



< FOCUS > < DISCOVER > < INTEGRATE > < ADVANCE >

Information Security Governance – The Federal Perspective

Mike Nelson, CISA, CISM, CISSP

President – SecureNet Technologies

The San Francisco Chapter of ISACA Proudly Presents The 2004 Annual
2004 SF ISACA FALL CONFERENCE

October 4–6, 2004

About this session

- ◆ The Federal Standard for Information Security Assurance
 - ◆ The IT Security Landscape
 - ◆ The Gist of NIST
 - ◆ The NIST Family of IT Security Guidance
 - ◆ The NIST Risk Management Framework
 - ◆ Security Plans
 - ◆ Categories of Information Systems
 - ◆ Security Control Architecture
 - ◆ System Certification and Accreditation
 - ◆ The NIST Self-Assessment Process
 - ◆ The ASSET Application
 - ◆ The System Security Steering Wheel
 - ◆ Summary and Conclusions
 - ◆ Questions and Answers

The IT Security Landscape

- ◆ Highly interactive environment of powerful computing devices and interconnected systems of systems across global networks
- ◆ Government agencies routinely interact with industry, private citizens, state and local governments, and the governments of other nations
- ◆ The complexity of today's systems and networks presents great security challenges for both producers and consumers of information technology

The IT Security Landscape

- ◆ The Advantage of the Offense
 - ◆ Sophisticated attack tools now available over the Internet to anyone who wants them
 - ◆ Powerful, affordable computing platforms to launch sophisticated attacks now available to the masses
 - ◆ Little skill or sophistication required to initiate extremely harmful attacks

The IT Security Landscape

◆ Key Security Challenges

- ◆ Adequately protecting enterprise information systems within constrained budgets
- ◆ Changing the current culture of:
 - ◆ *“Connect first...ask security questions later”*
- ◆ Bringing standards to:
 - ◆ Information system security control selection and specification
 - ◆ Methods and procedures employed to assess the correctness and effectiveness of those controls

The IT Security Landscape

- ◆ **Legislative and Policy Drivers - Federal**
 - ◆ **Public Law 107-347 (Title III)**
 - ◆ *Federal Information Security Management Act of 2002*
 - ◆ **Homeland Security Presidential Directive #7**
 - ◆ *Critical Infrastructure Identification, Prioritization, and Protection*
 - ◆ **OMB Circular A-130 (Appendix III)**
 - ◆ *Security of Federal Automated Information Resources*

The IT Security Landscape

- ◆ **Legislative and Policy Drivers – Private Sector**
 - ◆ The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
 - ◆ The Gramm-Leach-Bliley Act (GLBA), AKA the Financial Services Modernization Act of 1999
 - ◆ The Sarbanes-Oxley Act of 2002
 - ◆ California SB-1386 - Protection of Personal Data

The Gist of NIST

- ◆ Established in 1901 as the National Bureau of Standards
- ◆ Government's first physical science research laboratory
- ◆ Measurement tools and technical services integrated deeply into manufacturing, satellite systems, communication and transportation networks, laboratories, factories, hospitals, businesses, and the emerging digital economy
- ◆ Each day NIST receives more than 20 million automated requests for time via the Internet



The Gist of NIST

- ◆ A non-regulatory agency in the Technology Administration of the United States Department of Commerce
- ◆ Chartered to promote United States economic growth by working with industry to develop and apply technology, measurements and standards
- ◆ Headquartered in Gaithersburg, Maryland with fundamental scientific research at its Boulder, Colorado campus where two Nobel Prize winners are currently on staff

The Gist of NIST

- ◆ **The Computer Security Division (CSD) Mission**
- ◆ **Improve information systems security by:**
 - ◆ Raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies;
 - ◆ Researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive Federal systems;
 - ◆ Developing standards, metrics, tests and validation programs designed to:
 - ◆ Promote, measure, and validate security in systems and services;
 - ◆ Educate consumers; and
 - ◆ Establish minimum security requirements for Federal systems.
 - ◆ Developing guidance to increase secure IT planning, implementation, management and operation

The NIST Family of IT Security Guidance

- ◆ Security Considerations in the Information System Development Life Cycle (SP 800-64)
- ◆ Computer Security Incident Handling Guide (SP 800-61)
- ◆ Security Metrics Guide for Information Technology Systems (SP 800-55)
- ◆ Building an Information Technology Security Awareness and Training Program (SP 800-50)
- ◆ Wireless Network Security: 802.11, Bluetooth, and Handheld Devices (SP 800-48)
- ◆ Security Guide for Interconnecting Information Technology Systems (SP 800-47)
- ◆ Guidelines on Electronic Mail Security (SP 800-45)
- ◆ Guidelines on Securing Public Web Servers (SP 800-44)
- ◆ Guideline on Network Security Testing (SP 800-42)
- ◆ Guidelines on Firewalls and Firewall Policy (SP 800-41)
- ◆ Procedures for Handling Security Patches (SP 800-40)

The NIST Family of IT Security Guidance

- ◆ Guide to Selecting Information Security Products (SP 800-36)
- ◆ Guide to Information Technology Security Services (SP 800-35)
- ◆ Contingency Planning Guide for Information Technology Systems (SP 800-34)
- ◆ Underlying Technical Models for Information Technology Security (SP 800-33)
- ◆ Intrusion Detection Systems (SP 800-31)
- ◆ Risk Management Guide for Information Technology Systems (SP 800-30)
- ◆ Information Technology Security Training Requirements: A Role- and Performance-Based Model (SP 800-16)

The NIST Family of IT Security Guidance

- ◆ SP 800-58 (DRAFT): Security Considerations for Voice Over IP Systems
- ◆ SP 800-67 (DRAFT): Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
- ◆ SP 800-63 (DRAFT): Recommendation for Electronic Authentication
- ◆ SP 800-38B (DRAFT): Recommendation for Block Cipher Modes of Operation: the RMAC Authentication Mode
- ◆ SP 800-38C (DRAFT): Recommendation for Block Cipher Modes of Operation: The CCM Model for Authentication and Confidentiality
- ◆ SP 800-56 & 57 (DRAFT): Recommendation on Key Management



The NIST Risk Management Framework

- ◆ FISMA requires each federal agency to “develop, document, and implement an agency-wide information security program ... to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.”

The NIST Risk Management Framework

- ◆ **At a high level, FISMA requires agencies to:**
 - ◆ Plan for security
 - ◆ Ensure that appropriate officials are assigned security responsibility
 - ◆ Review the security controls in their information systems
 - ◆ Authorize system processing prior to operations and, periodically, thereafter

The NIST Risk Management Framework

- ◆ **Periodic assessments of risk**, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency
- ◆ **Policies and procedures that are based on risk assessments**, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system
- ◆ **Subordinate plans** for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate

The NIST Risk Management Framework

- ◆ **Security awareness training** to inform personnel of the information security risks associated with their activities and their responsibilities in complying with policies
- ◆ **Periodic testing and evaluation** of the effectiveness of security policies, procedures, practices, and controls to be performed with a frequency depending on risk, but no less than annually
- ◆ **A process for planning, implementing, evaluating, and documenting remedial action** to address any deficiencies in the security policies, procedures, and practices
- ◆ **Procedures for detecting, reporting, and responding to security incidents**
- ◆ **Plans and procedures to ensure continuity of operations**

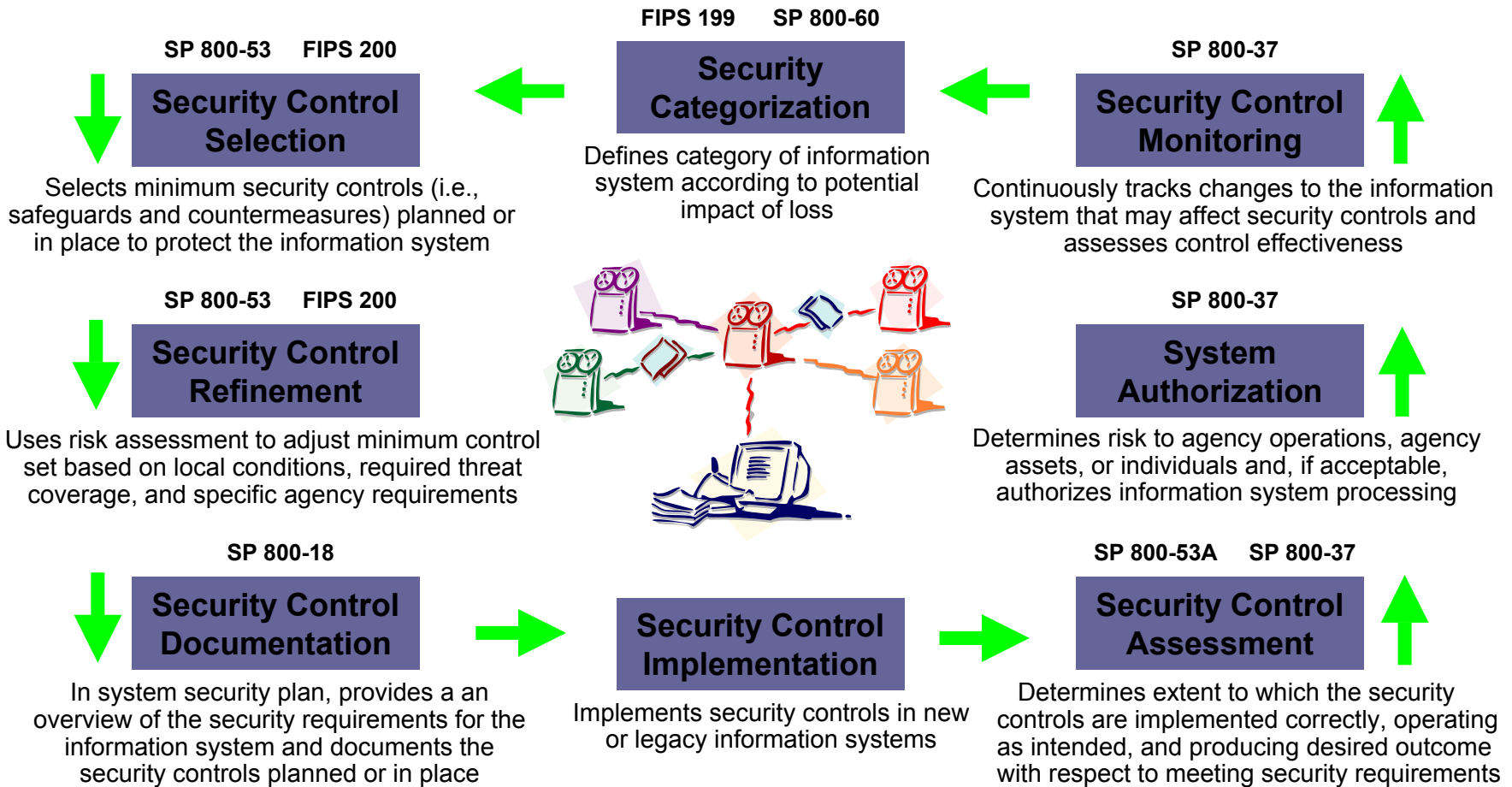
The NIST Risk Management Framework

- ◆ **The NIST response to FISMA**
 - ◆ Standards to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels
 - ◆ Guidelines recommending the types of information and information systems to be included in each category
 - ◆ Minimum information security requirements, (i.e., management, operational, and technical security controls), for information and information systems in each such category

The NIST Risk Management Framework

- ◆ **NIST documents designed to comply with FISMA requirements:**
 - ◆ Guide for Developing Security Plans for Information Technology Systems (SP 800-18)
 - ◆ Standards for Security Categorization of Federal Information Systems (FIPS 199)
 - ◆ Guide for Mapping Types of Information and Information Systems to Security Categories (SP 800-60 – target final publication 3Q04)
 - ◆ Recommended Security Controls for Federal Information Systems (SP 800-53 – to be reissued as FIPS 200 EOY05)
 - ◆ Guide for Assessing the Security Controls in Federal Information Systems (SP 800-53A – target final publication 1Q05)
 - ◆ Guide for the Security Certification and Accreditation of Federal Information Systems (SP 800-37)

The NIST Risk Management Framework



The NIST Risk Management Framework

- ◆ *The Guide for Developing Security Plans for Information Technology Systems (SP 800-18)*
 - ◆ Describes NIST's view of the system analysis process
 - ◆ Provides guidance on the general information contained in all security plans
 - ◆ Defines the concept and function of the three security control categories:
 - ◆ Management Control
 - ◆ Operational Controls
 - ◆ Technical Controls
 - ◆ Defines the distinction between major applications and general support systems
 - ◆ Provides examples of system "rules of behavior" and a template for security plans

The NIST Risk Management Framework

- ◆ *The Standards for Security Categorization of Federal Information Systems (FIPS 199)*
 - ◆ Sets out the standards for categorizing information and information systems
 - ◆ Security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals
 - ◆ Security categories are used in conjunction with vulnerability and threat information in assessing the risk to an organization

The NIST Risk Management Framework

- ◆ FIPS 199 defines three levels of potential impact on organizational operations, assets or individuals resulting from the loss of confidentiality, integrity, or availability:
 - LOW if the loss of is expected to have a **limited** adverse effect
 - MODERATE if the loss is expected to have a **serious** adverse effect
 - HIGH if the loss is expected to have a **severe or catastrophic** adverse effect

The NIST Risk Management Framework

- ◆ The generalized format for expressing the security category, SC, of an information type is:

SC information type = {(confidentiality, *impact*), (integrity, *impact*), (availability, *impact*)}

where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE



The NIST Risk Management Framework

- ◆ *The Guide for Mapping Types of Information and Information Systems to Security Categories (SP 800-60)*
 - ◆ Designed to help organizations map security impact levels in a consistent manner
 - ◆ Defines relationships between:
 - ◆ Types of information (e.g., privacy, medical, proprietary, financial, trade) and
 - ◆ Information systems (e.g., mission critical, mission support, administrative)
 - ◆ Divided into two volumes
 - ◆ Volume I: guidelines for information type identification and security categorization
 - ◆ Volume II: appendices, including examples of impact assignments and security categorization rationale



The NIST Risk Management Framework

- ◆ *The Recommended Security Controls for Federal Information Systems (SP 800-53)*
 - ◆ Security controls are based on:
 - ◆ **Mechanisms** (e.g., identification and authentication mechanisms, physical access control devices, cryptographic mechanisms) or
 - ◆ **Documentation** (e.g., policies, plans, procedures)
 - ◆ Security controls possess two important properties:
 - ◆ **Robustness** – the property that allows security controls to be defined with varying strengths of function and with varying degrees of assurance regarding the effectiveness of implementation
 - ◆ **Flexibility** – the property allows organizations to tailor security controls to satisfy unique security policies and to meet specific operational needs



The NIST Risk Management Framework

◆ Three levels of security control robustness are defined:

◆ **Basic**

◆ **Enhanced**

◆ **Strong**

THREAT CHARACTERISTICS		BASELINE CONTROL COVERAGE ESTIMATE		
		LOW	MODERATE	HIGH
INTENTIONAL ATTACK: LOCAL (Physical presence of attacker required at the site of attack)				
ATTACK SOPHISTICATION: LOW		√	√	TBD
ATTACK SOPHISTICATION: HIGH				
ATTACKER INTENT: NON-MALICIOUS				
ATTACKER RESOURCES: ALL LEVELS (Minimal, Moderate, Substantial)				
ATTACKER ACCESS: OUTSIDER		√	√	TBD
ATTACKER ACCESS: INSIDER		√-	√-	TBD
ATTACKER INTENT: MALICIOUS				
ATTACKER RESOURCES: MINIMAL				
ATTACKER ACCESS: OUTSIDER		√	√	TBD
ATTACKER ACCESS: INSIDER		√-	√-	TBD
ATTACKER RESOURCES: MODERATE				
ATTACKER ACCESS: OUTSIDER		√	√	TBD
ATTACKER ACCESS: INSIDER		√-	X	TBD
ATTACKER RESOURCES: SUBSTANTIAL				
ATTACKER ACCESS: OUTSIDER		√	√	TBD
ATTACKER ACCESS: INSIDER		√-	X	TBD
LEGEND				
√ = The security controls in the selected baseline provide adequate security and coverage for the stated threats.				
√- = The combination of the security controls in the selected baseline and the situation and context in which the controls are employed including any general risk mitigation factors provide adequate security and coverage for the stated threats.				
X = The security controls in the selected baseline do not provide adequate security and coverage for the stated threats.				

The NIST Risk Management Framework

◆ Security controls are organized into *classes and families*

CLASS	FAMILY NAME	IDENTIFIER
Management	Risk Assessment	RA
	Security Planning	PL
	System and Services Acquisition	SA
	Security Control Review	CR
	Processing Authorization	PA
Operational	Personnel Security	PS
	Physical and Environmental Protection	PE
	Contingency Planning and Operations	CP
	Configuration Management	CM
	Hardware and Software Maintenance	MA
	System and Information Integrity	SI
	Media Protection	MP
	Incident Response	IR
	Security Awareness and Training	AT
Technical	Identification and Authentication	IA
	Logical Access Control	AC
	Accountability (Including Audit Trails)	AU
	System and Communications Protection	SP

The NIST Risk Management Framework

- ◆ **The security controls have a well-defined structure consisting of three components:**
 - ◆ **A control objective section** which provides the overall objective for the particular security control when applied to an information system
 - ◆ **A control mapping section** which lists source documents that have similar security controls which were considered during the development of the control catalog
 - ◆ **A control description section** which provides the specific control requirements and details of each control

The NIST Risk Management Framework

Security Control Example

IA-13.b UNSUCCESSFUL LOGIN ATTEMPTS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to take defined action in the face of multiple unsuccessful login attempts.

For a given user, there is a limit of *[Assignment: number, typically three]* invalid information system access attempts that may occur over *[Assignment: time period (e.g., fifteen minutes)]*. When the maximum number of unsuccessful attempts is exceeded, the information system automatically *[Selection: locks the account/node until released by an administrator, locks the account/node for an [Assignment: time period (e.g., fifteen minutes)], delays next login prompt according to [Assignment: delay algorithm e.g., the standard Unix algorithm that accomplishes successively longer delays with each subsequent failure]]*.

The NIST Risk Management Framework

- ◆ For the **ENHANCED** level of the same control, the following text is added to the **BASIC** level text:
 - ◆ *Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed*

The NIST Risk Management Framework

- ◆ *The Guide for Assessing the Security Controls in Federal Information Systems (SP 800-53A)*
 - ◆ Scheduled for final publication in early 2005
 - ◆ Will establish methods and procedures to assess security controls
 - ◆ Will provide guidance on:
 - ◆ Assessment methods and procedures
 - ◆ Interviewing personnel associated with the security aspects of the system
 - ◆ Reviewing and examining security-related policies, procedures, and documentation
 - ◆ Observing security-related activities and operations
 - ◆ Analyzing, testing, and evaluating the security relevant and security critical aspects of system hardware, software, firmware, and operations
 - ◆ Conducting demonstrations and exercises

System Certification and Accreditation

- ◆ *Guide for the Security Certification and Accreditation of Federal Information Systems (SP 800-37)*
 - ◆ The heart of the NIST Information Security Program
 - ◆ An official management act reflecting their unambiguous acceptance of the risk to the organization's operations, assets, or staff based on the implementation of a defined set of security controls
 - ◆ By accrediting an information system, a single company official accepts ultimate responsibility for the security of the system and is fully accountable for any negative impacts to the organization if a breach of security occurs

System Certification and Accreditation

- ◆ Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system
- ◆ It determines the extent to which the controls are:
 - ◆ Implemented correctly
 - ◆ Operating as intended
 - ◆ Producing the desired outcome with respect to meeting the security requirements for the system
- ◆ Security **certification** is a technical process while system **accreditation** is a management function

System Certification and Accreditation

Role	Responsibilities
<p>Authorizing Official (sometimes referred to as the Approving or Accrediting Authority)</p>	<ul style="list-style-type: none"> ◆ Senior management official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk ◆ Assumes responsibility and is accountable for the risks associated with operating an information system ◆ Typically has the authority to oversee the budget or business operations of the information system ◆ May be called upon to approve system security requirements and system security plans ◆ Can issue an interim approval to operate the system under specific terms and conditions ◆ Can deny authorization to operate the system (or if the system is already operational, halt operations)



System Certification and Accreditation

Role	Responsibilities
Authorizing Official Designated Representative	<ul style="list-style-type: none"> ◆ Acts on the authorizing official's behalf in coordinating and carrying out the necessary activities required during the Certification and Accreditation process ◆ May be empowered by the authorizing official to make certain decisions with regard to the planning and resourcing of the security Certification and Accreditation activities, the acceptance of the system security plan, and the determination of risk to company operations, assets, and individuals ◆ May be called upon to prepare the final security accreditation package, obtain the authorizing official's signature on the security accreditation decision letter, and transmit the accreditation package to the appropriate oversight officials ◆ May NOT be delegated the task of making the final security accreditation decision and the signing of the accreditation decision letter

System Certification and Accreditation

Role	Responsibilities
Chief Information Officer	<ul style="list-style-type: none"> ◆ Management official responsible for: <ul style="list-style-type: none"> ◆ designating a senior company information security officer ◆ developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements ◆ training and overseeing personnel with significant responsibilities for information security ◆ assisting management concerning their security responsibilities ◆ reporting to senior management on the effectiveness of the information security program, including progress of remedial actions ◆ Encourages the maximum reuse and sharing of security-related information including: <ul style="list-style-type: none"> ◆ threat and vulnerability assessments ◆ risk assessments ◆ results from common security control assessments ◆ any other general information that may be of assistance to information system owners ◆ Determines the appropriate allocation of resources dedicated to the protection of information systems ◆ May be designated as the authorizing official for company-wide general support systems

System Certification and Accreditation

Role	Responsibilities
Senior Information Security Officer	<ul style="list-style-type: none"> ◆ Carries out the Chief Information Officer responsibilities under FISMA ◆ Possesses professional qualifications, including training and experience, required to administer the information security program ◆ Has information security duties as their primary duty ◆ Heads an office with the mission and resources to assist in ensuring company compliance with regulations and laws ◆ May also serve as the authorizing official's designated representative ◆ Serves as the Chief Information Officer's primary liaison to the authorizing officials, information system owners, and information system security officers

System Certification and Accreditation

Role	Responsibilities
<p>Information System Owner</p>	<ul style="list-style-type: none"> ◆ Overall procurement, development, integration, modification, or operation and maintenance of an information system ◆ Develops and maintains the system security plan ◆ Ensures the system is deployed and operated according to the agreed upon security requirements ◆ Decides who has access to the information system (and with what types of privileges or access rights) ◆ Ensures that system users and support personnel receive security training (e.g., instruction in rules of behavior) ◆ Informs management of the need to conduct a security Certification and Accreditation of the information system, ensures appropriate resources are available for the effort, and provides the necessary system-related documentation to the certification agent ◆ Receives the security assessment results from the certification agent ◆ Assembles the accreditation package and submits the package to the authorizing official or the authorizing official's designated representative

System Certification and Accreditation

Role	Responsibilities
Information Owner	<ul style="list-style-type: none"> ◆ Has legal or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal ◆ Establishes the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with other organizations ◆ Is not necessarily the same person as the information system owner (indeed, a single information system may utilize information from multiple information owners) ◆ Should provide input to information system owners regarding the security requirements and security controls for the information systems where their information resides

System Certification and Accreditation

Role	Responsibilities
Information System Security Officer	<ul style="list-style-type: none"> ◆ Responsible to the authorizing official, information system owner, or the senior information security officer for ensuring the appropriate operational security posture is maintained ◆ Serves as the principal advisor to the authorizing official, information system owner, or senior information security officer on all matters involving the security of the information system ◆ Has the detailed knowledge required to manage the security aspects of the information system and, in many cases, is assigned responsibility for the day-to-day security operations of the system ◆ May include physical security, personnel security, incident handling, and security training and awareness ◆ May be called upon to assist in the development of the system security policy and to ensure compliance with that policy on a routine basis ◆ Plays an active role in developing and updating the system security plan and in managing and controlling changes to the system and assessing the security impact of those changes

System Certification and Accreditation

Role	Responsibilities
Certification Agent	<ul style="list-style-type: none"> ◆ An individual, group, or organization responsible for conducting a security certification, or comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system ◆ Provides recommended corrective actions to reduce or eliminate vulnerabilities in the information system ◆ Provides an independent assessment of the system security plan (prior to the assessment activities associated with the certification process) to ensure the plan provides a complete and consistent security specification for the information system that is adequate to meet all applicable security requirements ◆ Should be independent from the persons directly responsible for the development of the information system and the day-to-day operation of the system ◆ Should be independent of those individuals responsible for correcting security deficiencies identified during the security certification



System Certification and Accreditation

Role	Responsibilities
User Representative	<ul style="list-style-type: none"> ◆ Identifies mission/operational requirements ◆ Complies with the security requirements and security controls described in the security plan ◆ Represents the operational interests of the user community ◆ Serves as a liaison for the user community throughout the system development life cycle ◆ Assists in the security Certification and Accreditation process to ensure mission requirements are satisfied while meeting the security requirements and employing the security controls defined in the system security plan



System Certification and Accreditation

- ◆ **The independence of the Certification Agent is an important concept**
- ◆ **The security category of the information system should guide the degree of independence of the certification agent**
 - ◆ When the potential impact on company operations, assets or staff is low, a self-assessment activity may be reasonable and appropriate and not require an independent certification agent
 - ◆ When the potential impact level is moderate or high, certification agent independence is needed and justified

System Certification and Accreditation

- ◆ The **accreditation package** documents the results of the security certification and provides the authorizing official with the information required to make a valid, risk-based decision
- ◆ The information system owner is responsible for the assembly, compilation, and submission of the security accreditation package
- ◆ The accreditation package contains the following documents:
 - ◆ Approved system security plan
 - ◆ Security assessment report
 - ◆ Plan of action and milestones

System Certification and Accreditation

- ◆ The **system security plan** is prepared by the system owner and approved by the authorizing official and/or senior information security officer
- ◆ It provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements
- ◆ It contains other key security-related documents:
 - ◆ Risk assessment
 - ◆ Contingency plan
 - ◆ Incident response plan
 - ◆ Configuration management plan
 - ◆ Any system interconnection agreements

System Certification and Accreditation

- ◆ The **security assessment report** is prepared by the certification agent
- ◆ It documents the results of the security control assessment to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system security requirements
- ◆ It should also list the corrective actions recommended by the certification agent

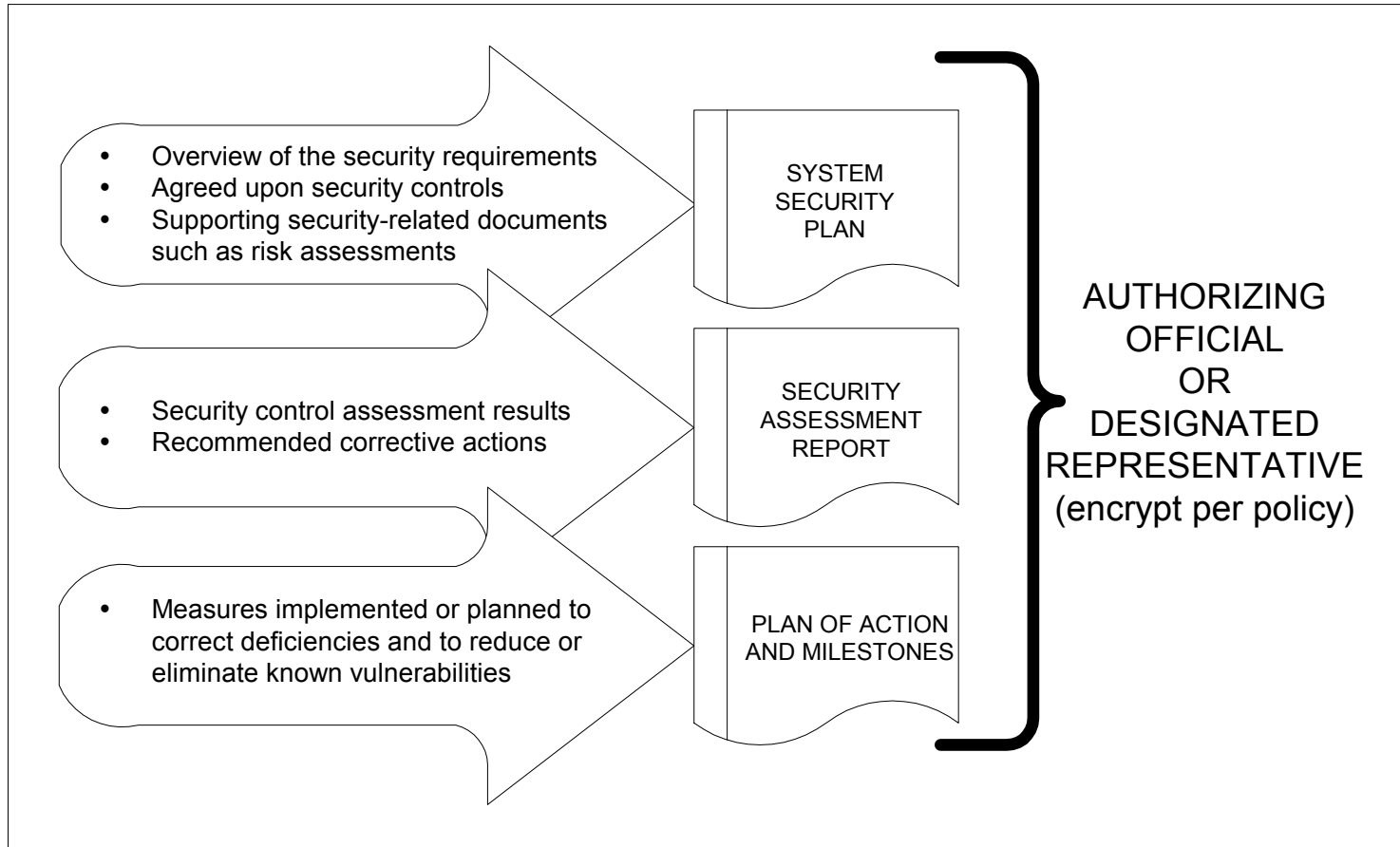
System Certification and Accreditation

- ◆ **The plan of action and milestones** is prepared by the system owner
- ◆ It describes the measures that have been implemented or planned to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the information system



System Certification and Accreditation

The Security Accreditation Package



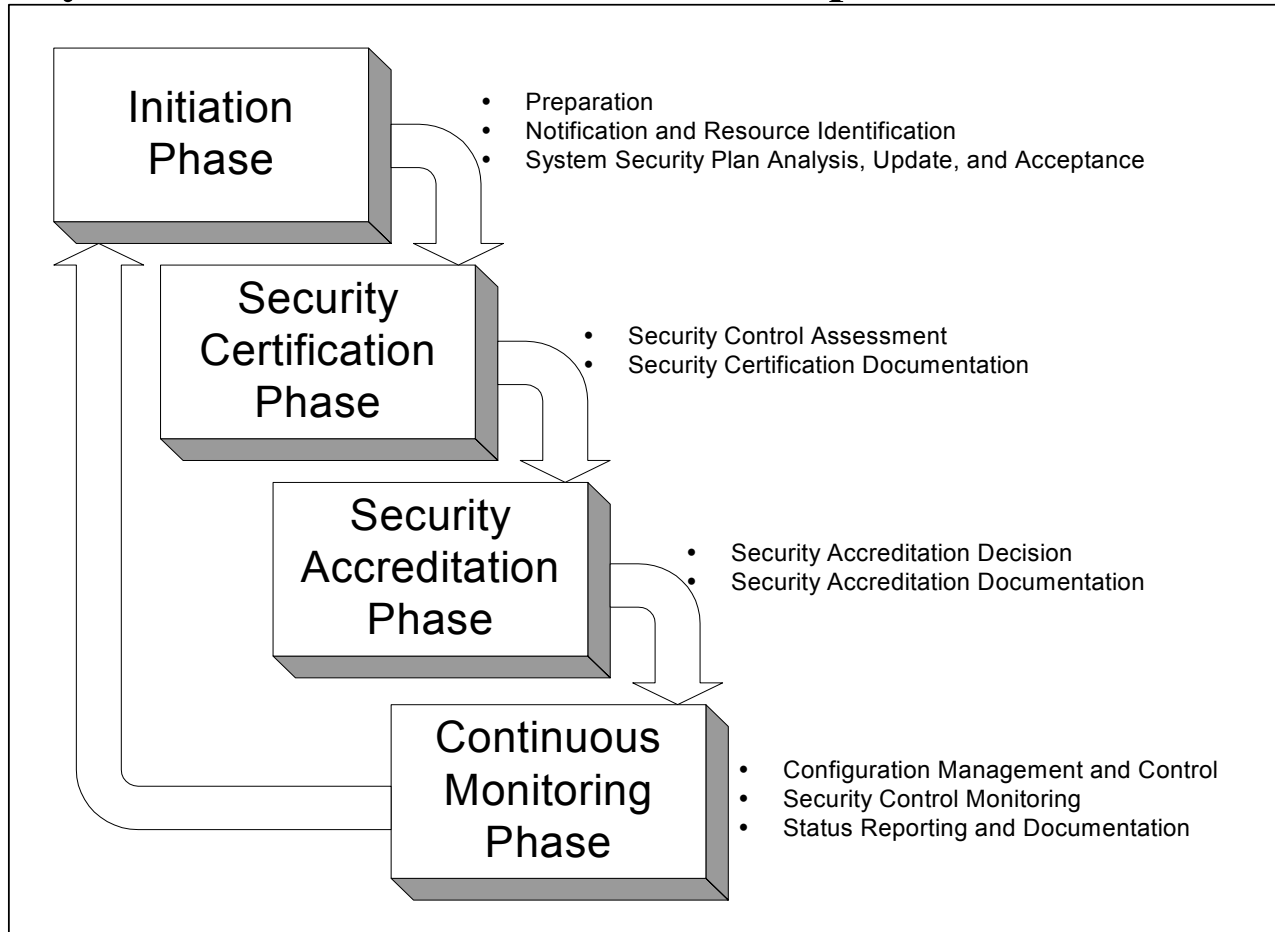
System Certification and Accreditation

- ◆ The security accreditation decision letter transmits the security accreditation decision from the authorizing official to the information system owner
- ◆ It contains the following elements:
 - ◆ Accreditation decision
 - ◆ Supporting rationale for the decision
 - ◆ Terms and conditions for the authorization
- ◆ The letter is the indication to the information system owner whether the system is fully authorized to operate, authorized to operate on an interim basis under strict terms and conditions or not authorized to operate at all



System Certification and Accreditation

◆ The Security Certification and Accreditation process consists of four phases:



System Certification and Accreditation

◆ Certification and Accreditation Process Steps

Phase	Primary Task	Sub-Task Number	Sub-Task Description
Initiation	Preparation	Subtask 1.1	Information System Description
		Subtask 1.2	Security Categorization
		Subtask 1.3	Threat Identification
		Subtask 1.4	Vulnerability Identification
		Subtask 1.5	Security Control Identification
		Subtask 1.6	Initial Risk Determination
	Notification and Resource Identification	Subtask 2.1	Notification
		Subtask 2.2	Planning and Resources
	System Security Plan Review, Analysis, and Acceptance	Subtask 3.1	Security Categorization Review
		Subtask 3.2	System Security Plan Analysis
Subtask 3.3		System Security Plan Update	
Subtask 3.4		System Security Plan Acceptance	

Phase	Primary Task	Sub-Task Number	Sub-Task Description
Security Certification	Security Control Assessment	Subtask 4.1	Documentation and Supporting Materials
		Subtask 4.2	Reuse of Assessment Results
		Subtask 4.3	Methods and Procedures
		Subtask 4.4	Security Assessment
		Subtask 4.5	Security Assessment Report
	Security Certification Documentation	Subtask 5.1	Findings and Recommendations
		Subtask 5.2	System Security Plan Update
		Subtask 5.3	Accreditation Package Assembly

System Certification and Accreditation

◆ Certification and Accreditation Process Steps

Phase	Primary Task	Sub-Task Number	Sub-Task Description
Security Accreditation	Security Accreditation Decision	Subtask 6.1	Final Risk Determination
		Subtask 6.2	Risk Acceptability
	Security Accreditation Documentation	Subtask 7.1	Security Accreditation Package Transmission
		Subtask 7.2	System Security Plan Update
Phase	Primary Task	Sub-Task Number	Sub-Task Description
Continuous Monitoring	Configuration Management and Control	Subtask 8.1	Documentation of Information System Changes
		Subtask 8.2	Security Impact Analysis
	Security Control Monitoring	Subtask 9.1	Security Control Selection
		Subtask 9.2	Selected Security Control Assessment
	Status Reporting and Documentation	Subtask 10.1	System Security Plan Update
		Subtask 10.2	Status Reporting

System Certification and Accreditation

- ◆ **Special Publication 800-37 documents the specific properties of each sub-task including:**
 - ◆ A description of the sub-task deliverable
 - ◆ Identification of the entity responsible for the sub-task
 - ◆ Specific guidance to aid in the execution of the sub-task
 - ◆ Pointers to reference documentation
 - ◆ Supplemental guidance specifically for LOW impact systems to help those responsible for the Certification and Accreditation process to invest only the resources necessary to provide adequate protection (this element of the guidance is a recent addition to the 800-37 document)

The NIST Self- Assessment Process



Why Conduct a Security Self Assessment

- ◆ In some cases, it may be mandated by law
- ◆ Customers, employees and partners expect it
- ◆ If you don't, someone else will
- ◆ Prudent due diligence demands it
- ◆ You don't know what you don't know

Keys to the Process

- ◆ A structured, repeatable process
- ◆ As complex as it needs to be, as simple as it can be
- ◆ Designed to fix problems, not blame
- ◆ Designed to match the cost of controls with the value of the asset being protected
- ◆ A well documented process which produces well defined outputs
- ◆ Not yet another proprietary methodology
- ◆ Adopt and adapt

Self-Assessment Methodology

- ◆ NIST = National Institute of Standards and Technology, part of the Technology Administration of the US Department of Commerce
- ◆ NIST Special Publication 800-26 “Self-Assessment Guide for IT Systems”
- ◆ Designed for Federal Agencies, but built in collaboration with industry so it cleanly transfers to the commercial sector
- ◆ In the public domain



The Assessment Framework

- ◆ Designed to focus on a single system with the ability to aggregate the assessment results of multiple systems
- ◆ Defines five levels of IT security program effectiveness (maturity)
- ◆ Each level has well defined criteria to determine the extent to which a system meets assessment components
- ◆ System boundaries and the degree of sensitivity of information must first be determined

The Assessment Structure

- ◆ Cover Sheet
 - ◆ Control of completed questionnaire
 - ◆ System identification
 - ◆ Assessor information
 - ◆ Criticality of system and sensitivity of data
- ◆ Questionnaire
 - ◆ Three control areas
 - ◆ 36 Critical Elements
 - ◆ 225 Questions

Five Levels of Effectiveness

- ◆ Level 1 – Control objective is documented in a security policy
- ◆ Level 2 – Security controls are documented as procedures
- ◆ Level 3 – Procedures have been implemented
- ◆ Level 4 – Procedures and security controls are tested and reviewed
- ◆ Level 5 – Procedures and security controls are fully integrated into a comprehensive program

Management Controls

Control Item	Critical Element	Number of Questions
Risk Management	Is risk periodically assessed?	6
	Do program officials understand the risk to systems under their control and determine the acceptable level of risk?	3
Review of Security Controls	Have the security controls of the system and interconnected systems been reviewed?	5
	Does management ensure that corrective actions are effectively implemented?	1
Life Cycle	Has a system development life cycle methodology been developed?	12
	Are changes controlled as programs progress through testing to final approval?	13
Authorize Processing (Certification and Accreditation)	Has the system been certified/recertified and authorized to process (accredited)?	8
	Is the system operating on an interim authority to process in accordance with specified procedures?	1
System Security Plans	Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?	3
	Is the plan kept current?	1

Operational Controls

Control Item	Critical Element	Number of Questions
Personnel Security	Are duties separated to ensure least privilege and individual accountability?	8
	Is appropriate background screening for assigned positions completed prior to granting access?	4
Physical Security	Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?	19
	Is data protected from interception?	2
	Are mobile and portable systems protected?	2
Production Input/Output Controls	Is there user support?	1
	Are there media controls?	10
Contingency Planning	Have the most critical and sensitive operations and their supporting computer resources been identified?	3
	Has a comprehensive contingency plan been developed and documented?	10
	Are tested contingency/disaster recovery plans in place?	3

Operational Controls (continued)

Control Item	Critical Element	Number of Questions
Hardware and Systems Software Maintenance	Is access limited to system software and hardware?	5
	Are all new and revised hardware and software authorized, tested and approved before implementation?	13
	Are systems managed to reduce vulnerabilities?	2
Data Integrity	Is virus detection and elimination software installed and activated?	2
	Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?	9
Documentation	Is there sufficient documentation that explains how software/hardware is to be used?	9
	Are there formal security and operational procedures documented?	5
Security Awareness, Training and Education	Have employees received adequate training to fulfill their security responsibilities?	5
Incident Response Capability	Is there a capability to provide help to users when a security incident occurs in the system?	6
	Is incident related information shared with appropriate organizations?	3

Technical Controls

Control Item	Critical Element	Number of Questions
Identification and Authentication	Are users individually authenticated via passwords, tokens, or other devices?	14
	Are access controls enforcing segregation of duties?	2
Logical Access Controls	Do the logical access controls restrict users to authorized transactions and functions?	10
	Are there logical controls over network access?	15
	If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?	1
Audit Controls	Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?	9

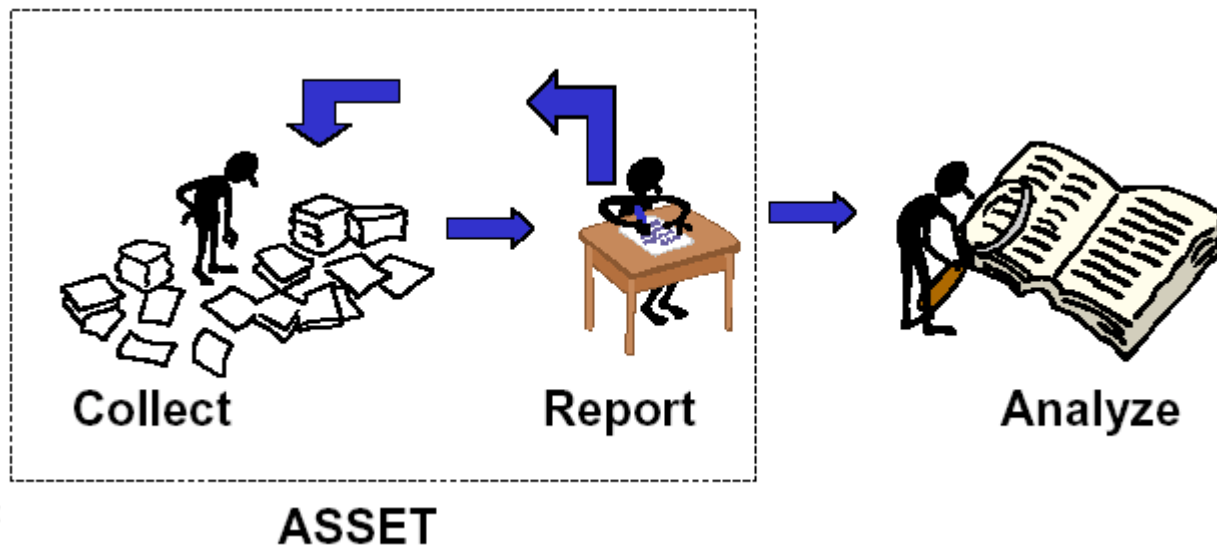
The NIST ASSET Application

- ◆ ASSET = Automated Security Self-Evaluation Tool
- ◆ Free, open source Java application
- ◆ Designed to assist assessment participants gather system data and create reports
- ◆ Not really “automated”



The ASSET Process

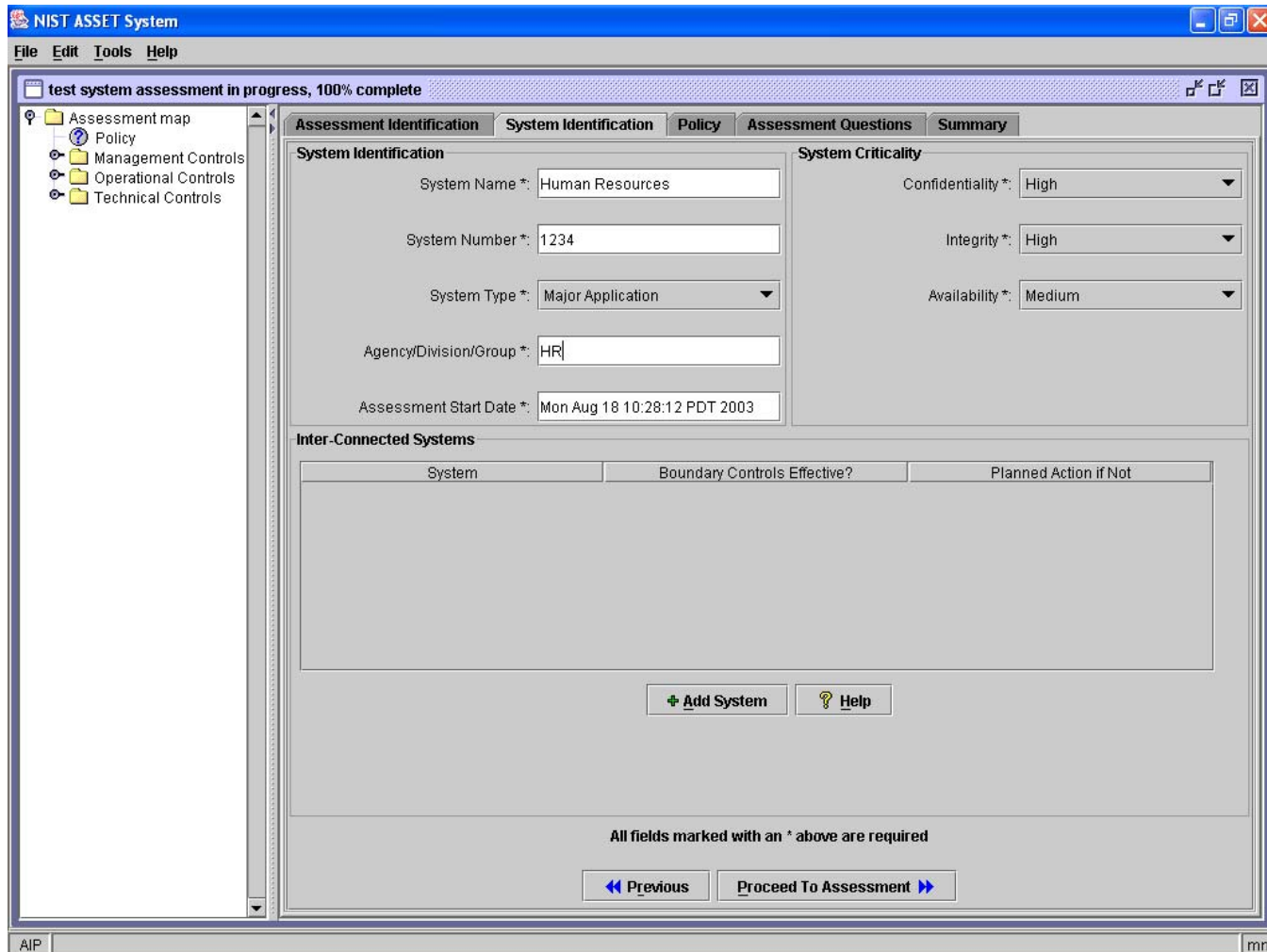
- ◆ The ASSET application assists with data gathering, serves as the repository for system security data and produces summary reports
- ◆ It does NOT automate data analysis



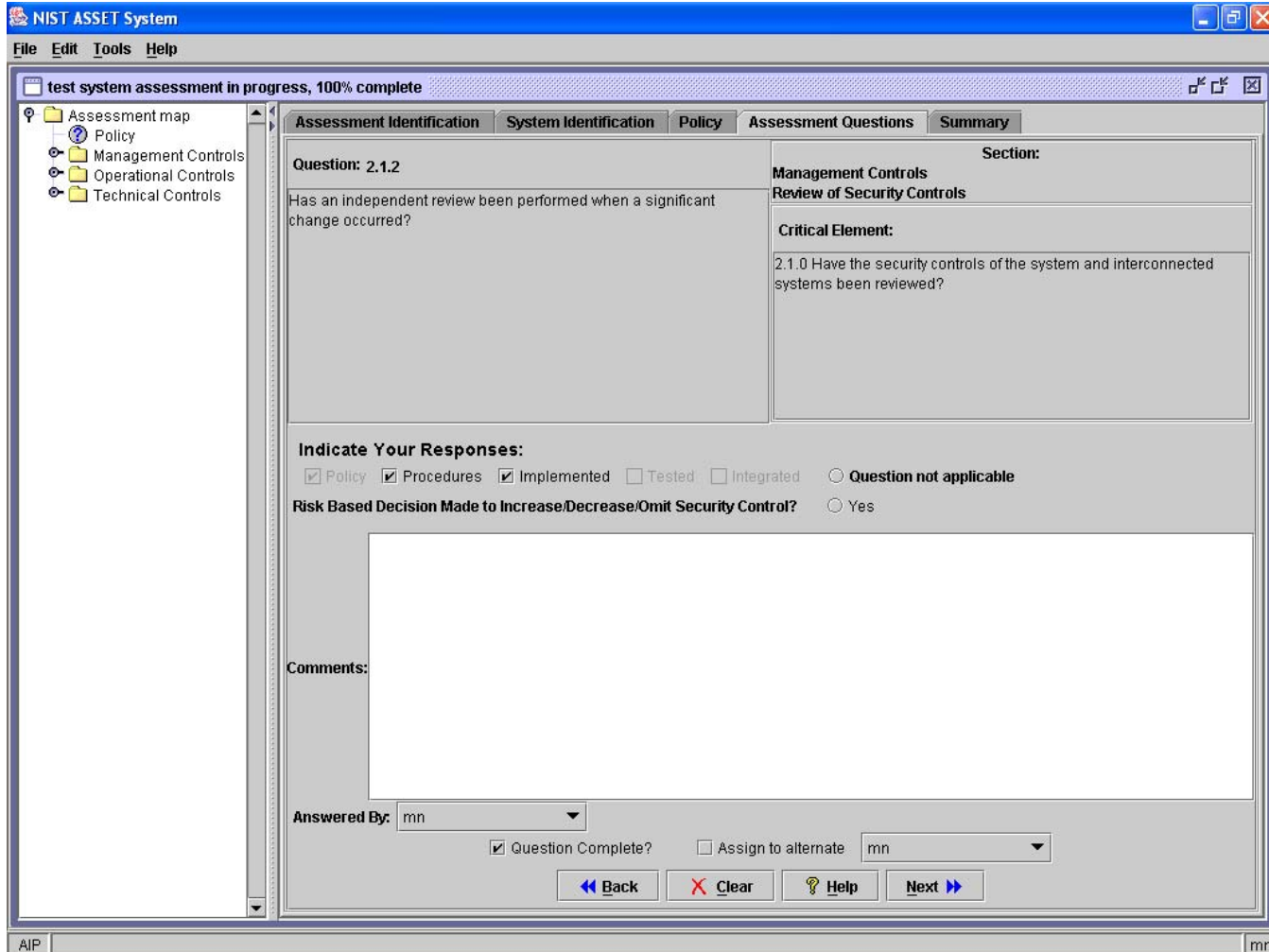
ASSET Limitations

- ◆ ASSET does not
 - ◆ Establish new security requirements or policies
 - ◆ Analyze report results
 - ◆ Directly assess system or program risk
- ◆ It is not web-based
- ◆ Users of ASSET are responsible for security of data

ASSET – System Identification



ASSET – Assessment Questions



ASSET – System Summary

NIST ASSET System

File Edit Tools Help

test system assessment in progress, 100% complete

Assessment Identification System Identification Policy Assessment Questions Summary

Current Assessment Progress: 100% complete

Critical Element Response Table:

Critical Element	N/A	Risk-based De...	Policy	Procedures	Implemented	Tested	Integrated
1.1.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.1.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.1.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.1.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.2.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.1.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.1.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.2.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.1.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.2.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.3.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.1.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.2.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.3.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.1.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.1.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11.2.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.1.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.2.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13.1.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14.1.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14.2.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15.1.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save Assessment to Database Export Assessment

AIP mn

ASSET - Reports

The screenshot shows the NIST ASSET System interface. The window title is "NIST ASSET System". The menu bar includes "File", "Edit", "Tools", and "Help". The main window is titled "ASSET Reporting" and has a toolbar with icons for file operations and help. Below the toolbar, there are two tabs: "Choose Report" and "Tabular Output".

The "Choose Report" tab is active, displaying the following information:

- Report:** Summary of topic areas by level of effectiveness
- System Name:** Human Resources
- System Number:** 1234
- Primary Assessor:** mn
- Today's Date:** Thu Aug 28 09:14:45 PDT 2003
- Confidentiality:** High
- Integrity:** High
- Availability:** Medium
- Location:** HR
- Totals:** 17 records returned

Below this information is a table with three columns: "Topic #", "Topic Area", and "Level".

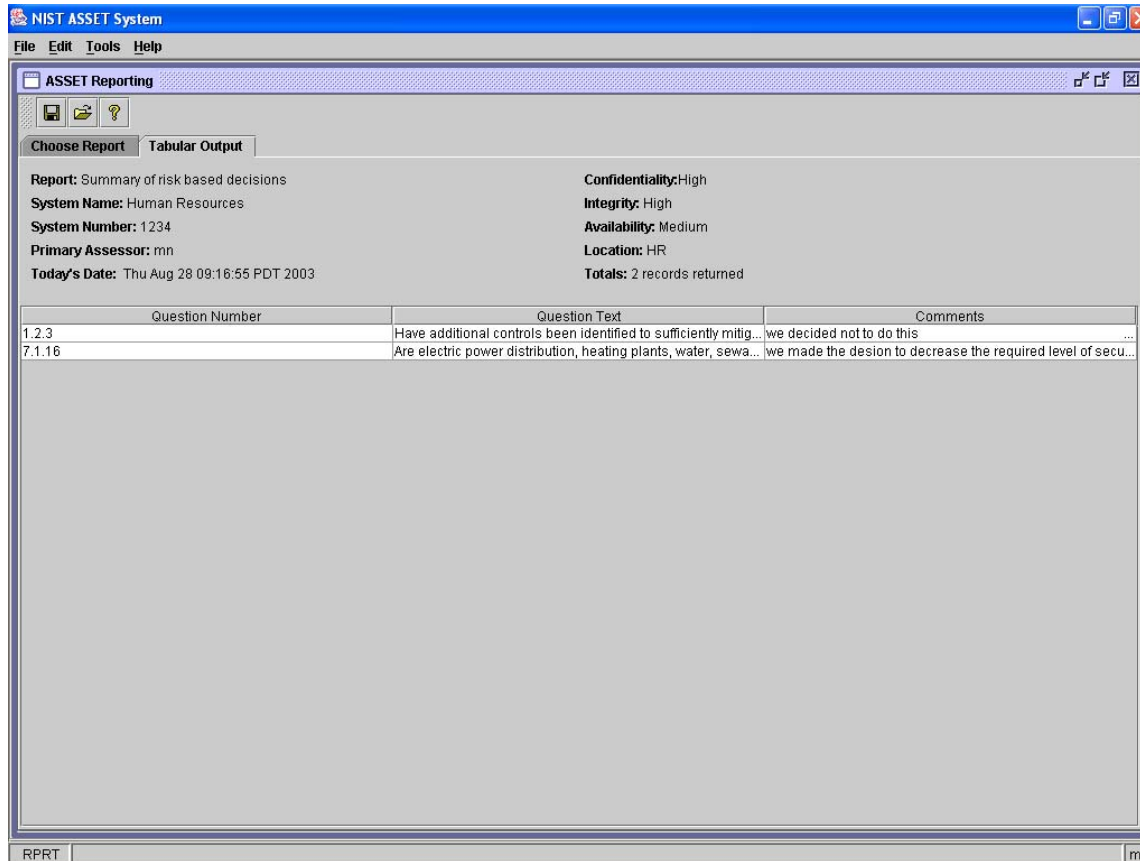
Topic #	Topic Area	Level
1.0.0	Risk Management	Policy
2.0.0	Review of Security Controls	Procedures
3.0.0	Life Cycle	Policy
4.0.0	Authorize Processing (Certification & Accreditation)	Policy
5.0.0	System Security Plan	Policy
6.0.0	Personnel Security	Tested
7.0.0	Physical and Environmental Protection	Policy
8.0.0	Production, Input/Output Controls	Policy
9.0.0	Contingency Planning	Policy
10.0.0	Hardware and System Software Maintenance	Policy
11.0.0	Data Integrity	Policy
12.0.0	Documentation	Policy
13.0.0	Security Awareness, Training, and Education	Policy
14.0.0	Incident Response Capability	Policy
15.0.0	Identification and Authentication	Policy
16.0.0	Logical Access Controls	Policy
17.0.0	Audit Trails	Policy

At the bottom of the window, the status bar shows "RPRT" on the left and "mn" on the right.

System Summary

Reports can be exported in tab-delimited format

ASSET - Reports



Summary of Risk Based Decisions

Reports can be exported in tab-delimited format



ASSET - Reports

The screenshot shows the NIST ASSET System interface. The window title is "NIST ASSET System". The menu bar includes "File", "Edit", "Tools", and "Help". The main area is titled "ASSET Reporting" and has a "Tabular Output" tab selected. The report summary includes:

- Report: List of non-applicable questions
- System Name: Human Resources
- System Number: 1234
- Primary Assessor: mn
- Today's Date: Thu Aug 28 09:16:18 PDT 2003
- Confidentiality: High
- Integrity: High
- Availability: Medium
- Location: HR
- Totals: 5 records returned

Question #	Question Text	Comments
1.1.6	Has an analysis been conducted that determines whether ...	this question does not apply to my test case ...
2.2.1	Is there an effective and timely process for reporting signifi...	we have no weaknesses ...
5.1.1	Is the system security plan approved by key affected partie...	not applicable to us ...
14.2.2	Is incident information shared with FedCIRC concerning in...	we're not a federal agency ...
14.2.3	Is incident information reported to FedCIRC, NIPC4, and lo...	does not apply to us ...

The status bar at the bottom shows "RPRT" and "mn".

Summary of Not Applicable Questions

Reports can be exported in tab-delimited format



ASSET - Reports

NIST ASSET System
 File Edit Tools Help

ASSET Reporting

Choose Report Tabular Output

Report: System Summary
 System Name: Human Resources
 System Number: 1234
 Primary Assessor: mn
 Today's Date: Thu Aug 28 09:17:22 PDT 2003

Confidentiality: High
 Integrity: High
 Availability: Medium
 Location: HR
 Totals: 225 records returned

Question #	Question Text	Level Reached	N/A	Risk Based Decis...	Comments	Answered By	Completed?	Refer To
1.1.1	Is the current syst...	Implemented	No	No		mn	Yes	N/A
1.1.2	Are risk assessm...	Procedures	No	No		mn	Yes	N/A
1.1.3	Has data sensitiv...	Tested	No	No		mn	Yes	N/A
1.1.4	Have threat sourc...	Procedures	No	No		mn	Yes	N/A
1.1.5	Has a list of know...	Integrated	No	No		mn	Yes	N/A
1.1.6	Has an analysis ...	None	Yes	No	this question doe...	mn	Yes	N/A
1.2.1	Are final risk dete...	Procedures	No	No		mn	Yes	N/A
1.2.2	Has a mission/b...	Implemented	No	No		mn	Yes	N/A
1.2.3	Have additional c...	Policy	No	Yes	we decided not to...	mn	Yes	N/A
2.1.1	Has the system a...	Procedures	No	No		mn	Yes	N/A
2.1.2	Has an independ...	Implemented	No	No		mn	Yes	N/A
2.1.3	Are routine self-a...	Implemented	No	No		mn	Yes	N/A
2.1.4	Are tests and exa...	Implemented	No	No		mn	Yes	N/A
2.1.5	Are security alerts...	Implemented	No	No		mn	Yes	N/A
2.2.1	Is there an effecti...	None	Yes	No	we have no weak...	mn	Yes	N/A
3.1.1	Is the sensitivity o...	Implemented	No	No		mn	Yes	N/A
3.1.2	Does the busine...	Procedures	No	No		mn	Yes	N/A
3.1.3	Does the Investm...	Implemented	No	No		mn	Yes	N/A
3.1.4	Are authorization...	Procedures	No	No		mn	Yes	N/A
3.1.5	Does the budget ...	Procedures	No	No		mn	Yes	N/A
3.1.6	During the syste...	Implemented	No	No		mn	Yes	N/A
3.1.7	Was an initial risk...	Integrated	No	No		mn	Yes	N/A
3.1.8	Is there a written ...	Procedures	No	No		mn	Yes	N/A
3.1.9	Are security contr...	Procedures	No	No		mn	Yes	N/A
3.1.10	Are the appropriat...	Tested	No	No		mn	Yes	N/A
3.1.11	Do the solicitatio...	Implemented	No	No		mn	Yes	N/A
3.1.12	Do the requireme...	Procedures	No	No		mn	Yes	N/A
3.2.1	Are design review...	Policy	No	No		mn	Yes	N/A

RPRT mn

Summary of Topic Areas by Level of Effectiveness

Reports can be exported in tab-delimited format

The System Security Steering Wheel

- ◆ Builds on the ASSET results to provide a graphical depiction of the overall system security posture
- ◆ Provides the ability to compare the current state with the planned state
- ◆ Provides the ability to compare the current state with industry averages to establish benchmarks

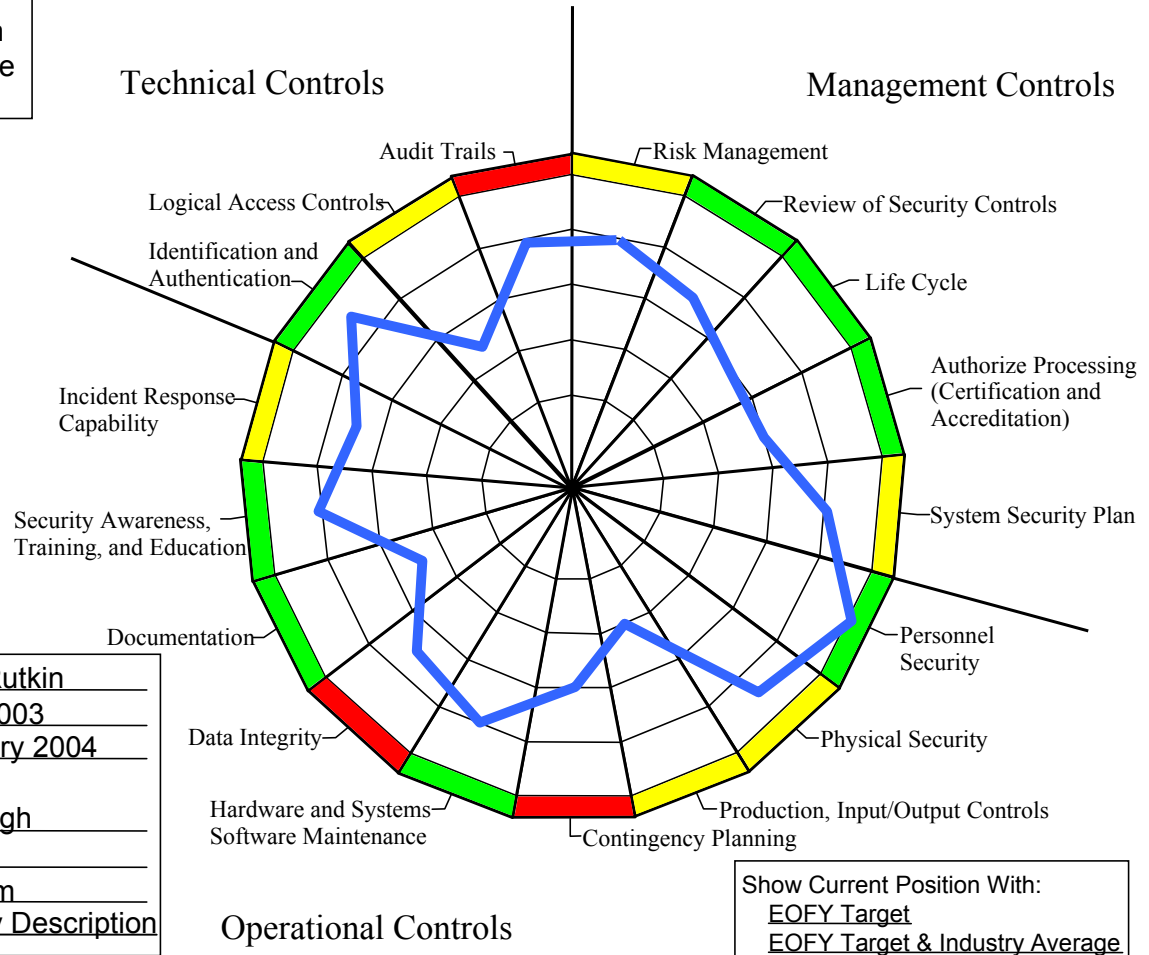
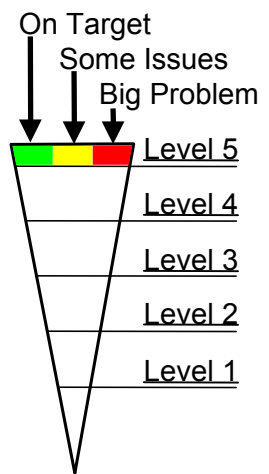


The System Security Steering Wheel

Overall System Security Posture: ●

System Name: Human Resources

— Current Position
— Industry Average
— EOFY Target



System Owner: Manny Rutkin
 Last Review Date: July 2003
 Next Review Date: January 2004
 System Sensitivity:
 Confidentiality: High
 Integrity: High
 Availability: Medium
[Link to System Boundary Description](#)

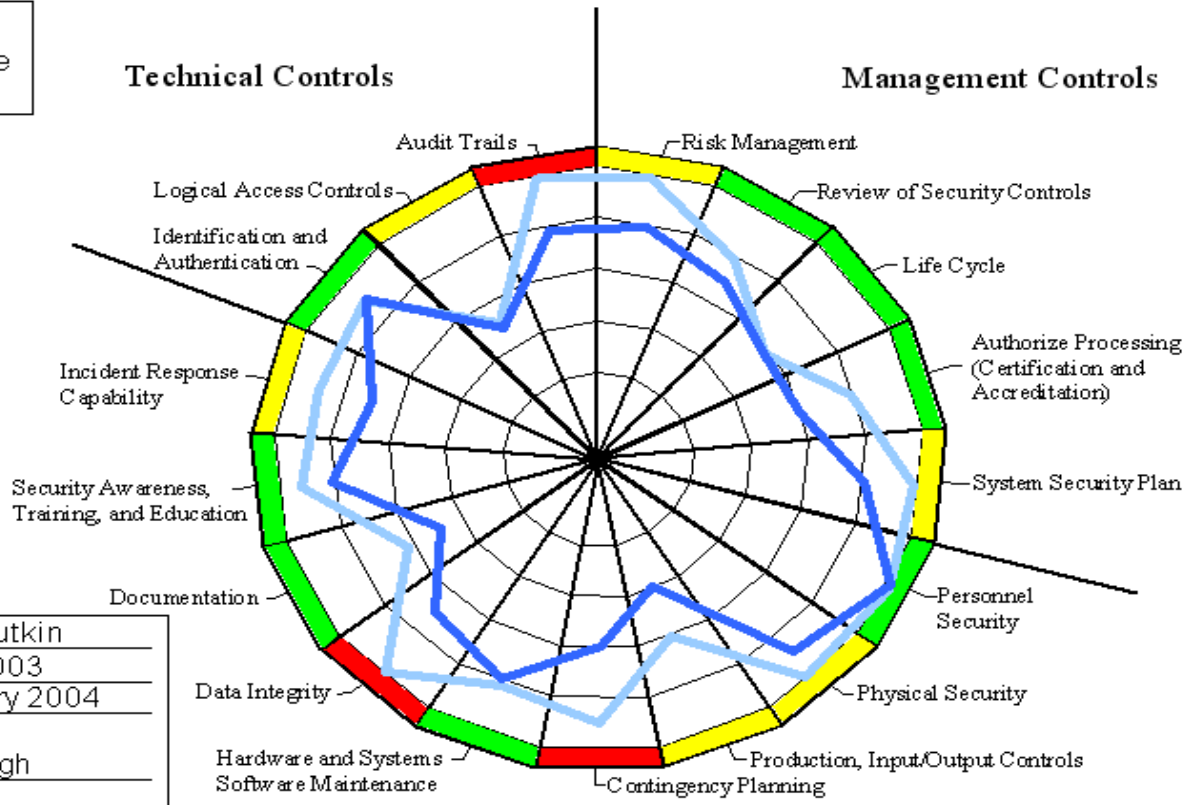
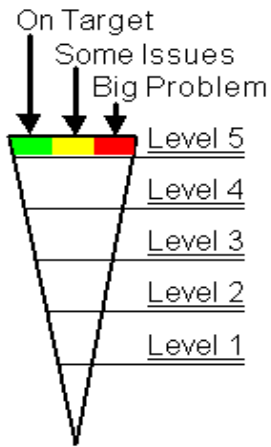
Show Current Position With:
 EOFY Target
 EOFY Target & Industry Average

The System Security Steering Wheel

Overall System Security Posture: ●

System Name: Human Resources

- Current Position
- Industry Average
- EOFY Target



System Owner: Manny Rutkin
 Last Review Date: July 2003
 Next Review Date: January 2004
 System Sensitivity:
 Confidentiality: High
 Integrity: High
 Availability: Medium
[Link to System Boundary Description](#)

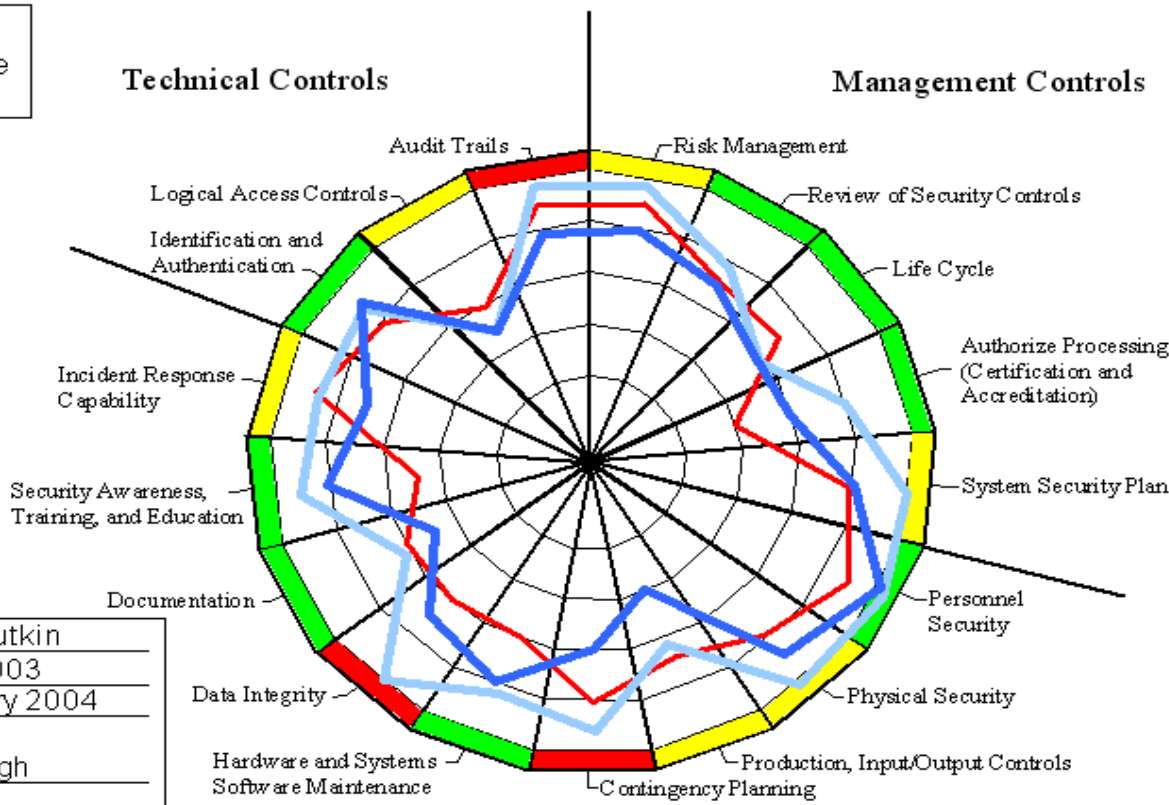
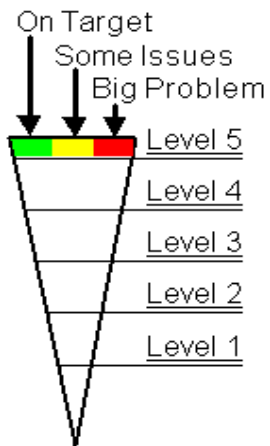
Show:
 Current Position Only
 Current Position & EOFY Target & Industry Average

The System Security Steering Wheel

Overall System Security Posture: ●

System Name: Human Resources

— Current Position
 — Industry Average
 — EOFY Target



System Owner: Manny Rutkin
 Last Review Date: July 2003
 Next Review Date: January 2004
 System Sensitivity:
 Confidentiality: High
 Integrity: High
 Availability: Medium
[Link to System Boundary Description](#)

Show:
 Current Position Only
 Current Position & EOFY Target

Steering Wheel Components

- ◆ Link to criteria for each level
- ◆ Link to System Boundary Description
- ◆ Link to Overall System Security Posture analysis
- ◆ Link to analysis pages for each control area

The Analysis Process – The “So What?”

- ◆ Detail the characteristics of the risk exposure
- ◆ What are the threats?
- ◆ What is the nature of the vulnerabilities?
- ◆ What are the implications (impact) of the vulnerabilities being exploited and the threats realized?
- ◆ A risk assessment matrix could be included

The Analysis Process – The “So, How?”

- ◆ Detail the root cause analysis for the current exposure in an attempt not to fix blame, but to understand the circumstances and make adjustments to the planning process going forward
- ◆ Was an existing process not adequately implemented?
- ◆ Is there a gap in the existing process?
- ◆ Did technology evolution outpace our security controls?
- ◆ This section may not be populated in every case



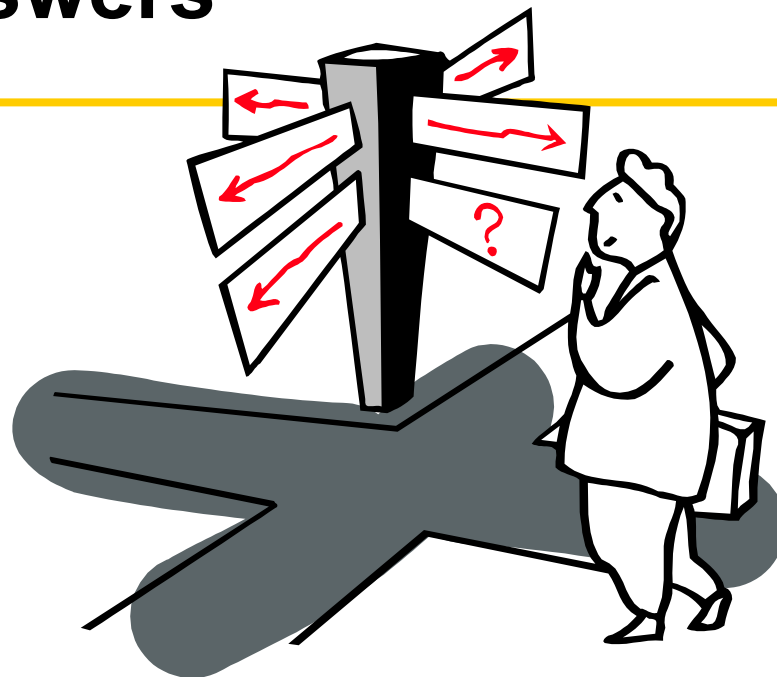
The Analysis Process – The “So, What Now?”

- ◆ Detail what’s being done to address the gap between the current state and the desired state
- ◆ Include the plan, the high level timeline, the cost forecast, and the resource requirements
- ◆ In some cases, the level of exposure represented by the gap may be such that risk-based decisions are made to defer plan implementation

Summary and Conclusions

- ◆ The NIST Information Security Governance framework provides cost effective security through:
 - ◆ The tight coupling of the security architecture to business requirements (mission)
 - ◆ Emphasizing a risk-based approach to control selection
- ◆ The framework can be adopted and adapted by all sizes of government agencies and private sector enterprises
- ◆ It encourages taking a step back to look at the “big picture” with respect to how information security enables business processes and protects the enterprise
- ◆ It does so without sacrificing the level of granularity of guidance that it takes to “make the rubber meet the road”
- ◆ It’s in the public domain!

Questions and Answers



Mike Nelson, CISA, CISM, CISSP, MBA
President – SecureNet Technologies, Inc.
Toll Free: 1-866-660-0249
mnelson@securenet-technologies.com
www.securenet-technologies.com