

Automated Security Self-Evaluation Tool (ASSET) Overview

March 27, 2002

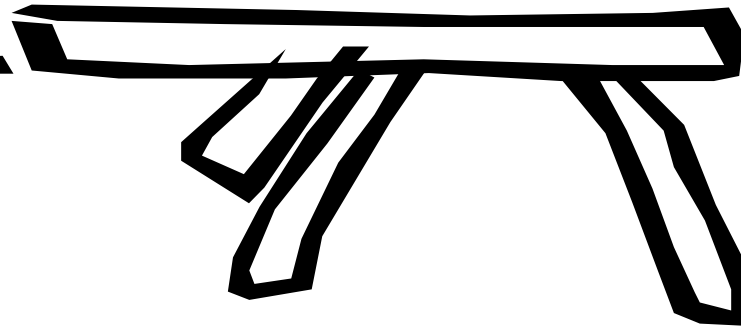
NIST
**National Institute of
Standards and Technology**
Technology Administration
U.S. Department of Commerce

Introduction

- Upon completion of this presentation, you will understand:
 - The history of and future plans for ASSET
 - The purpose of ASSET
 - The capabilities of ASSET
 - Information security considerations of ASSET

Agenda

- Background
- Assessment Process
- ASSET Description
- Installation and Administration
- ASSET Demonstration
- Information Security Considerations



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”
 - <http://csrc.nist.gov>

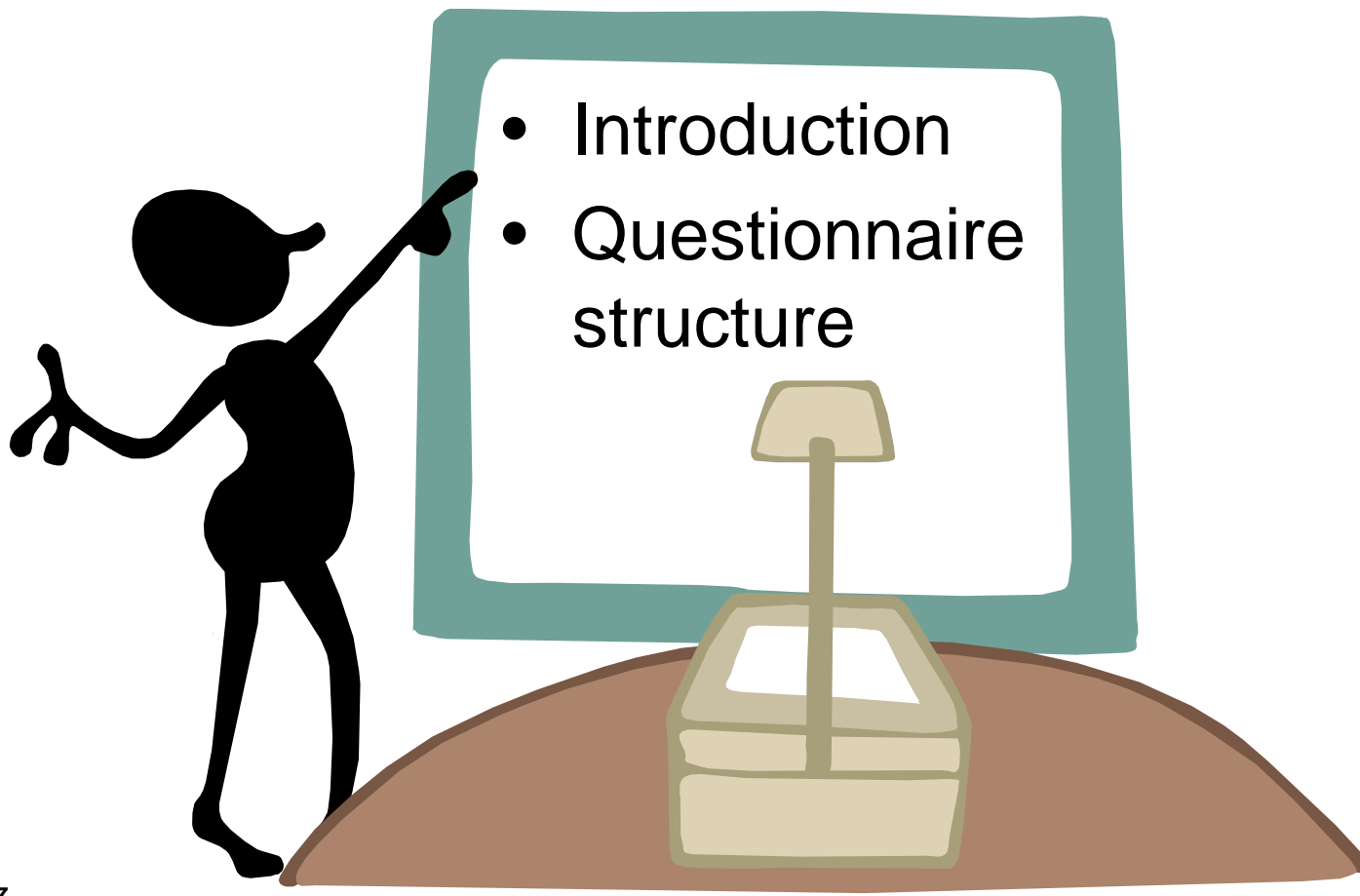
Federal IT Security Assessment Framework

- 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



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 information

Questions

- Critical elements
- Subordinate elements



ASSET - Purpose

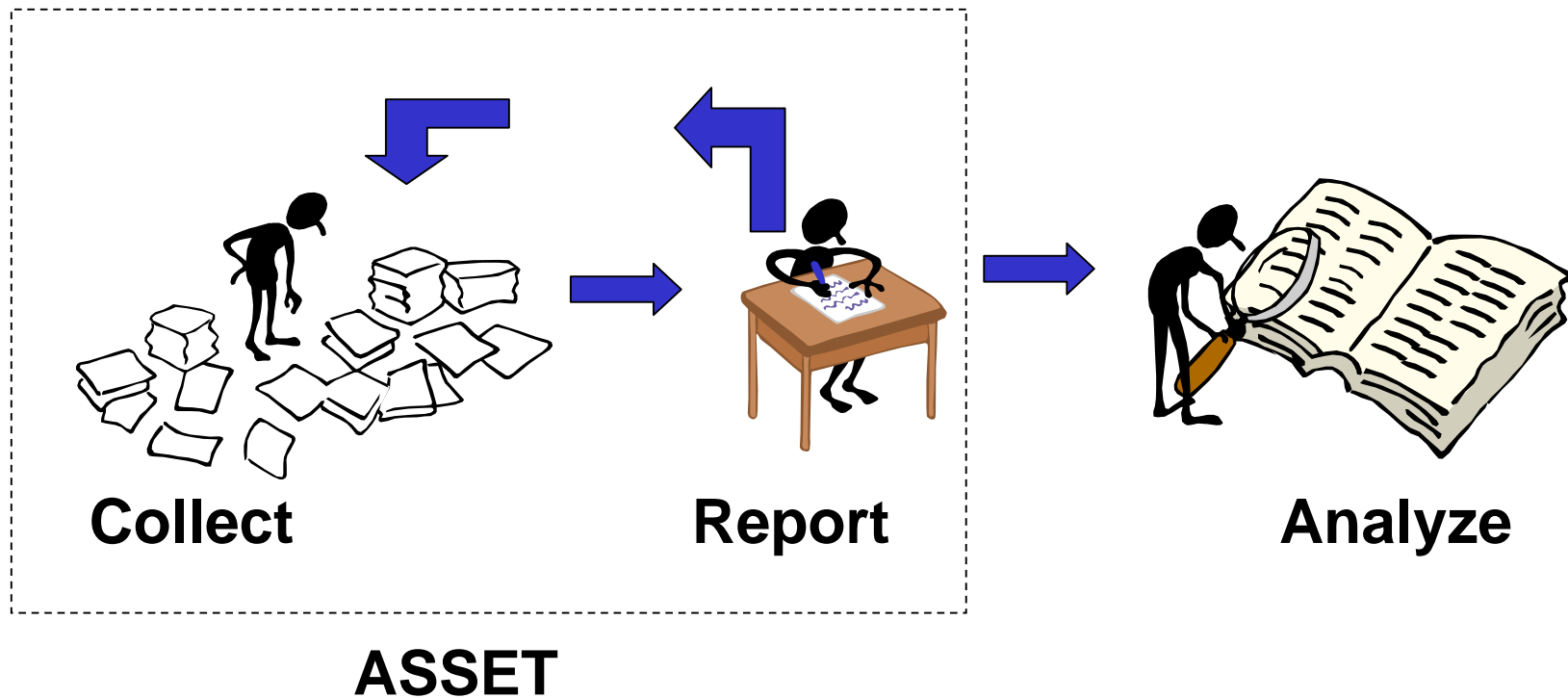


The purpose of ASSET is to assist managers in gathering system data and creating reports in support of NIST Special Publication 800-26 IT security self-assessment questionnaire.

Assessment Process

Assessment

The entire process of collecting and analyzing system data



Assessment Process Steps

Data Collection

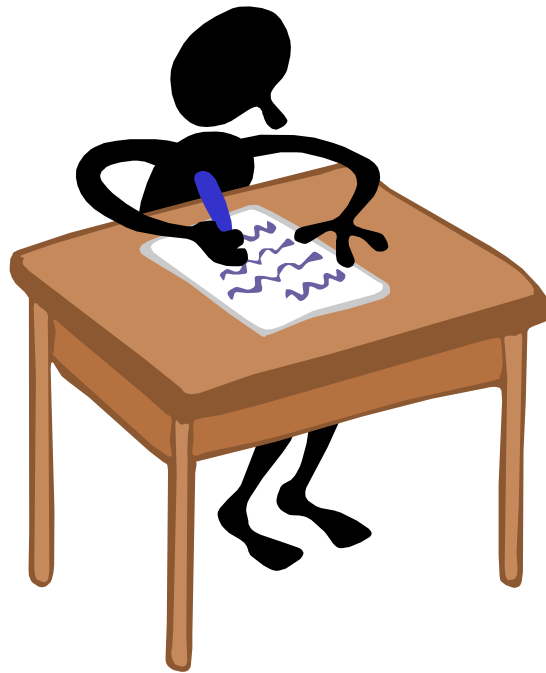
- The process of gathering and entering system data



Assessment Process Steps

Reporting

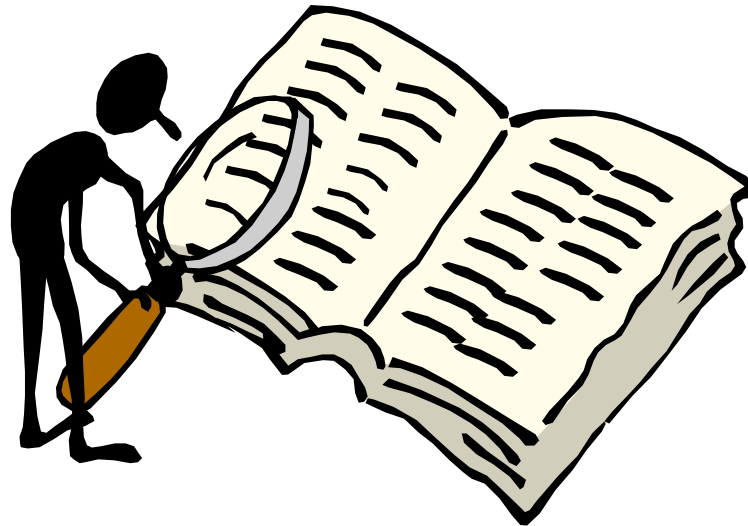
- Creating aggregate data so that it can be analyzed



Assessment Process Steps

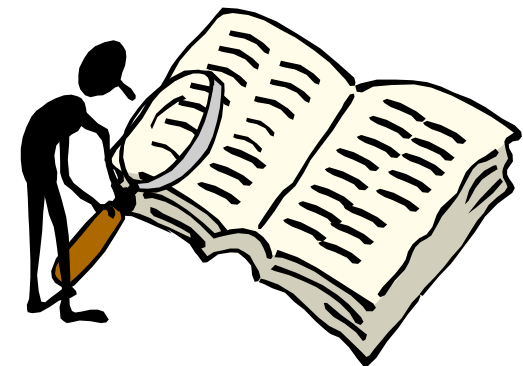
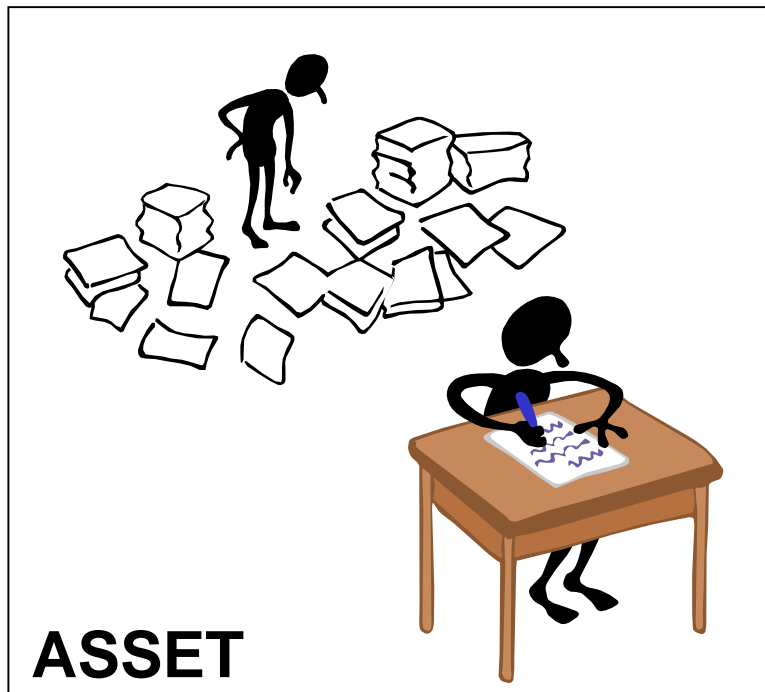
Analysis

- The process of understanding, evaluating, and making judgments upon a set of system data

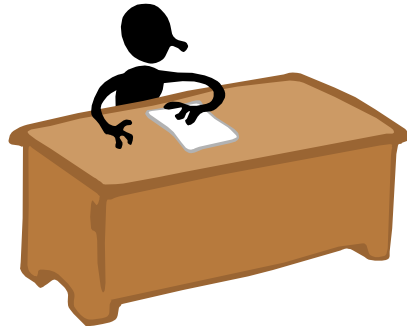


ASSET Role

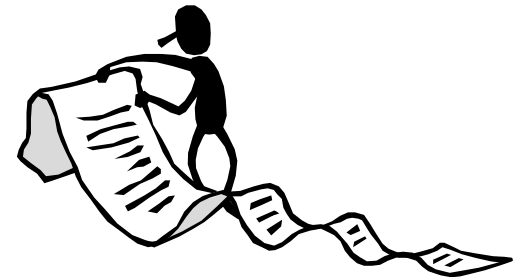
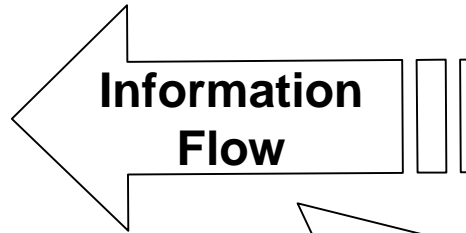
- Asset facilitates data collection and reporting and thus supports assessment process



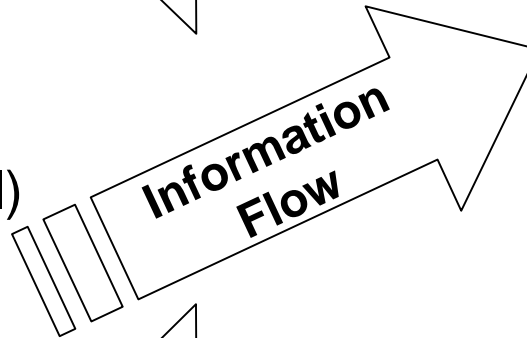
Roles and Responsibilities 1 of 5



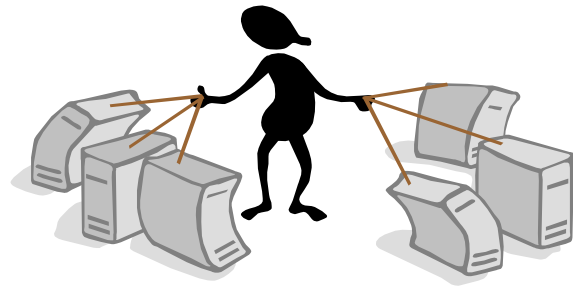
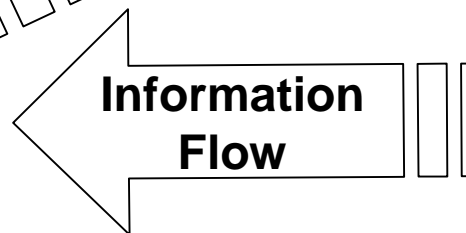
Manager
(CIO / Program Official)



Reporter



Collector



**Subject Matter Expert
(SME)**

Roles and Responsibilities 2 of 5

Manager

- Individual(s) with the responsibility for the assessment
- Responsible for analysis of the results



Roles and Responsibilities 3 of 5

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 5

Collector

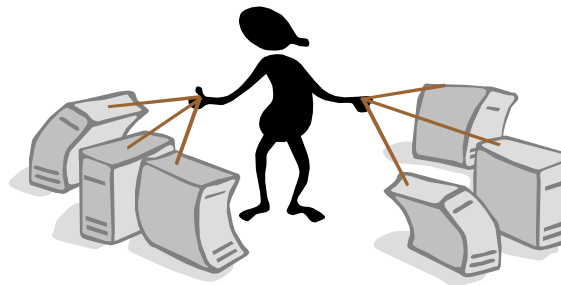
- Ensures that all questions are answered for each system under a collector's review
- Interacts with the SME to gather system information
- Responsible for conferring with SME(s) for clarification where necessary
- Enters individual system data into ASSET



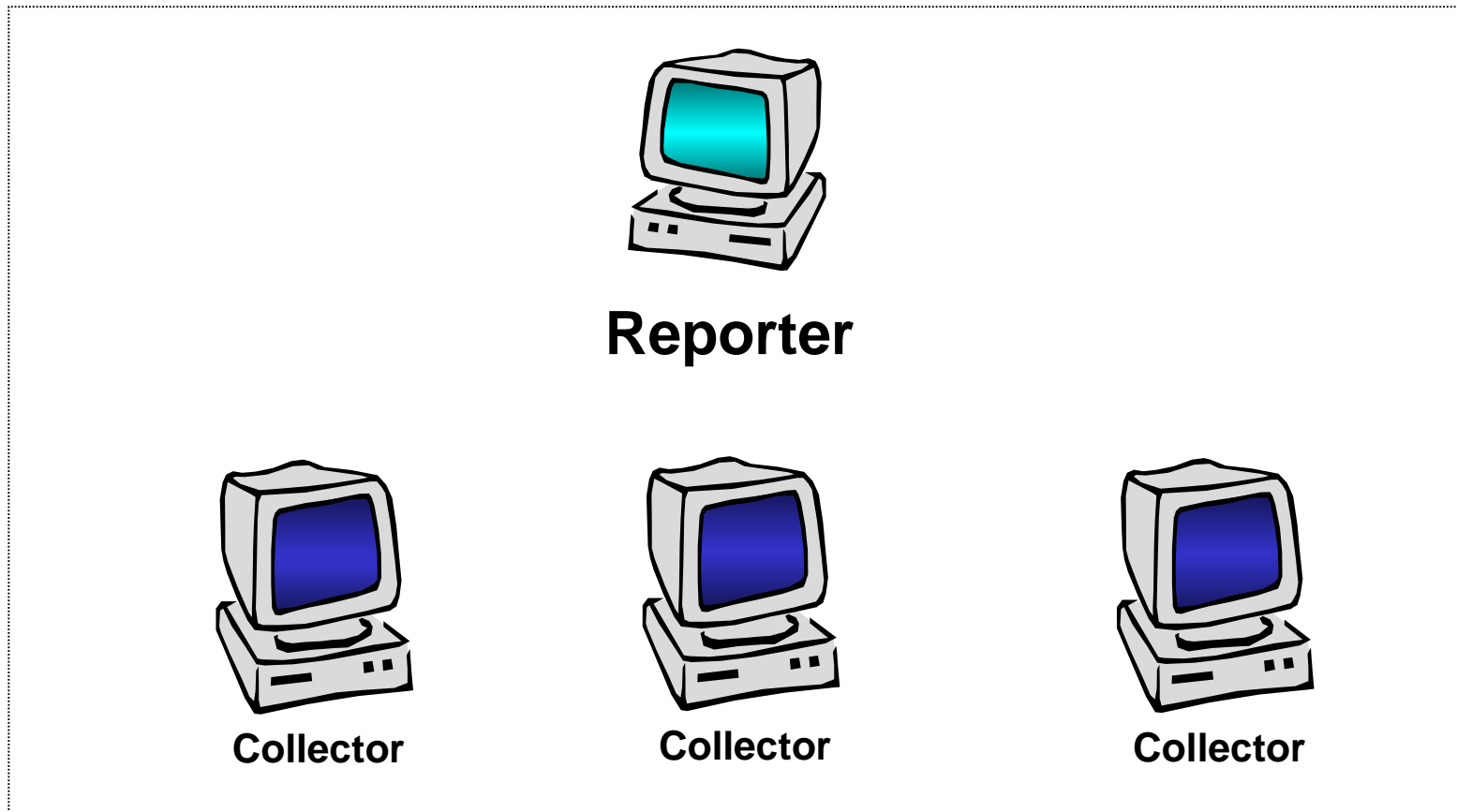
Roles and Responsibilities 5 of 5

Subject Matter Expert

- Knowledgeable about the system or topic areas (i.e. physical security) being assessed
- Provides specific responses to assessment questions
- Interacts with the Collector on an as-needed basis



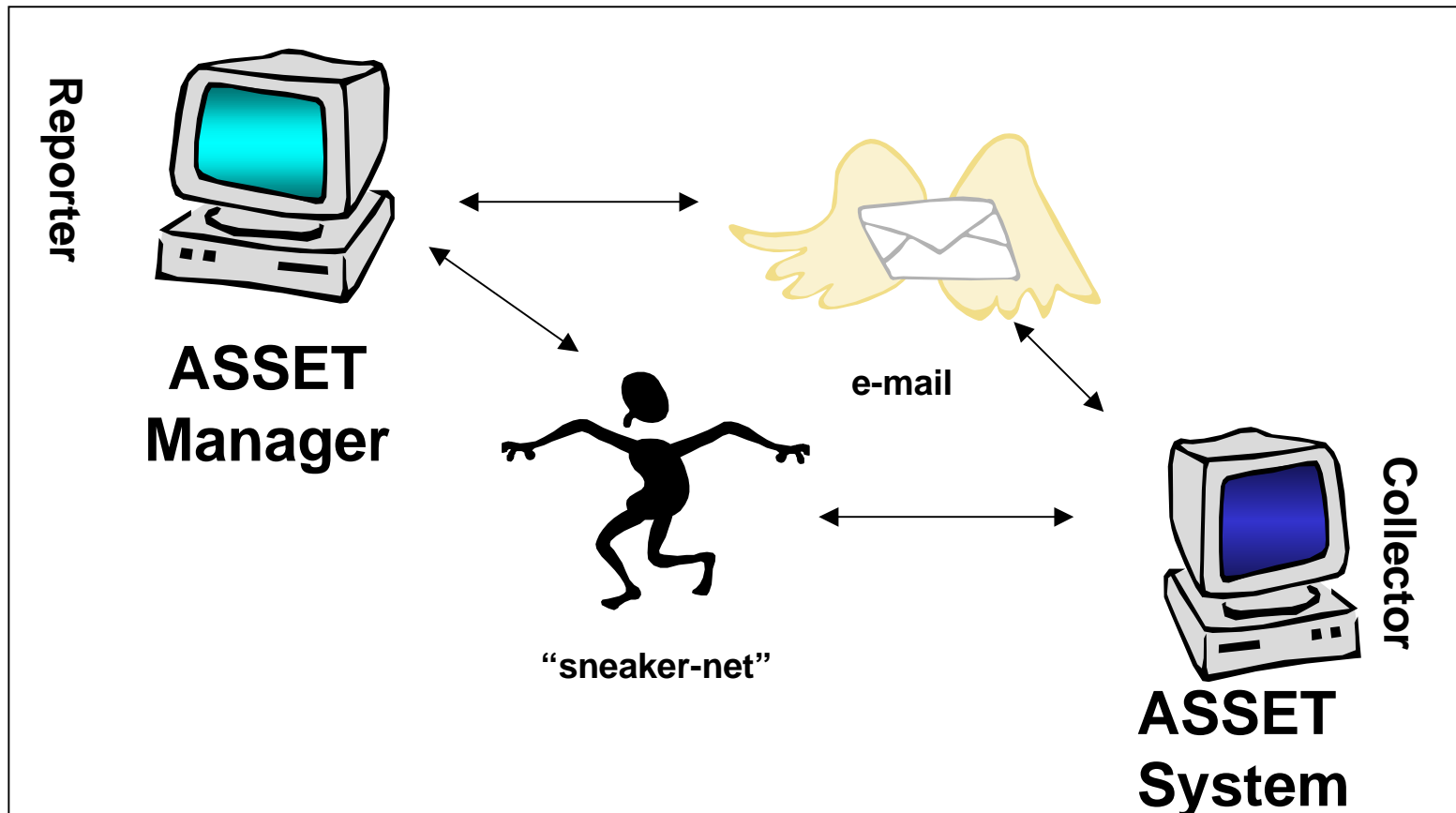
Assessment Framework



A typical assessment will have multiple 'Collectors' and one 'Reporter'

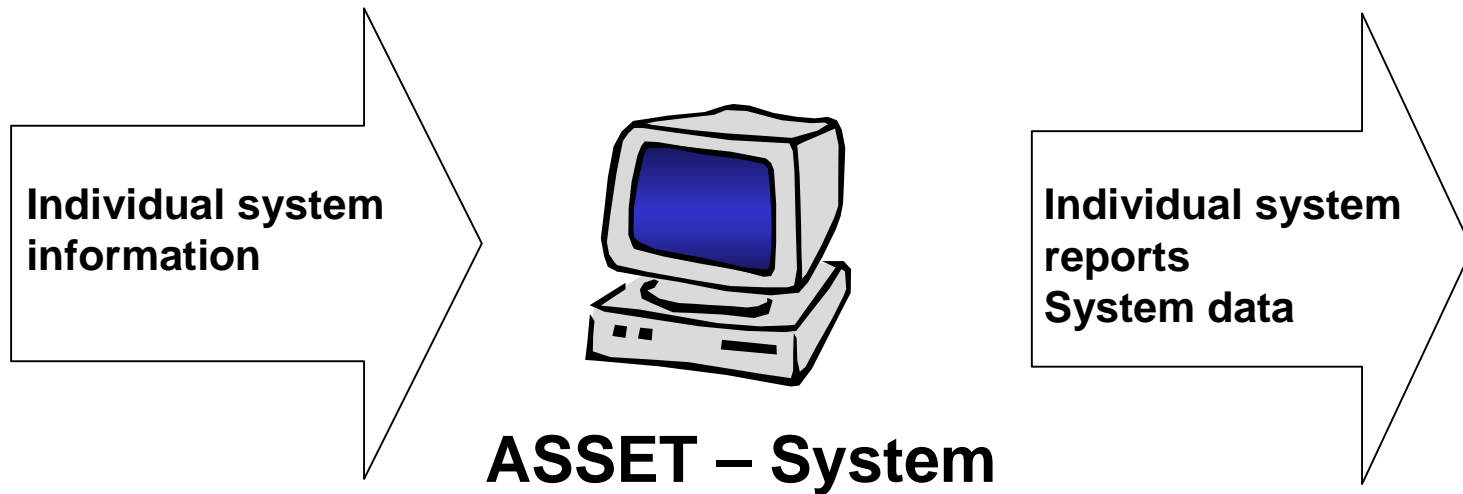
ASSET Description

ASSET Architecture

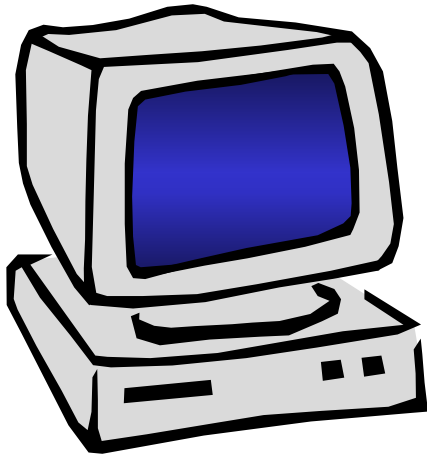


24 ASSET is comprised of two separate host-based applications

ASSET – System 1 of 3

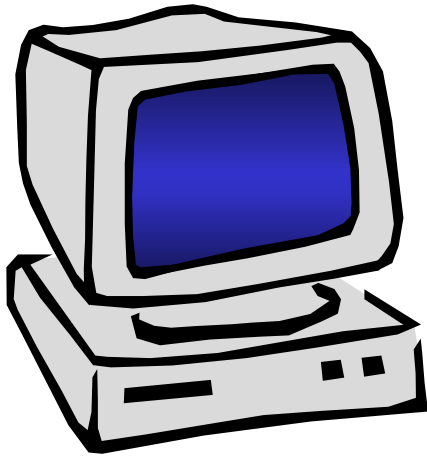


ASSET – System 2 of 3



- 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
- Tracks all collectors and SMEs who provide answers to ASSET questions

ASSET – System 3 of 3



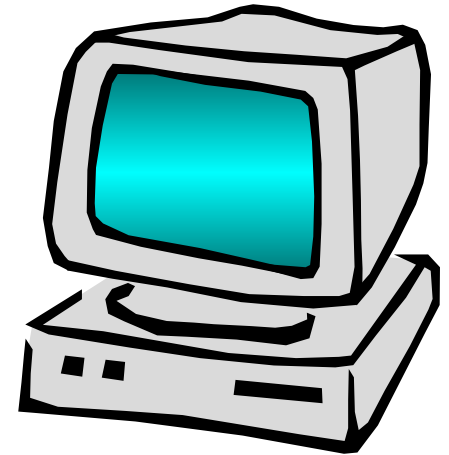
- Reports can be exported to any popular spreadsheet or charting program
- Reports
 - Summary of topic areas by levels of effectiveness
 - List of N/A questions
 - List of risk-based decisions
 - System summary

ASSET – Manager 1 of 3



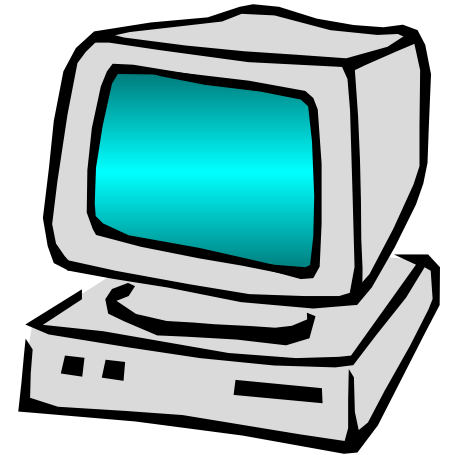
ASSET – Manager 2 of 3

- Aggregates data from multiple systems so that agency-wide reports can be developed
- Tracks all collectors and SMEs who provide answers to ASSET questions



ASSET – Manager 3 of 3

- 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; host-based security is a must
- It is the first of a number of modules that will assist IT security managers in providing for effective security

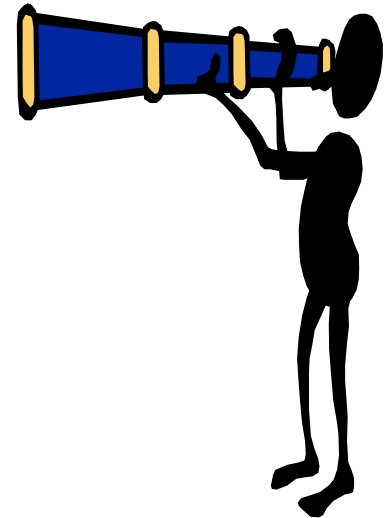
ASSET Limitations

- 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)



Future Plans for ASSET

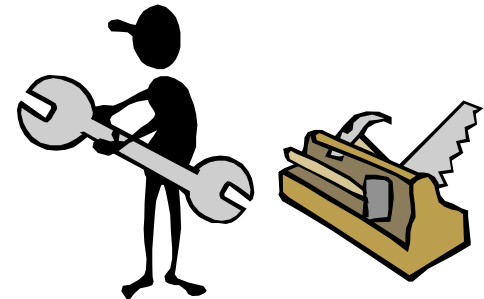
- Enhance current capabilities of ASSET
- Additional capabilities under consideration:
 - Performance measures
 - Plan of action and milestone report
 - Certification and accreditation
 - Linkage to system inventory
 - Customization of application
- What do you need?



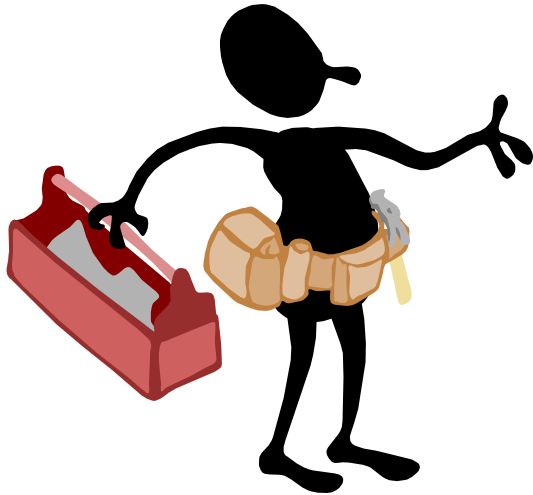
ASSET Installation

Minimum System Requirements

- Hardware
 - Pentium II – 266 MHz processor
- Operating Systems
 - Designed to operate on all Windows 9X operating systems
 - Initial operating capability on W2000 Professional
- Memory Requirements
 - 120 MB free space



ASSET Installation



- Installation wizard –
 - Guides the user through installation process
 - Follows Windows conventions

ASSET Delivery Media

- CD
 - Contains all needed ASSET - System and ASSET - Manager files
 - User Manual and Help files
 - NIST Special Publication 800-26
- Web site
 - IT Security Self-Assessment web site will be developed to host ASSET software and documentation
 - Spreadsheet templates for report analysis

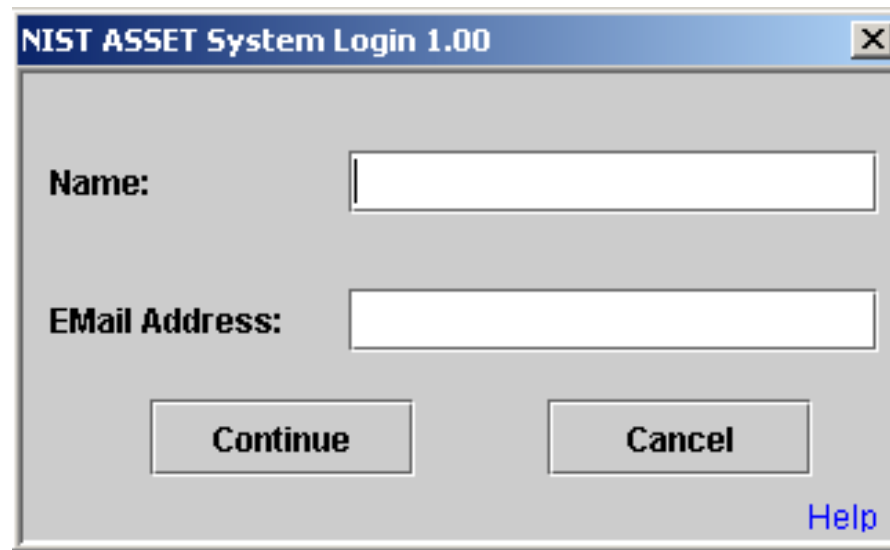


BREAK

ASSET – System Demonstration

- Log in
- New Assessment
- Existing Assessment
- Export Data
- Generate Individual
System Reports
- Export Reports

ASSET - System Log In



The image shows a screenshot of a Windows-style dialog box titled "NIST ASSET System Login 1.00". The dialog box has a blue title bar with a close button (X) in the top right corner. The main area is light gray and contains two text input fields. The first field is labeled "Name:" and the second is labeled "EMail Address:". Below the input fields are two buttons: "Continue" and "Cancel". In the bottom right corner, there is a blue hyperlink labeled "Help".

NIST ASSET System Login 1.00 [X]

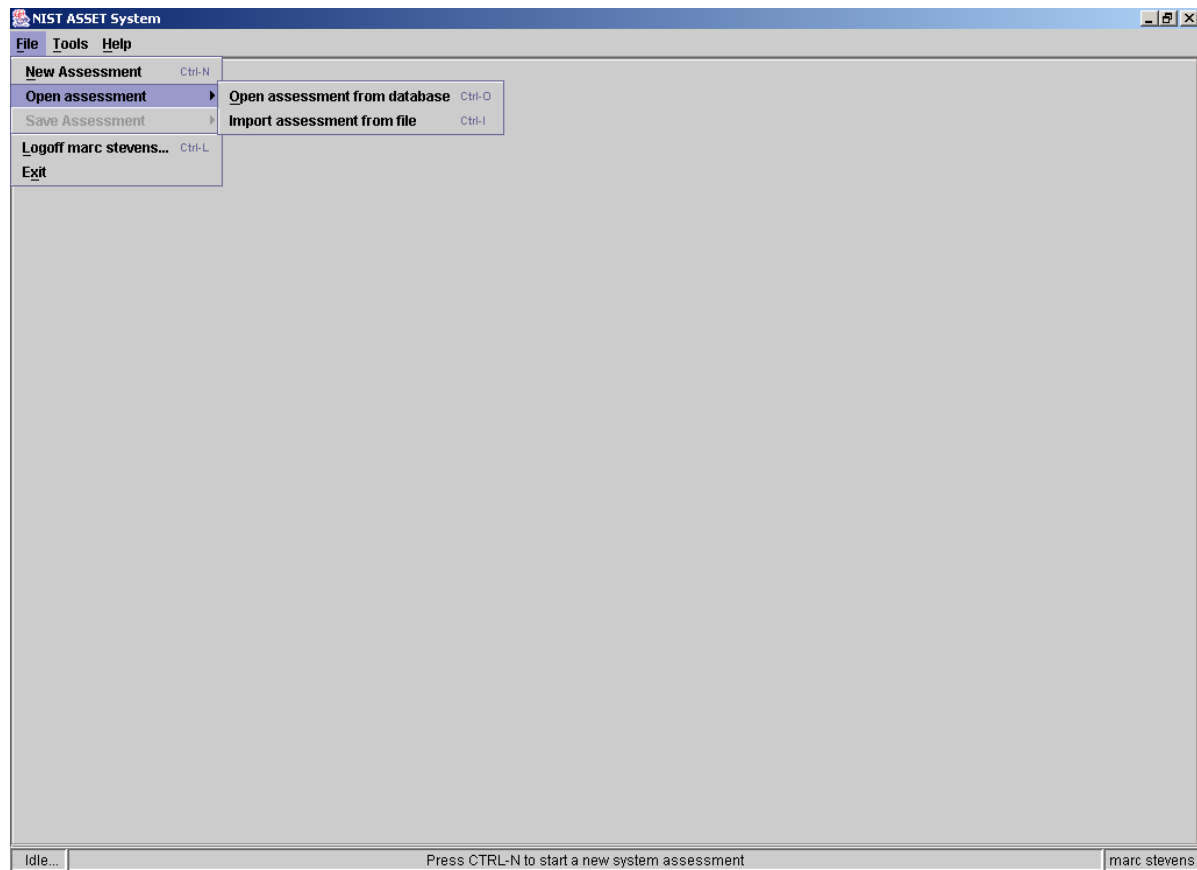
Name:

EMail Address:

Continue **Cancel**

[Help](#)

ASSET - System Open New / Existing Assessment



ASSET - System New Assessment

NIST ASSET System

File Tools Help

Self-Assessment

Assessment Identification System Identification Policy Assessment Questions Summary

System Assessors

| Primary | Name | Email | Phone |
|-------------------------------------|--------------|----------------------|-------|
| <input checked="" type="checkbox"/> | marc stevens | stevens_marc@bah.com | |

+ Add Assessor X Delete Assessor ? Help

Assessment Objective

Next >>

AIP New assessment active... marc stevens

ASSET - System System Identification

System Identification

System Name *: System XYZ

System Number *: 2006234

System Type *: General Support System

Agency/Group/Division *: FB4623

Assessment Start Date *: Mon Mar 25 21:35:48 EST 2002

System Criticality

Confidentiality *: High

Integrity *: Medium

Availability *: Low

Inter-Connected Systems

| System | Boundary Controls Effective? | Planned Action if Not |
|--------------------------|------------------------------|-----------------------|
| Interconnected System XY | Yes | |

[+ Add System](#) [X Delete System](#) [? Help](#)

All fields marked with an * above are required

[<< Previous](#) [Proceed To Assessment >>](#)

AIP | marc.stevens

ASSET - System Policy Tab

The screenshot shows the NIST ASSET System interface. The title bar reads "NIST ASSET System". The menu bar includes "File", "Tools", and "Help". The main window title is "System XYZ assessment in progress...". The "Policy" tab is selected, showing a "Policy Definition:" section with a table of control objectives. The table has three columns: "Number", "Control Objective", and "Policy Defined?". The rows are numbered 1.0.0 through 17.0.0. The "Policy Defined?" column contains checkboxes, some of which are checked. At the bottom of the table, there are "Previous" and "Next" navigation buttons.

| Number | Control Objective | Policy Defined? |
|--------|--|-------------------------------------|
| 1.0.0 | Risk Management | <input checked="" type="checkbox"/> |
| 2.0.0 | Review of Security Controls | <input checked="" type="checkbox"/> |
| 3.0.0 | Life Cycle | <input checked="" type="checkbox"/> |
| 4.0.0 | Authorize Processing (Certification & Accreditation) | <input type="checkbox"/> |
| 5.0.0 | System Security Plan | <input type="checkbox"/> |
| 6.0.0 | Personnel Security | <input type="checkbox"/> |
| 7.0.0 | Physical and Environmental Protection | <input type="checkbox"/> |
| 8.0.0 | Production, Input/Output Controls | <input checked="" type="checkbox"/> |
| 9.0.0 | Contingency Planning | <input checked="" type="checkbox"/> |
| 10.0.0 | Hardware and System Software Maintenance | <input type="checkbox"/> |
| 11.0.0 | Data Integrity | <input type="checkbox"/> |
| 12.0.0 | Documentation | <input checked="" type="checkbox"/> |
| 13.0.0 | Security Awareness, Training, and Education | <input type="checkbox"/> |
| 14.0.0 | Incident Response Capability | <input type="checkbox"/> |
| 15.0.0 | Identification and Authentication | <input type="checkbox"/> |
| 16.0.0 | Logical Access Controls | <input checked="" type="checkbox"/> |
| 17.0.0 | Audit Trails | <input checked="" type="checkbox"/> |

ASSET - System Assessment Questions

The screenshot displays the NIST ASSET System interface. The window title is "NIST ASSET System" and the menu bar includes "File", "Tools", and "Help". The main window is titled "System XYZ assessment in progress...".

The interface is divided into several sections:

- Left Panel (Assessment map):** A tree view showing the assessment structure. The selected path is: Assessment map > Policy > Management Controls > 1.1.0 Is risk periodically assessed? > 1.1.1.
- Top Panel (Assessment Identification):** Contains the question text: "Question: 1.1.1 Is the current system configuration documented, including links to other systems?".
- Right Panel (Section):** Shows the section "Management Controls Risk Management" and the critical element "1.1.0 Is risk periodically assessed?".
- Response Section:** Titled "Indicate Your Responses:", it includes checkboxes for "Policy", "Procedures", "Implemented", "Tested", and "Integrated", and radio buttons for "Question not applicable" and "Risk Based Decision Made to Increase/Decrease/Omit Security Control?" (with a "Yes" option).
- Comments:** A large text area for providing additional information.
- Footer:** Includes "Answered By: marc stevens", "Question Complete?", "Assign to alternate: marc stevens", and navigation buttons: "Back", "Clear", "Help", and "Next".

The status bar at the bottom shows "AIP" on the left, "For help, press F1" in the center, and "marc stevens" on the right.

ASSET - System Summary

NIST ASSET System

File Tools Help

Critical System 1 assessment in progress, 3% complete

Assessment map

- Policy
 - Management Controls
 - 1.1.0 Is risk periodically assessed?
 - 1.1.1
 - 1.1.2
 - 1.1.3
 - 1.1.4
 - 1.1.5
 - 1.1.6
 - 1.2.0 Do program officials understand the risk to systems under their control and determine the acceptable level of risk?
 - 1.2.1
 - 1.2.2
 - 1.2.3
 - 2.1.0 Have the security controls of the system and interconnected systems been reviewed?
 - 2.1.1
 - 2.1.2
 - 2.1.3
 - 2.1.4
 - 2.1.5
 - 2.2.0 Does management ensure that corrective actions are effectively implemented?
 - 3.1.0 Has a system development life cycle methodology been developed?
 - 3.2.0 Are changes controlled as programs progress through testing to final approval?
 - 4.1.0 Has the system been certified/recertified and authorized to process (accredited)?
 - 4.2.0 Is the system operating over internet authority?

Assessment Identification Component Identification Policy Assessment Questions Summary

Current Assessment Progress: 3% complete

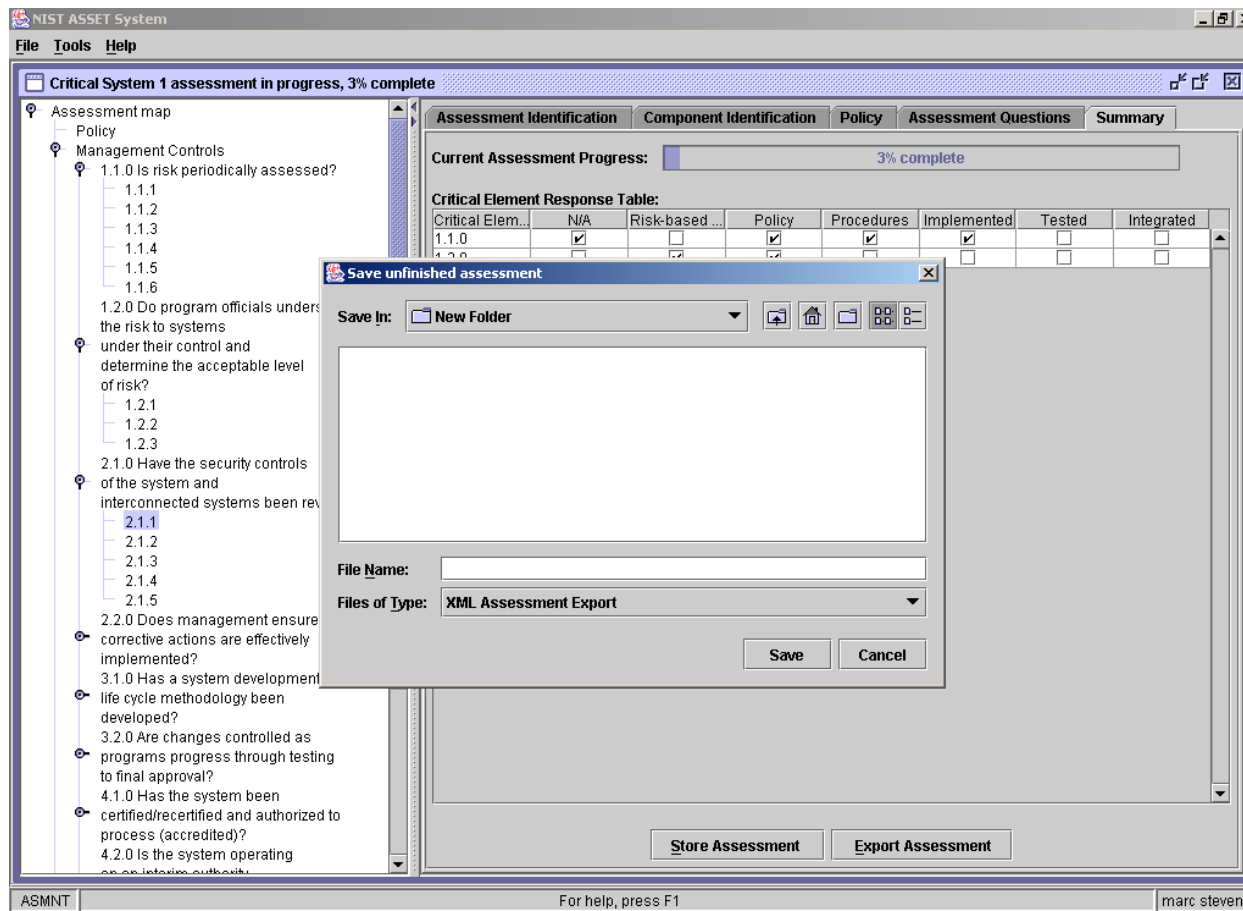
Critical Element Response Table:

| Critical Elem... | N/A | Risk-based ... | Policy | Procedures | Implemented | Tested | Integrated |
|------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------------------|
| 1.1.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.0 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

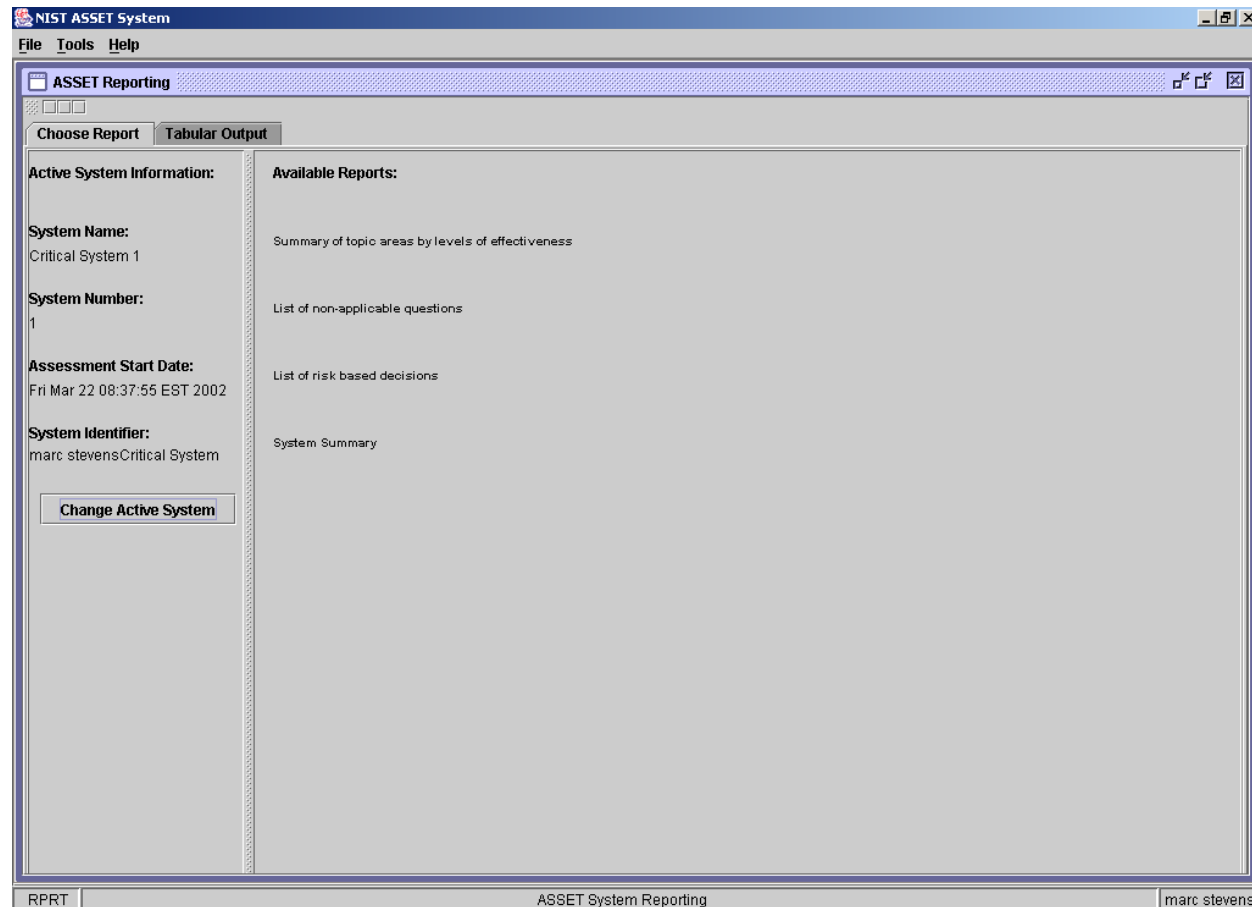
Store Assessment Export Assessment

ASMNT For help, press F1 marc.stevens

ASSET - System Export Data

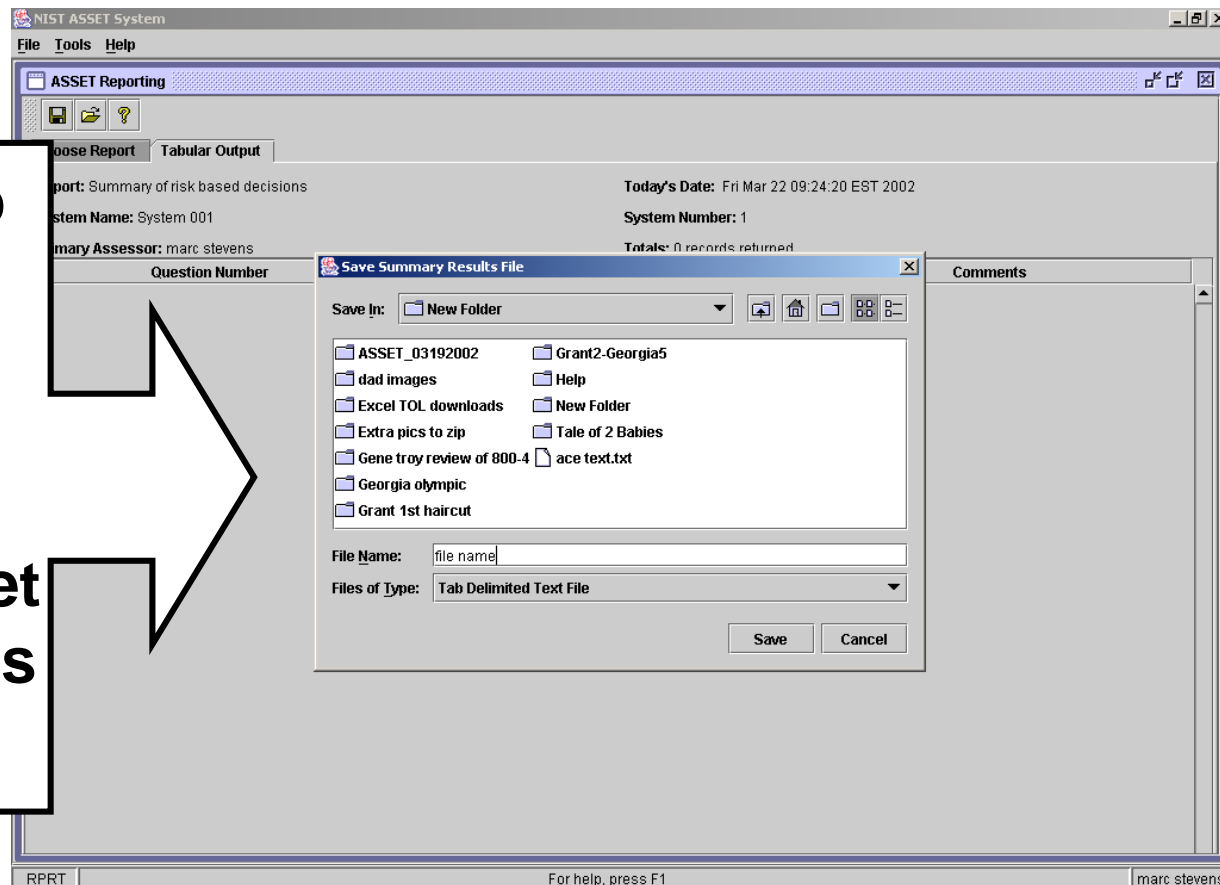


ASSET – System Generate Reports



ASSET – System Export Reports

**Save to tab
delimited
text file,
compatible
with
spreadsheet
applications**



Information Security Considerations

Data Sensitivity

- Agencies should determine report and data sensitivity
- Agencies are responsible for data protection
- ASSET does NOT provide for any security of data, such as encryption, while the data is stored or in transit

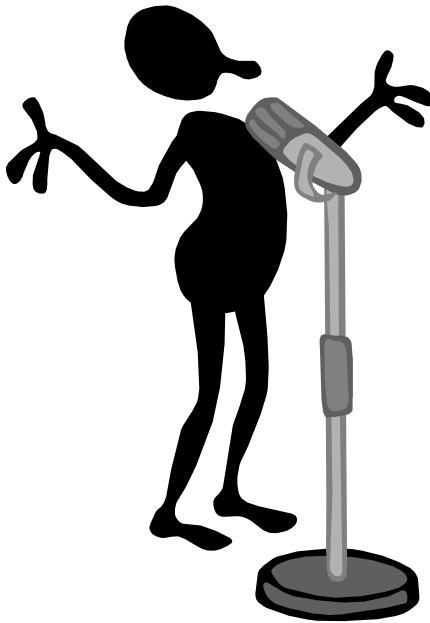


Data Sensitivity

- Application-based security is not provided for data transmitted between data collector and reporter
- ASSET uses Microsoft SQL Server Desktop Engine (MSDE) and therefore has the vulnerabilities of MSDE. Users should mitigate these vulnerabilities before using ASSET
- ASSET – System should be uninstalled after an assessment is completed as a best practice of all assessments

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
- No password protection is provided for accessing application or data

Summary

- ASSET System and ASSET Manager work together to assist an organization in collecting and reporting IT security self-assessment data

Questions

