The Institute of Internal Auditors
Detroit Chapter
Presents

Earning CPE Credit

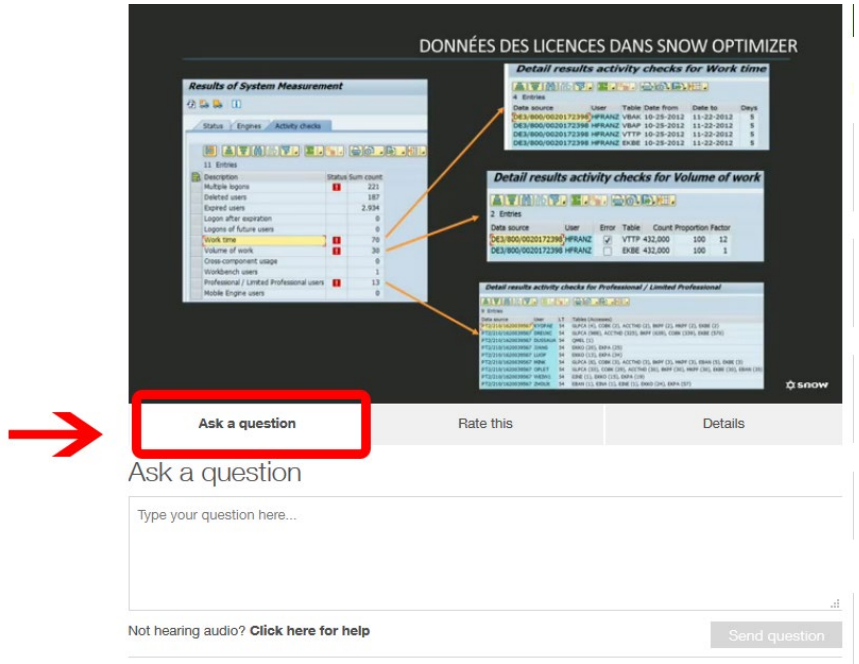
In order to receive CPE credit for this webcast, participants must:

- Attend the webcast on individual computers (one person per computer)
- Answer polling questions asked throughout the webcast
- When answering polling questions, select your answer and the click “Vote” button (next to the “Ask a Question” button) to submit / save your answer.
- CPE certificates will be sent to the e-mail address on your BrightTALK account within two weeks of this webinar.

If You Have Questions…

If you have questions during the webcast:

- **If necessary, exit Full Screen View by pressing the Esc key**
- **Submit questions through the *Ask a question button***



Polling Question:
Please tell us your member status

LEVERAGING NIST'S PUBLICATIONS TO BUILD CYBERSECURITY AUDIT PROGRAMS

PRESENTED BY: BRAD BARTON

WEBINAR ABSTRACT

As a continuation to last month's webinar where Jeff Sisolak discussed how to leverage the National Institute of Standards and Technology (NIST) library to assist in planning and development of audit strategy, this month's topic will cover select NIST publications which provide details on how to assess cyber security controls.

Whether you are an IT Auditor, Audit department leader, business manager or just personally interested in understanding IT and Security best practices, this webinar will touch on specific actions to help assess related policies, practices and procedures. Armed with this information, risk and control assessments can be developed or enhanced to help organizations align with regulatory, professional and/or industry expectations for proper and secure information technology controls.

WEBINAR PRESENTER - BRAD BARTON, CISA

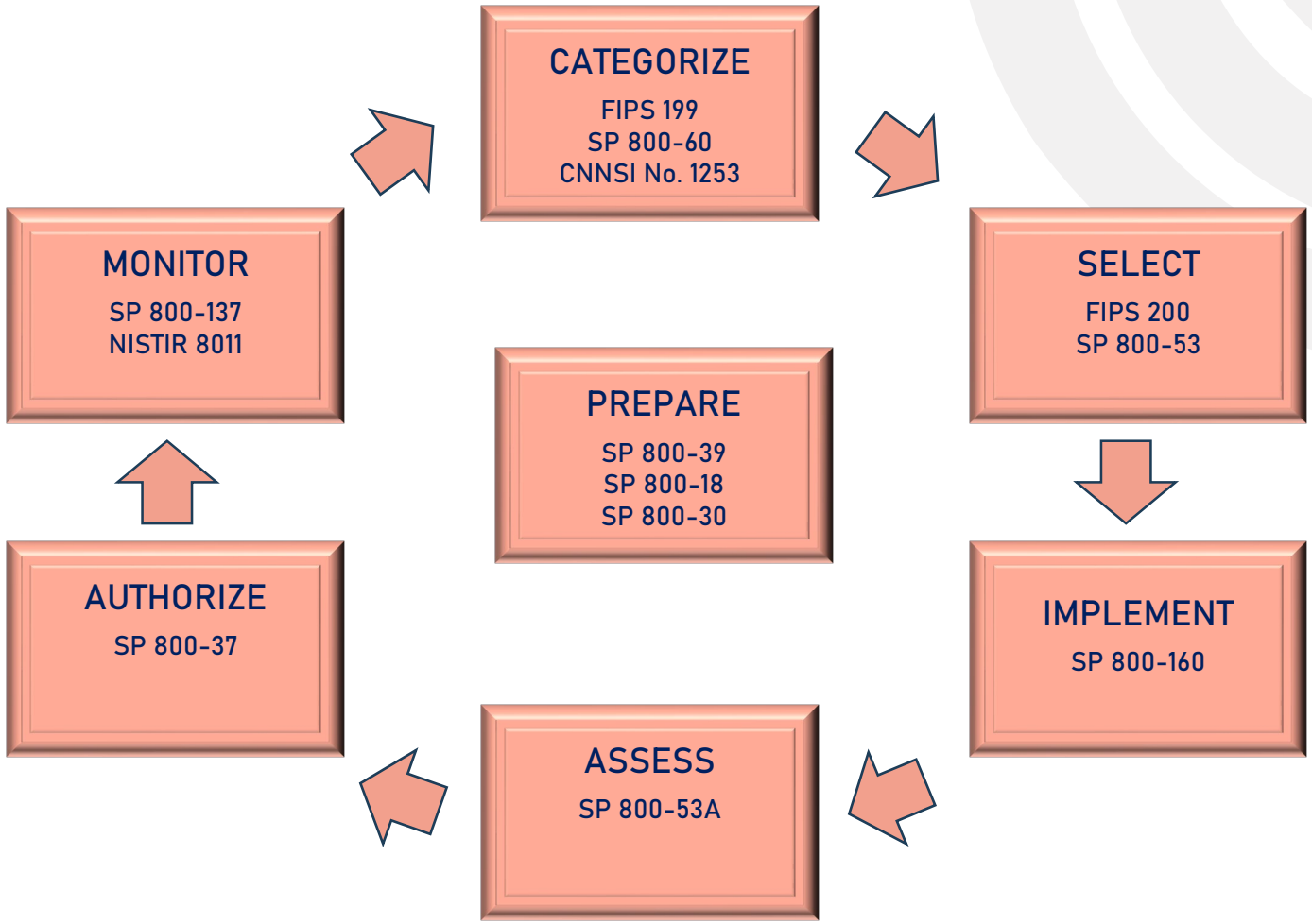
Brad is the owner of Century Governance, Risk, Compliance and Security (GRCS), a consulting company specializing in assessment of Information and Security policies, practices and procedures. He is the past Global Director of IT Governance, Compliance, Controls and Security for Lear Corporation where he provided company-wide leadership in the analysis of IT risks and implementation of related controls. This assignment included global IT Security responsibility where Brad led the implementation of the company's security policies, practices and awareness initiatives.

Brad also was Lear's Global IT Audit Director with responsibility for world-wide IT audit activities and reporting. Prior to Lear, Brad was responsible for global infrastructure, communications and IT services at Johns Manville corporation.

FEBRUARY WEBINAR RE-CAP

- Jeff Sisolak, in support of this statement: ***"To be effective, the internal auditor must see the forest for the trees"***, provided an approach for leveraging NIST publications to assist in the audit planning and strategy development process
- Jeff referenced the following as a (**Prepare**) starting point:
  - NIST Special Publication 800-39 - Managing Information Security Risk
  - NIST Special Publication 800-18 - Guide for Developing Security Plans for Federal Information Systems
  - NIST Special Publication 800-30 - Guide for Conducting Risk Assessments
- He then followed up with a walkthrough of steps: **Select, Implement, Assess, Authorize, Monitor and Categorize** referencing NIST publications to support each step

FEBRUARY WEBINAR RE-CAP



Jeff's Webinar can be viewed at: https://www.brighttalk.com/webcast/6551/384125

QUESTION #1

- Did you attend, or watch after the fact, Jeff Sisolak's February 19, 2020 Webinar: ***Seeing the Risk Management Forest for the Trees***?
  - Yes
  - No
  - No, but I am familiar with all, or most, of the referenced document and processes

LEVERAGING NIST PUBLICATIONS
A CLOSER LOOK AT THE IT SECURITY "TREES"

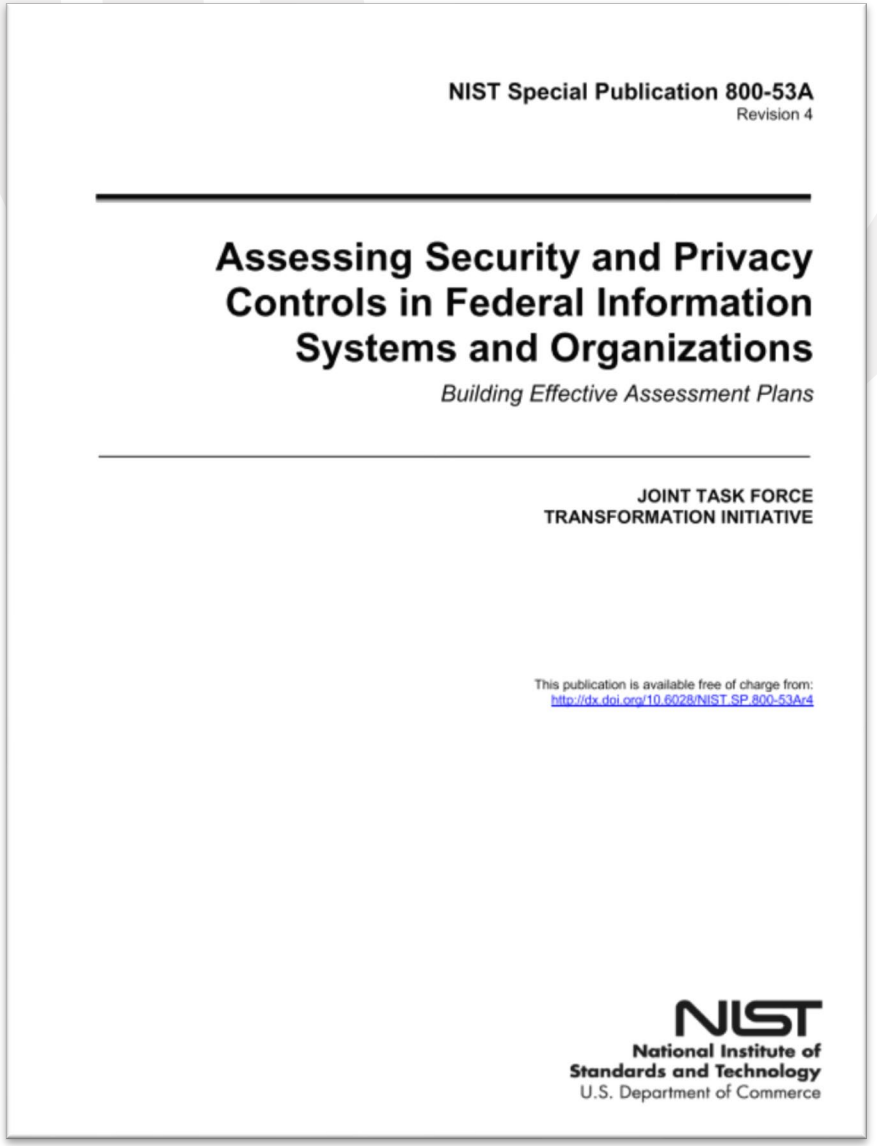
- If Jeff's advice, or other advice, guided your security audit planning and strategy, let's now move on to security audit tests/program development
- NIST provides fundamental (general) security definition and guidance docs
  - Examples:
    - SP 800-12 - An Introduction to Information Security
    - SP 800-34 - Contingency Planning Guide for Federal Information Systems
    - SP 800-35 - Guide to Information Technology Security Services
    - SP 800-53A - Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans
    - SP 800-55 - Performance Measurement Guide for Information Security
    - SP 800-70 - National Checklist Program for IT Products: Guidelines for Checklist Users and Developers
    - SP 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
    - SP 800-100 - Information Security Handbook: A Guide for Managers

LEVERAGING NIST PUBLICATIONS
A CLOSER LOOK AT THE IT SECURITY "TREES"

- NIST also provides specific (detailed) security definition and guidance docs
  - Examples:
    - SP 800-40 - Guide to Enterprise Patch Management Technologies
    - SP 800-61 - Computer Security Incident Handling Guide
    - SP 800-82 - Guide to Industrial Control Systems (ICS) Security
    - SP 800-88 - Guidelines for Media Sanitization
    - SP 800-92 - Guide to Computer Security Log Management
    - SP 800-144 - Guidelines on Security and Privacy in Public Cloud Computing
    - SP 800-150 - Guide to Cyber Threat Information Sharing
    - SP 800-167 - Guide to Application Whitelisting
    - SP 800-207 - Zero Trust Architecture (2nd Draft)

LEVERAGING NIST PUBLICATIONS

- Let’s take a closer look at one of the foundational NIST documents for reference when building your audit testing program
  - SP 800-53A - Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans



LEVERAGING NIST PUBLICATIONS - SP 800-53A

PURPOSE AND APPLICABILITY

- The purpose of this publication is to **provide a comprehensive set of procedures for assessing the effectiveness of security controls and privacy controls**.
  - Organizations can use this publication in developing viable assessment plans for producing and compiling the information necessary to **determine the effectiveness of the security and privacy controls** employed in the information system and organization.

LEVERAGING NIST PUBLICATIONS - SP 800-53A

PURPOSE AND APPLICABILITY – Cont.

- Note:
  - Like all reference documents, individual organizations must determine what applies to their operations and what degree of criticality a given risk/control might represent to their individual control needs.
    - 800-53A should be used as a starting point in the process of defining procedures for assessing the security and privacy controls, based on:
      - organizational policies and requirements,
      - known threat and vulnerabilities
      - operational considerations
      - information system and platform dependencies
      - and tolerance for risk.

LEVERAGING NIST PUBLICATIONS - SP 800-53A

ASSESSMENT METHOD DESCRIPTIONS

- Describes three assessment methods:
  - Examine - checking, inspecting, reviewing, observing, studying, or analyzing
  - Interview - conducting discussions with individuals or groups
  - Test - exercising one or more assessment objects under specified conditions to compare actual with expected behavior

- The above assessment methods utilized to:
  - support the determination of security and privacy control existence, functionality, correctness, completeness, and potential for improvement over time.

LEVERAGING NIST PUBLICATIONS - SP 800-53A

ASSESSMENT METHOD DESCRIPTIONS – Cont.

- Each of the three assessment methods include:
  - Supplemental Guidance to expand understanding, e.g. for Test method:
    - access control, identification and authentication, and audit mechanisms
    - security configuration settings
    - testing physical access control devices
    - conducting penetration testing of key information system components
    - information system backup operations
    - incident response capability
    - exercising contingency planning capability

LEVERAGING NIST PUBLICATIONS - SP 800-53A

ASSESSMENT METHOD DESCRIPTIONS – Cont.

- Additionally, each of the three assessment methods can include:
  - A **Depth attribute** to addresses the rigor and level of detail of the assessment
  - A **Coverage attribute** addresses the scope or breadth of the assessment
    - For each attribute, there's **Basic**, **Focused** and **Comprehensive** testing descriptions
    - Examples for Test:
      - Focused Depth Test - Conducted using a functional specification and limited system architectural information for determining whether the controls are implemented and free of obvious errors and whether there are increased grounds for confidence that the controls are implemented correctly and operating as intended.
      - Focused Coverage Test - uses a representative sample of assessment objects deemed particularly important to achieving the assessment objective for determining whether controls are implemented and free of obvious errors.

Note: The attribute values of depth and coverage are assigned by the organization and applied by the auditor in the execution of the assessment method against an assessment object.

QUESTION #2

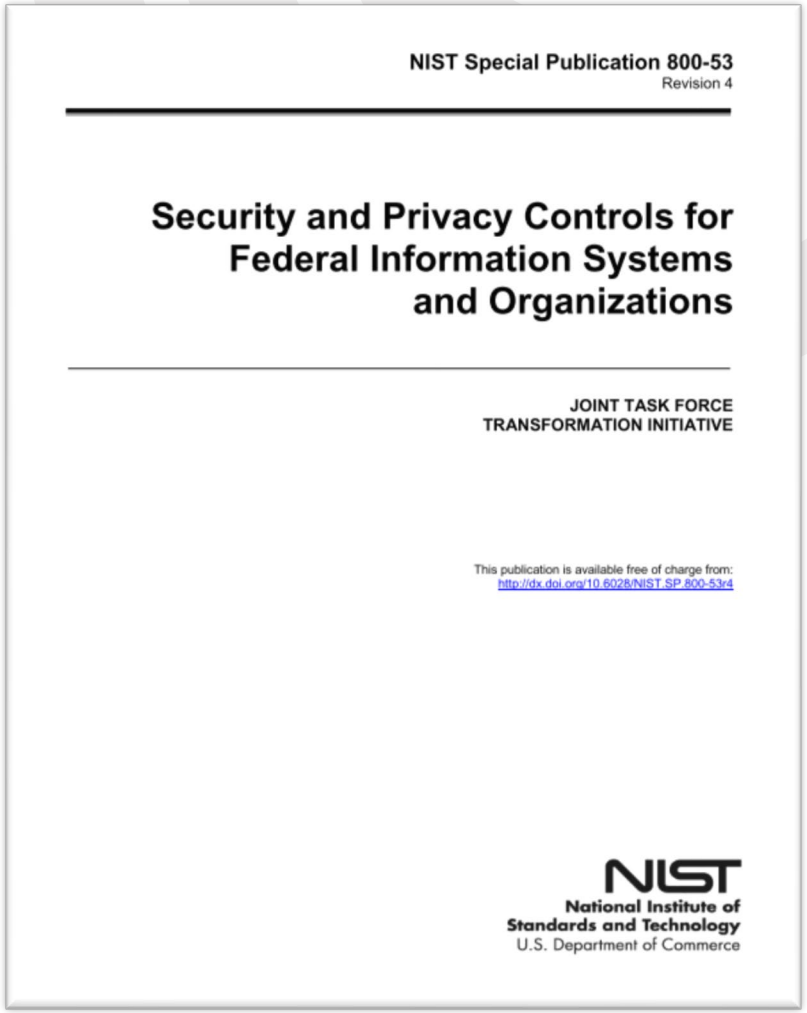
- Has your organization relied on NIST SP 800-53A as a reference for establishing/enhancing your security/privacy audit programs?

  - Yes, our programs as well aligned with NIST SP 800-53A
  - Mostly, we've aligned with NIST SP 800-53A, but rely on other sources too
  - Somewhat, we've referenced NIST 800-53A, but mostly align with other sources
  - No, we have not referenced, or chosen to align with NIST 800-53A
  - No, we don't have established security/privacy audit programs

LEVERAGING NIST PUBLICATIONS - SP 800-53A

SECURITY ASSESSMENT PROCEDURES

- Important note: SP 800-53A is directedly related to document to SP 800-53
  - SP 800-53, Appendix F, Security Controls Catalog and Appendix J, Privacy Controls Catalog contain the detailed descriptions to which SP 800-53A, Security Assessment Procedures, relate



LEVERAGING NIST PUBLICATIONS - SP 800-53A

- Short overview of SP 800-53
  - Descriptions are organized based on Control ID/Family Name

Security

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

LEVERAGING NIST PUBLICATIONS - SP 800-53A

- Short overview of SP 800-53 - Cont.
  - Descriptions are organized based on Control ID/Family Name

ID	PRIVACY CONTROLS
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal

LEVERAGING NIST PUBLICATIONS - SP 800-53A

SECURITY ASSESSMENT PROCEDURES

- Short overview of SP 800-53 - Cont.
  - Each control ID/Family (18 for Security and 4 for Privacy) consists of the following components:
    - a control section;
    - a supplemental guidance section;
    - a control enhancements section;
    - a references section; and
    - a priority and baseline allocation section

- Again, it's important to understand the relationship of SP 800-53 to SP 800-53A so that the Assessment Procedures are tied to their associated control descriptions

LEVERAGING NIST PUBLICATIONS - SP 800-53A

SECURITY ASSESSMENT PROCEDURES

- Qualifications/Advice:
  - Auditors should reference/select assessment procedures from the catalog based on the specifications of the security plan
    - Listed procedures should serve as a starting point for development of tests
    - Other assessment methods may also be needed to address a particular control objective
  - For efficiency/optimization purposes, consider:
    - Combining and consolidating assessment procedures whenever possible or practical.
    - Optimize assessment procedures by determining the best sequencing allowing for downstream reuse of testing data/documentation
  - Values selected for the **depth** and **coverage** attributes indicate the relative effort required in applying an assessment method to an assessment object

Note: The attribute values of depth and coverage are assigned by the organization and applied by the auditor in the execution of the assessment method against an assessment object.

LEVERAGING NIST PUBLICATIONS - SP 800-53A

SECURITY ASSESSMENT PROCEDURES

- For illustrative purposes, let's look at control ID/Family - Contingency Planning
  - Comparing Control specification to assessment description

CP-1	Contingency Planning Policy and Procedures
CP-2	Contingency Plan
CP-3	Contingency Training
CP-4	Contingency Plan Testing
CP-5	**Withdrawn**
CP-6	Alternate Storage Site
CP-7	Alternate Processing Site
CP-8	Telecommunications Services
CP-9	Information System Backup
CP-10	Information System Recovery and Reconstitution
CP-11	Alternate Communications Protocols
CP-12	Safe Mode
CP-13	Alternative Security Mechanisms

LEVERAGING NIST PUBLICATIONS - SP 800-53A

SECURITY ASSESSMENT PROCEDURES

- CP-1 (Contingency Policy and Procedures)
  - As specified in SP 800-53
    - The organization:
      - Develops, documents, and disseminates a contingency planning policy, and procedures to facilitate the implementation
      - Reviews and updates the Contingency planning policy, and Contingency planning procedures
  - Assessment as suggested in SP 800-53A
    - Determine if:
      - The organization develops and documents a contingency planning policy, defines personnel or roles to whom the contingency planning policy is to be disseminated, and develops and documents procedures to facilitate the implementation
      - The organization defines the frequency to review and update the current contingency planning policy, reviews and updates the current contingency plan and procedures.

LEVERAGING NIST PUBLICATIONS - SP 800-53A

SECURITY ASSESSMENT PROCEDURES

- For illustrative purposes, let's look at control ID/Family - Contingency Planning
  - A closer look at suggested assessment methods

CP-1	Contingency Planning Policy and Procedures
CP-2	Contingency Plan
CP-3	Contingency Training
CP-4	Contingency Plan Testing
CP-5	**Withdrawn**
CP-6	Alternate Storage Site
CP-7	Alternate Processing Site
CP-8	Telecommunications Services
CP-9	Information System Backup
CP-10	Information System Recovery and Reconstitution
CP-11	Alternate Communications Protocols
CP-12	Safe Mode
CP-13	Alternative Security Mechanisms

LEVERAGING NIST PUBLICATIONS - SP 800-53A

POTENTIAL ASSESSMENT METHODS

- CP-4 (Contingency Plan Testing)
  - Determine if:
    - The organization defines tests to determine the effectiveness of the contingency plan, determines organizational readiness, sets frequency to test, uses organization-defined tests, determines organizational readiness to execute the plan, reviews test results, and initiates corrective actions.
  - Assessment methods:
    - **Examine**: SELECT FROM: Contingency planning policy; procedures addressing contingency plan testing; contingency plan; security plan; contingency plan test documentation; contingency plan test results; other relevant documents or records.
    - **Interview**: SELECT FROM: Organizational personnel with responsibilities for contingency plan testing, reviewing or responding to contingency plan tests; organizational personnel with information security responsibilities.
    - **Test**: SELECT FROM: Organizational processes for contingency plan testing; automated mechanisms supporting the contingency plan and/or contingency plan testing.

LEVERAGING NIST PUBLICATIONS - SP 800-53A

BOTTOMLINE

- For any audit group who has established Security/Privacy audit programs, or who are developing programs, SP 800-53 and SP 800-53A are a readily available and well-rounded espected reference source.

QUESTION #3

- Given this overview of NIST SP 800-53A, are you now more likely to take a look at SP 800-53A to establish and/or enhance your IT Security audit programs?

  - Yes
  - No
  - No, we have already aligned with NIST 800-53A

LEVERAGING NIST PUBLICATIONS
A CLOSER LOOK AT THE IT SECURITY "TREES"

- Other NIST documents that can be useful as reference for developing/enhancing audit programs
- NIST fundamental (general) security definition and guidance docs
  - Examples:
    - SP 800-12 - An Introduction to Information Security
    - SP 800-34 - Contingency Planning Guide for Federal Information Systems
    - SP 800-35 - Guide to Information Technology Security Services
    - SP 800-55 - Performance Measurement Guide for Information Security
    - SP 800-70 - National Checklist Program for IT Products: Guidelines for Checklist Users and Developers
    - SP 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
    - SP 800-100 - Information Security Handbook: A Guide for Managers

LEVERAGING NIST PUBLICATIONS
A CLOSER LOOK AT THE IT SECURITY "TREES"

SP 800-12 - An Introduction to Information Security

- Roles and Responsibilities
  - Helpful to understand who to interview and/or who is impacted by security plan

  - Examples:
    - Risk Executive Function – Developing, supporting and overseeing the risk management strategy
    - Chief Information Officer – Allocating resources, system protections and effective implementation
    - Information Owner – Set rules for information use and protection
    - System Owner - Developing and maintaining the system security plan and operated per plan
    - Information Security Architect – Liaison between IT Engineers, system owners, security officers, etc.
    - System Administrator - Installing, configuring, and updating systems, user access, backups, etc.
    - User – Understanding and following policies, proper system use and reporting anomalies

LEVERAGING NIST PUBLICATIONS
A CLOSER LOOK AT THE IT SECURITY "TREES"

SP 800-34 - Contingency Planning Guide for Federal Information Systems

- Sample Business Impact Analysis (BIA) Template
  - Key input to Contingency and Recovery plans, and
  - Used to identify and prioritize systems and characterize impacts when unavailable
- Template elements:
  - System Description - System architecture, operating environment, physical/user location and external partnerships
  - Determine Process and System Criticality - Input from users, managers, process owners, and others to identify the automated business processes
  - Outage Impacts and Downtime - Characterizes the types of impact, e.g. Severe, Moderate or Minimal, and Maximum Tolerable Downtime, Recovery Time Objective and Recovery Point Objective
  - Resource Requirements - Hardware, software, and other resources such as data files
  - Recovery Priorities - order of recovery of system resources

LEVERAGING NIST PUBLICATIONS
A CLOSER LOOK AT THE IT SECURITY "TREES"

SP 800-35 - Guide to Information Technology Security Services

- Overview of IT Security Services
- Overview of IT Security Services Management tools
  - Metrics
  - Agreements
- Overview of Security Services Issues and Considerations
  - Strategic/Mission – Services should result in enhanced mission effectiveness
  - Funding - Focus should be on value and full life-cycle costs
  - Organizational – Damage to image and reputation, core competencies and resiliency
  - Personnel - Major ramifications could exist for current employees
  - Policy/Process - Implications to policies and process must be considered

LEVERAGING NIST PUBLICATIONS
A CLOSER LOOK AT THE IT SECURITY "TREES"

SP 800-55 - Performance Measurement Guide for Information Security

- Measures Template and Instructions
  - Goal - Strategic and/or information security goal
  - Measure - numeric statement of measurement, e.g. percentage, frequency, average, or similar term
  - Type - Whether the measure is implementation, effectiveness/efficiency, or impact
  - Formula - Calculation to be performed that results in a numeric expression
  - Implementation Evidence – That used to compute, validate and identify probable causes
  - Frequency - How often the data is collected, analyzed and reported
  - Responsible Parties – Key Stakeholders
  - Data Source - Location of the data to be used in calculating the measure
  - Reporting Format - How the measure will be reported, e.g. pie chart, line chart, bar graph or other

LEVERAGING NIST PUBLICATIONS
A CLOSER LOOK AT THE IT SECURITY "TREES"

SP 800-70 - National Checklist Program for IT Products: Guidelines for Checklist Users and Developers

- Provides a full description of the National Checklist Program (NCP)
- The NCP is:
  - A repository of publicly available security checklists, a.k.a.:
    - lockdown guides, hardening guides, security guides, security technical implementation guides, or benchmarks
  - Provides detailed guidance on setting the security configuration of operating systems and applications
  - Lists for over 500 configurations, e.g. Apache Servers, Mac OS, Cisco IOS, Linux Distros, Android, Juniper, Microsoft OS/Apps, Oracle, VMware, and more

LEVERAGING NIST PUBLICATIONS
A CLOSER LOOK AT THE IT SECURITY "TREES"

SP 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

- Provides multiple examples of test and testing facilitation guidance, e.g.:
  - Master Scenario Events List
    - Key scenario events
    - Expected actions
    - Objectives
  - Example:

Master Scenario Events List

Event #	MSEL Key Event Description	Expected Actions Resulting from MSEL Event	Objectives
1	***Example*** The [*insert organization name*] experiences electronic intrusions on critical information systems.	***Example*** Supporting Injects: Day 1, 0900 - 1700 ■ Activate cyber incident response team ■ Implement Cyber Intrusion Response Plan ■ Notify and coordinate with customers and other stakeholders ■ Take actions to clean infected systems	***Example*** ■ Familiarize staff with responsibilities under Cyber Intrusion Response Plan ■ Validate Cyber Intrusion Response Plan ■ Coordinate with Federal cyber entities, customers, and key stakeholders

LEVERAGING NIST PUBLICATIONS
A CLOSER LOOK AT THE IT SECURITY "TREES"

SP 800-100 - Information Security Handbook: A Guide for Managers

- Provides a broad overview of information security program elements
  - Helpful to assist interested parties in understanding how to establish and implement an information security program
- Highlights:
  - Information Security Governance
  - Awareness and Training
  - Performance Measures
  - Security Planning
  - Security Services and Products Acquisition
  - Incident Response

LEVERAGING NIST PUBLICATIONS
A CLOSER LOOK AT THE IT SECURITY "TREES"

The NIST library contains many documents that can be useful in development or enhancement of IT Security Audit Programs

- A few previously shown include:
  - SP 800-40 - Guide to Enterprise Patch Management Technologies
  - SP 800-61 - Computer Security Incident Handling Guide
  - SP 800-82 - Guide to Industrial Control Systems (ICS) Security
  - SP 800-88 - Guidelines for Media Sanitization
  - SP 800-92 - Guide to Computer Security Log Management
  - SP 800-144 - Guidelines on Security and Privacy in Public Cloud Computing
  - SP 800-150 - Guide to Cyber Threat Information Sharing
  - SP 800-167 - Guide to Application Whitelisting
  - SP 800-207 - Zero Trust Architecture (2nd Draft)

LEVERAGING NIST PUBLICATIONS
A CLOSER LOOK AT THE IT SECURITY "TREES"

In Summary:

- If you have a solid IT Security Audit plan and strategy* NIST can supply direct guidance for development of audit testing (SP 800-53A), and
- NIST can provide several documents which provide:
  - Education
  - Checklists
  - Standards
  - Templates
  - References
  - Examples and More

QUESTION #4

- Would you like to hear more in the future on how NIST can be leverage to establish or enhance audit plans/programs?
  - Yes, these NIST overviews are helpful
  - Yes, however, focus on individual NIST documents (deep dive) as opposed to overviews
  - No, I've heard enough about NIST

Questions

THANKS FOR ATTENDING

Brad Barton’s contact Info:

Email: bbarton424@gmail.com

Phone: 248-707-9372