- Delayed answers
- Pre-answered questions
Summary

• The main components of ASSET are ASSET System and ASSET Manager
• ASSET System is used to record data on individual systems
• ASSET Manager aggregates reports on various systems to provide an organizational view.
Information Security Considerations
Data Sensitivity

• Organization should determine report and data sensitivity.
• Organizations are responsible for data protection.
• ASSET does NOT provide for any security of data, such as encryption, while the data is stored.
Data Sensitivity

- Security is not provided for data transmitted between data assessor and reporter.
File Back-up Considerations

- Data collection efforts represent a substantial expenditure of labor.
  - ASSET saves the current file on specified intervals but does not provide automated back up for data.
  - Organizations should determine and implement an appropriate back up strategy.
Access Controls

- Access controls are provided by operating system log in requirements
- New ASSET user accounts are created when ASSET is installed
  - Log in consists of user name and e-mail address
  - Log in is case sensitive
- No password protection is provided for accessing application or data
MSDE

• The Microsoft Data Engine has known vulnerabilities that are mitigated during installation
• During installation, install the current Service Pack
• Change the default password
• If appropriate, disable MSDE network communications
Summary

• ASSET supports IT security analysis requirements
• ASSET System and ASSET Manager work together to assist an organization in collecting and reporting IT security self-assessment data
• ASSET considerations
• ASSET and information security
ASSET System Demonstration
Objective

• Upon completion of this demonstration, you will be able to describe
  – The ASSET installation process
  – ASSET System data entry
  – Saving and exporting ASSET System files
Installation

• Minimum system requirements
• Installation of ASSET System
• Installation of JRE
• Disabling MSDE Network Communications
Tool Installation
Minimum System Requirements

• Hardware
  – Pentium II – 266 MHz processor

• Operating Systems
  – Designed to initially operate on Windows 2000 Professional operating system
  – Future testing will qualify ASSET for NT and XP operating systems

• Memory Requirements
  – 120 MB free space
ASSET Installation Files

• CD
  – Contains all pertinent ASSET System and ASSET Manager files
  – User Manual and Help files
  – NIST Special Pub 800-26

• Web site
  – All software and documentation can be downloaded from
    http://csrc.nist.gov/asset/
ASSET Installation

• Installation wizard –
  – Guides the user through installation process
  – Follows Windows conventions
Begin Installation from CD

Double click on setup.exe
Installation Wizard

Click **Next** to continue
License Agreement

Please read the license, then click Yes to accept the license terms.
Installation Options

Make your selection, then click Next
Setup Status

This window provides a visual indicator of installation progress
JRE Installation Wizard

The JRE Installation window appears

Click **Next** to continue
License Agreement

Please read the license and click Yes to accept its terms.
JRE Destination Location

Click **Next** to accept the default location for the files.
Select Default JRE Browser

Select the appropriate browser supported by your system
Then click Next
Change ASSET DB Password

Change the default password.  Click here
Then
Click here
Password Confirmation Box

Depending on your installation, you will see one or both of these boxes.

Click on OK to continue.
ASSET Installation Completion

- Click **Finish** to close Wizard

- Continue with Service Pack installation
Service Pack Update

Install the Service Pack Update
Disabling MSDE Network Communications

- Disable to eliminate network-based vulnerabilities
- Process
  - Follow instructions in ASSET User Manual Section 3.2.5
Installation - Summary

• ASSET can be installed from the CD or using downloaded files from the NIST website

• As an assessor, you should follow installation for ASSET System
Using ASSET System
Objectives

• Upon completion of this demonstration, you will be able to explain how to:
  – Create a new assessment
  – Open an existing assessment
  – Save assessments to file and database
  – Export assessments
  – Print assessment reports
Start ASSET System

- Double click on shortcut on desktop
Log In

- Enter name and email address (name is case sensitive)
- By logging in when starting a new assessment, you are identified as the primary assessor
- Click **Continue** to log in
Command Window Appears

- Command window appears
- Do not close this window
- Closing the window will force ASSET to quit
- Minimize it, if you want
Main ASSET Window Opens

Maximize the window to full screen
Create New Assessment

- Select File, New Assessment
- Or use Ctrl + N
- Result: Main window opens
- Maximize the main window
Main Window Layout
Purpose of Tabs

<table>
<thead>
<tr>
<th>Assessment Identification</th>
<th>Identifies assessors and assessment objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Identification</td>
<td>Entry fields for identifying system information</td>
</tr>
<tr>
<td>Policy</td>
<td>Allows you to indicate all the control objectives for which you have established policies</td>
</tr>
<tr>
<td>Assessment Questions</td>
<td>Collects all the responses to the self-assessment questions</td>
</tr>
<tr>
<td>Summary</td>
<td>Displays status of current assessment and question response levels</td>
</tr>
</tbody>
</table>
Assessment Identification Tab
System Identification Tab
System ID Tab

**System Identification**

- **System Name**: Test Assessment System 1
- **System Number**: AN/TAB-1
- **System Type**: Other
- **Agency/Division/Group**: Tester Lab
- **Assessment Start Date**: Fri Jun 14 12:13:56 EDT 2002

**System Criticality**

- **Confidentiality**: High
- **Integrity**: High
- **Availability**: High

**System** | **Boundary Controls Effective?** | **Planned Action if Not**
--- | --- | ---

**Buttons:**
- **Add System**
- **Help**

**Note:** All fields marked with an * above are required
## Policy Tab

### Policy Definition:

<table>
<thead>
<tr>
<th>Number</th>
<th>Control Objective</th>
<th>Policy Defined?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>Risk Management</td>
<td></td>
</tr>
<tr>
<td>2.0.0</td>
<td>Review of Security Controls</td>
<td></td>
</tr>
<tr>
<td>3.0.0</td>
<td>Life Cycle</td>
<td></td>
</tr>
<tr>
<td>4.0.0</td>
<td>Authorize Processing (Certification &amp; Accreditation)</td>
<td></td>
</tr>
<tr>
<td>5.0.0</td>
<td>System Security Plan</td>
<td></td>
</tr>
<tr>
<td>6.0.0</td>
<td>Personnel Security</td>
<td></td>
</tr>
<tr>
<td>7.0.0</td>
<td>Physical and Environmental Protection</td>
<td></td>
</tr>
<tr>
<td>8.0.0</td>
<td>Production, Input/Output Controls</td>
<td></td>
</tr>
<tr>
<td>9.0.0</td>
<td>Contingency Planning</td>
<td></td>
</tr>
<tr>
<td>10.0.0</td>
<td>Hardware and System Software Maintenance</td>
<td></td>
</tr>
<tr>
<td>11.0.0</td>
<td>Data Integrity</td>
<td></td>
</tr>
<tr>
<td>12.0.0</td>
<td>Documentation</td>
<td></td>
</tr>
<tr>
<td>13.0.0</td>
<td>Security Awareness, Training, and Education</td>
<td></td>
</tr>
<tr>
<td>14.0.0</td>
<td>Incident Response Capability</td>
<td></td>
</tr>
<tr>
<td>15.0.0</td>
<td>Identification and Authentication</td>
<td></td>
</tr>
<tr>
<td>16.0.0</td>
<td>Logical Access Controls</td>
<td></td>
</tr>
<tr>
<td>17.0.0</td>
<td>Audit Trails</td>
<td></td>
</tr>
</tbody>
</table>
Assessment Questions Tab

<table>
<thead>
<tr>
<th>Question: 1.1.1</th>
<th>Management Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the current system configuration documented, including links to other systems?</td>
<td>Risk management</td>
</tr>
<tr>
<td></td>
<td>Critical Element:</td>
</tr>
<tr>
<td></td>
<td>1.1.0 Is risk periodically assessed?</td>
</tr>
</tbody>
</table>

**Indicate Your Responses:**
- [ ] Policy
- [ ] Procedures
- [ ] Implemented
- [ ] Tested
- [ ] Integrated
- [ ] Question not applicable

**Risk Based Decision Made to Increase/Decrease/Omit Security Control?**
- [ ] Yes

**Comments:**

**Answered By:** gail brown

**Question Complete?**
- [ ]

**Assign to alternate:**
- gail brown

**Back** | **Clear** | **Help** | **Next**
Assessment Map

- Located in left pane
- Maximize screen, then drag frame divider to the right
- Use the map to navigate through the assessment
Save Assessment to Database

To Save the assessment, select:

• File
• Save Assessment
• Save Assessment to Database.

Result: System message appears

Assessment saved at: Mon Jun 17 10:29:53 EDT 2002
Save Assessment to File

To Save the assessment, select:

• File
• Save Assessment
• Save Assessment to File.

Result: Save window appears
Summary Tab

Provides a summarized view of answers and progress

Current Progress

Critical Element

Response Table

Save

Export
Export Assessment

- **Purpose:** To create a file that can be transferred to the Reporter
- **An export can be made of a single or multiple files**
- **From the Summary tab, click:**

![Export Assessment]

- **Result:** Save As window opens
Export Assessment

- Select location for file
- Give export file a name
- Include file extension
- Select Save
Alternate Export Assessment

- Select **File**, Open assessment from data base
- Select files to be exported
- On Assessment Window, Select **Export**
Alternate Export Assessment

• Select location for export
• Name the file
• Select Save

You’ll see:
Import an Assessment

• Select Open Assessment, Import assessment from file

• Select location and file to be imported
Import an Assessment cont.

- Click **OK**

- Confirmation box appears
- Select **Yes** to continue
Reports

• Reports can only be created on ONE active system at a time
• Four types of reports
  – Summary of topic areas by levels of effectiveness
  – List of non-applicable questions
  – List of risk based decisions
  – System Summary
Create Reports

• Select Tools, Reporting
Select a System

![Select a System Interface](image)
Select an Assessment

• Highlight an assessment by clicking on it

• Select Continue
Selected System Info Appears

- Information from System Identification tab is displayed
Select the Desired Report

- The selected report will appear in the Tabular Results
### Tabular Output

**Report:** Summary of topic areas by level of effectiveness  
**System Name:** Test Assessment System 1  
**System Number:** AN/TAS-1  
**Primary Assessor:** gail brown  
**Today's Date:** Mon Jun 17 14:21:43 EDT 2002  

<table>
<thead>
<tr>
<th>Topic #</th>
<th>Topic Area</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>Risk Management</td>
<td>Policy</td>
</tr>
<tr>
<td>2.0.0</td>
<td>Review of Security Controls</td>
<td>Policy</td>
</tr>
<tr>
<td>3.0.0</td>
<td>Life Cycle</td>
<td>Policy</td>
</tr>
<tr>
<td>4.0.0</td>
<td>Authorize Processing (Certification &amp; Accreditation)</td>
<td>Policy</td>
</tr>
<tr>
<td>5.0.0</td>
<td>System Security Plan</td>
<td>Policy</td>
</tr>
<tr>
<td>6.0.0</td>
<td>Personnel Security</td>
<td>Policy</td>
</tr>
<tr>
<td>7.0.0</td>
<td>Physical and Environmental Protection</td>
<td>Policy</td>
</tr>
<tr>
<td>8.0.0</td>
<td>Production, Input/Output Controls</td>
<td>Policy</td>
</tr>
<tr>
<td>9.0.0</td>
<td>Contingency Planning</td>
<td>Policy</td>
</tr>
<tr>
<td>10.0.0</td>
<td>Hardware and System Software Maintenance</td>
<td>None</td>
</tr>
<tr>
<td>11.0.0</td>
<td>Data Integrity</td>
<td>None</td>
</tr>
<tr>
<td>12.0.0</td>
<td>Documentation</td>
<td>None</td>
</tr>
<tr>
<td>13.0.0</td>
<td>Security Awareness, Training, and Education</td>
<td>None</td>
</tr>
<tr>
<td>14.0.0</td>
<td>Incident Response Capability</td>
<td>None</td>
</tr>
<tr>
<td>15.0.0</td>
<td>Identification and Authentication</td>
<td>None</td>
</tr>
<tr>
<td>16.0.0</td>
<td>Logical Access Controls</td>
<td>None</td>
</tr>
<tr>
<td>17.0.0</td>
<td>Audit Trails</td>
<td>None</td>
</tr>
</tbody>
</table>

**Confidentiality:** High  
**Integrity:** High  
**Availability:** High  
**Location:** Tester Lab  
**Totals:** 17 records returned
Print Reports

- Reports are exported to another application (word processor, spreadsheet) to be printed
- Reports can not be printed directly from ASSET System
Export a Report cont.

- Click on the floppy disk icon in the ASSET Reporting window
- Select location to save file and name the file and add file extension
- Select Save
- Export confirmation window appears
Print a Report

• Open the exported file in the appropriate software application.

• Print
Wrap Up

End of Demo

Any Questions??????
Summary

• As a result of this morning’s training, you should now be able to describe:
  – The purpose of ASSET System
  – ASSET System roles and responsibilities
  – How to enter data into ASSET System
  – How to save assessments
  – How to import assessments into ASSET System
  – How to export assessments from ASSET System

• All processes demonstrated this morning can be found in the User Manual
Critique

Please take a minute to fill out the course critique

Thanks!
After Lunch

ASSET Manager Training