Evaluating System Controls Using a Risk Assessment Approach – Day 1
Evaluating System Controls – Day 1

Agenda

1. Risk Assessment – Preparation
2. Loss Risks – Finding Effect
3. Risk Controls Evaluation – Finding Conditions
Evaluating System Controls – Day 1

1. Risk Assessment Preparation
   • Obtaining General System Information
   • System Owner
   • System Purpose: Donor System
   • System Users
   • System Design and Architecture
   • Data Type
   • Regulatory Compliance Requirements
Evaluating System Controls – Day 1

1. Risk Assessment Preparation

Obtaining General System Information - Key Information to Obtain and Understand

- Who owns the application and what mission operations does it support?
- What type of data is hosted, created, or passes through the application?
- Who owns the data?
- Who are the users of the system – internal users, external users?
- Which IT organization provides Sys Admin and Security?
1. Risk Assessment Preparation

System Owner - owner should be a business leader for which the application supports the business or mission operations

Key Audit Purpose

• Without a clear application owner, responsibility for ensuring system is designed, secured, meets regulatory requirements, and system users are approved to access and use the application
Evaluating System Controls – Day 1

1. **Risk Assessment Preparation**

What type of data is hosted, created, or passes through the application

**Key Audit Purpose**

- Knowing the type of data stored within/through the application will assist in designing the audit objectives, audit steps, and internal control questionnaire (ICQ)

- Data may or may not be owned by the organization and therefore may have external contractual requirements and protection controls that will need to be incorporated into the ICQ.
Evaluating System Controls – Day 1

1. **Risk Assessment Preparation** - Who are the users of the system – internal users, external users?

Two types of users Regular/general and privileged

- Regular/general users are users who use the application for business purposes
  - Input data, obtain data reports, extract data, process data for business purposes
- Privileged users are typically of two types Application support admins and application infrastructure admins
  - Application admins – these users provide support in provisioning application user accounts, adhoc report creations, managing roles and permissions of user accounts
  - Application infrastructure admins – these users provide system administration support at the infrastructure level
- Infrastructure level is the operating systems, application, databases, web services, network routers, etc...
  - System admins are the server administrators, database administrators, network administrators

**Key Audit Purpose**

- Need to gain an understanding of who uses the application?
- Are there different roles for different user types?
- How are users granted, monitored, and removed from the application...this is called access provisioning..
Risk Associated With Failure/Ineffective Operation of Key Application Security Controls

<table>
<thead>
<tr>
<th>Key Application Security Controls</th>
<th>Unauthorised Access</th>
<th>Inappropriate Access/ Violation of SoD</th>
<th>Ineffective Security Management Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of unique/individual user accounts</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Access rights granted according to ‘least privilege’ principle</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strong password controls</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Segregation of duties principle followed during user provisioning</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Periodic management review of appropriateness of user access rights</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Periodic review of application users against authorisation records</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Security administration function independent of application support function</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Authorisation for grant of privileged and service (interactive) accounts</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Periodic monitoring over activities performed through privileged and service (interactive) accounts</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Regular monitoring of audit logs</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Timeliness of security administration function</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
Evaluating System Controls – Day 1

1. **Risk Assessment Preparation - System Design and Architecture**
Evaluating System Controls – Day 1

1. **Risk Assessment Preparation** – System Design and Architecture
   Information to gather and understand:
   - Virtual or hardware environment or both?
   - Is the application multi-tier?
   - Is access provided through the Internet or only within the intranet?
   - Is there two-factor authentication used?
   - Obtain inventory of all infrastructure components

   **Key Audit Purpose**
   Understanding the system and its architecture will assist in:
   - Identifying the complexity of the application
   - Assist in planning the security testing to be performed
   - Assist in planning access control testing
   - Assist in general application controls testing – backup and recovery, change and configuration management, user access controls, etc...

Copyright © SysAudits. All rights reserved.
Evaluating System Controls – Day 1

- Web application architecture is all about learning how to build a stable ecosystem for your web applications. It involves learning about infrastructure, what works the best and what kind of tools you need to make it all come together.

- The typical structure of a Web application is:
  - The presentation layer usually includes UI and presentation logic components
  - The business layer usually includes business logic, business work-flow and business entities components
  - The data layer usually includes data access and service agent components
N-Tier Architecture – Significance of Tiers

• N-Tier architectures have the same components
  – Presentation
  – Business / Logic
  – Data
Evaluating System Controls – Day 1

1 – Tier Architecture
1 – Tier Architecture

• All 3 layers are on the same machine
  – All code and processing is kept on a single machine

• Presentation, Logic, Data Layers are tightly connected
  – Scalability: Single processor means hard to increase volume of processing
  – Portability: Moving to a new machine may mean re-writing everything
  – Maintenance: Changing one layer requires changing other layers
Evaluating System Controls – Day 1

2 – Tier Architecture

[Diagram of a 2-tier architecture with layers labeled 'Presentation logic', 'Business logic', 'Data Access logic', and a 'Database']

Copyright © SysAudits. All rights reserved.
Evaluating System Controls – Day 1

2 – Tier Architecture

• Database runs on Server
  – Separated from client
  – Easy to shift to a different database

• Presentation and Logic layers still tightly connected
  – Heavy Load on Server
  – Potential congestion on network
  – Presentation still tied to business logic
Evaluating System Controls – Day 1

3 – Tier Architecture
Evaluating System Controls – Day 1

3 – Tier Architecture

- Each layer can potentially run on a different machine
- Presentation, logic, data layers disconnected
A Typical 3-tier Architecture

Architecture Principles:

- Client-Server architecture
- Each tier (Presentation, Logic, Data) should be independent and should not expose dependencies related to the implementation
- Unconnected tiers should not communicate
- Change in platform affects only the layer running on that particular platform
A Typical 3-tier Architecture

Presentation Layer:
- Provide user interface
- Handles the interaction with the user
- Sometimes called the GUI or client view or front-end
- Should not contain business logic or data access code
A Typical 3-tier Architecture

Logic Layer:
- The set of rules for processing information
- Can accommodate many users
- Sometimes called middleware / back-end
- Should not contain presentation or data access code
A Typical 3-tier Architecture

Data Layer:
- The physical storage layer for data persistence
- Manages access to DB or file system
- Sometimes called back-end
- Should not contain presentation or business logic code
3-tier Architecture Example

This is an example of simple 3-Tier Architecture

Web-browser with web-server renders the front-end screens making it the Presentation Layer

The data to be displayed on the front-end is computed by Application Servers based on Business logic. This makes the Business layer

The computed data and the raw data as per the requirement is stored in the Data Server and retrieved using DBMS queries. This is the Data Layer
3-tier Architecture Example

- This example talks of the technologies that can be used to code the various layers of a 3-Tier Architecture.
Evaluating System Controls – Day 1

3-tier Architecture Advantages

• Independence of Layers
  – Easier to maintain
  – Components are reusable
  – Faster development (division of work)
    • Web designer does presentation
    • Software engineer does logic
    • DB Admin does data model
Evaluating System Controls – Day 1

1. **Risk Assessment Preparation - Regulatory Compliance Requirements**

Need to obtain and understand application data, organization policies, regulatory compliance requirements, and any contractual requirements for data protection and restrictions.
Evaluating System Controls – Day 1

2. Loss Risks- finding effect
• Impact of data compromise/integrity
• Reputation Risk
• Non-Compliance Risks
• Liability Risk
• Loss of Revenue or Services
• System unavailable
• Data Compromise is Deemed Highest Risk
Evaluating System Controls – Day 1

2. Loss Risks- finding effect
   • Impact of data compromise

   • The compromise of data can have a significant impact on an organization
     – Non-compliance to policies, regulatory, PCI, HIPAA
     – Liability and fines
     – Reputation risk
     – Loss of revenue and or services

These are the effects to your findings

Copyright © SysAudits. All rights reserved.
Evaluating System Controls – Day 1

3. Risk Controls Evaluation – finding conditions

- Infrastructure Controls
  - Operating System Controls
  - Database Controls
  - Web Controls
  - Network Controls
Evaluating System Controls – Day 1

3. Risk Controls Evaluation – finding conditions

• Infrastructure Controls
  – Operating System Controls
    • Secure configuration and limited access controls
    • Change and configuration management processes
    • What secure standards are being used?
Evaluating System Controls – Day 1

3. Risk Controls Evaluation – finding conditions

- Infrastructure Controls
  - Database Controls
    - Secure configuration and limited access controls
    - Change and configuration management processes
    - What secure standards are being used
Evaluating System Controls – Day 1

3. Risk Controls Evaluation – finding conditions

• Infrastructure Controls
  – Web Controls
    • Secure configuration and limited access controls
    • Change and configuration management processes
    • What secure standards are being used

Copyright © SysAudits. All rights reserved.
Evaluating System Controls – Day 1

3. Risk Controls Evaluation – finding conditions

• Infrastructure Controls
  – Network Controls
    • Secure configuration and limited access controls
    • Change and configuration management processes
    • What secure standards are being used
Evaluating System Controls – Day 1

3. General Controls
   – Access Controls
   – Data Protection Controls
   – System Continuity Controls
   – Monitoring Controls
Evaluating System Controls – Day 1

3. General Controls

– Access Controls

– Assess different user types and determine how user provisioning process operates

– How are privileged users granted access, being monitored, and validated access
Evaluating System Controls – Day 1

3. General Controls

– Data Protection Controls

• Understanding the data assists in designing ICQ assessments

• Has a Privacy Impact Assessment (PIA) been performed
  – This assists in determining data protection controls
Evaluating System Controls – Day 1

3. General Controls

– System Continuity Controls
– This would include understanding backup and recovery processes
– Has a Business Continuity Assessment and Plan (BCP) been performed involving the application?
– What is the priority of the application within the organization Disaster Recovery Plan (DRP)?
Evaluating System Controls – Day 1

3. General Controls

– Monitoring Controls

• Assessing the system architecture will assist in determining if the application has protections for

• Intrusion Detection Protection – detects anomalies and activity and can log, report, and block depending on solution deployed

• Intrusion Prevention System – detects anomalies and prevents automatically
Evaluating System Controls – Day 1

These are only a few IT Risk Assessments to be Considered

Questions??

Copyright © SysAudits. All rights reserved.
Evaluating System Controls – Day 2

Agenda - Audit Design and Testing

Access Controls - Concentration
• Non-Privileged Accounts
• Application Accounts
• Privileged Accounts
• Service and Database Accounts
• IDS and IPS
• SIEMs
• Application Controls

Copyright © SysAudits. All rights reserved.
Evaluating System Controls – Day 2

Access Controls - Concentration

Non-Privileged Accounts

• Key controls for non-privileged accounts:
  – Process for evaluating the provisioning of users.
  – Approval process, roles and permissions needed, monitoring, and removals.
Evaluating System Controls – Day 2

Access Controls – Concentration

• Privileged Accounts and Service and Database Accounts

• Key controls for privileged accounts:
  – Process for evaluating the provisioning of users.
  – Approval process, roles and permissions needed, monitoring, removals, and recertification.

• Key controls for application/service accounts:
  • these accounts should not be allowed to act as a user or interactive account;
  • comply with password change policy; restricted, logged, and monitored
Evaluating System Controls – Day 2

Monitoring Controls Concentration
• Infrastructure Controls
• Operating Systems
• Databases
• Network Firewalls and Routers
• Network IPS and IDS
• SIEM Log Correlation
• Incident Handling/Response and Event Management
Evaluating System Controls – Day 2

Monitoring Controls Concentration

• Infrastructure Controls
  – Operating Systems
  – Databases

• Controls to assess include OS and DB hardening settings based on an industry standard such as Center for Internet Security, DOD STIG, others

• Auditing and logging of critical files and directories
• Auditing and logging of account activities – successful/unsuccessful logins

Copyright © SysAudits. All rights reserved.
Evaluating System Controls – Day 2

Monitoring Controls Concentration

• Network Firewalls, Routers, IPS, and IDS

• Controls to assess include network hardening settings based on an industry standard such as Center for Internet Security, DOD STIG, others

• Auditing and logging of privileged account activities – successful/unsuccessful logins

• Assess deployment and monitor sensing of firewall, router, IPS, and IDS sensors

Copyright © SysAudits. All rights reserved.
Evaluating System Controls – Day 2

IDS works with a copy of the traffic.

- It can detect an attack and send an alert (and take other actions), but it cannot prevent the attack because it does not operate on traffic inline in the forwarding path.
Evaluating System Controls – Day 2

• IPS device operates in inline mode i.e. because the IPS device is in the actual traffic path.

• This makes the device more effective against worms and atomic attacks (attacks that are carried out by a single packet).
IDS vs IPS

IDS usually records information related to an observed malicious event and notifies security administrators of events.

IPS is considered an IDS extension because they both monitor network traffic and system activities for malicious activity.

But unlike IDS, IPS are able to actively prevent/block intrusions that are detected.
Evaluating System Controls – Day 2

IPS Vs. Firewall

IPS monitors the system for unwanted entry and reports or alerts the same to the user and prevents the connection.

A firewall monitors the system based on the rules that are set by the user and regulates the activity between the system and the Internet.

Therefore, to protect the system from unwanted intrusions, it is always recommended to use firewalls in conjunction with Intrusion Prevention Systems (IPS).

This is also why the majority of internet security systems comes with both firewall and IPS.
Evaluating System Controls – Day 2

Key Audit point:

• Determine which are deployed

• What technology, version, and settings are enabled

• Not a lot of standardization similar to an OS, DB, NW device, you usually need to obtain the vendor deployment guide and make your own assessment guide
Evaluating System Controls – Day 2

Monitoring Controls Concentration

• SIEM Log Correlation, and Incident Handling/Response and Event Management

• Assessment of where all audits and logs collection and correlation.
A SIEM system collects logs and other security-related documentation for analysis.

Most SIEM systems work by deploying multiple collection agents to gather security-related events from end-user devices, servers, network equipment -- and even specialized security equipment like firewalls, antivirus or intrusion prevention systems.

The collectors forward events to a centralized management console, which performs inspections and flags anomalies.

To allow the system to identify anomalous events, it’s important that the SIEM administrator first creates a profile of the system under normal event conditions.
Evaluating System Controls – Day 2
Evaluating System Controls – Day 2

Enough logs

External alerts

SIEM system

Reports

Alerts

Forensics and troubleshooting
Evaluating System Controls – Day 2

**Monitor everything**
Logs, network traffic, user activity

**Correlate intelligently**
Connect the dots of disparate activity

**Detect anomalies**
Unusual yet hidden behavior

**Prioritize for action**
Attack high-priority incidents
1. Risk Assessment Preparation - Application Security Layers

Figure 1—Application Security Layered Approach

Copyright © SysAudits. All rights reserved.
<table>
<thead>
<tr>
<th>Tier</th>
<th>Tool</th>
<th>Purpose/Method</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Server</td>
<td>1. Port Scanner – Super Scan, NMAP</td>
<td>1. Identify open ports and services</td>
<td>Vulnerability scan reports.</td>
</tr>
<tr>
<td></td>
<td>3. Compliance Assessor – Nessus, SCAP</td>
<td>3. Assess web application configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Nikto</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Port Scanner – Super Scan, NMAP</td>
<td>1. Identify open ports and services</td>
<td>1. Identify open ports and services</td>
</tr>
<tr>
<td></td>
<td>3. Compliance Assessor – Nessus, SCAP</td>
<td>3. Custom assessment based on application deployment documentation</td>
<td></td>
</tr>
<tr>
<td>Application Server</td>
<td>1. Port Scanner – Super Scan, NMAP</td>
<td>1. Identify open ports and services</td>
<td>1. Identify open ports and services</td>
</tr>
<tr>
<td></td>
<td>3. Compliance Assessor – Nessus, SCAP</td>
<td>3. Custom assessment based on application deployment documentation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Custom Configuration Assessments</td>
<td>1. Identify open ports and services</td>
<td>1. Identify open ports and services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Best practice custom configuration</td>
<td>2. Best practice custom configuration</td>
</tr>
<tr>
<td>Database Server</td>
<td>1. Port Scanner – Super Scan, NMAP</td>
<td>1. Identify open ports and services</td>
<td>1. Identify open ports and services</td>
</tr>
<tr>
<td></td>
<td>3. Compliance Assessor – Nessus, SCAP</td>
<td>3. Assess database application configuration (assess the DB application and each DB instance if possible)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Custom Configuration Assessments</td>
<td>1. Identify open ports and services</td>
<td>1. Identify open ports and services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Best practice custom configuration</td>
<td>2. Best practice custom configuration</td>
</tr>
<tr>
<td></td>
<td>1. Custom Configuration Assessments</td>
<td>1. Identify open ports and services</td>
<td>1. Identify open ports and services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Best practice custom configuration</td>
<td>2. Best practice custom configuration</td>
</tr>
<tr>
<td></td>
<td>1. Port Scanner – Super Scan, NMAP</td>
<td>1. Identify open ports and services</td>
<td>1. Identify open ports and services</td>
</tr>
<tr>
<td></td>
<td>2. Custom Configuration Assessments</td>
<td>2. Best practice custom configuration</td>
<td>2. Best practice custom configuration</td>
</tr>
<tr>
<td>Data Storage</td>
<td>1. Port Scanner – Super Scan, NMAP</td>
<td>1. Identify open ports and services</td>
<td>1. Identify open ports and services</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>Compliance assessor – Nessus, SCAP</td>
<td>Assess best practices OS security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Devices</td>
<td>1. Super Scan and NMAP</td>
<td>Assess Best Practice NW Device Security</td>
<td>1. Identify open ports and services</td>
</tr>
<tr>
<td></td>
<td>2. Vulnerability Scanner – Nessus, CISCO Scanner</td>
<td>Assess Best Practice NW Device Security</td>
<td>2. Best practice configuration</td>
</tr>
<tr>
<td>Network Devices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Custom Review</td>
<td>Assess best practice configuration</td>
<td>Best practices</td>
</tr>
<tr>
<td>Firewalls/Proxy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewalls/Proxy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewalls/Proxy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interconnected</td>
<td>Custom Review</td>
<td>Review interconnection agreement</td>
<td>Agreement, system design</td>
</tr>
<tr>
<td>Systems</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Observe, obtain, and inspect password configurations, and obtain the query used to generate the password configurations, to determine whether they are in compliance with NIST SP 800-53 requirements and:

- are not displayed when entered;
- are changed periodically (e.g., every 30 to 90 days);
- contain alphanumeric and special characters;
- are sufficiently long (e.g., at least 8 characters in length);
- have lifetime restrictions (automatically expire);
- are prohibited from reuse for a specified period of time (e.g., at least 6 generations); and
- are not the same as the user ID

contain a lockout setting for invalid attempts in accordance with NIST requirements

- Check whether the above password protection rules are followed or not.
**Control Activity:** AC-2.1. Users are appropriately identified and authenticated.

**Control Technique:** AC-2.1.12. Use of and access to authenticators is controlled (e.g., their use is not shared with other users).

Topics covered include:

- Observe, obtain, and inspect system passwords and account IDs and obtain the query used to generate the listing to determine the listing contains a complete and accurate listing of all system passwords and accounts—check if the system accounts are compromised or not.

- Select a sample of accounts and passwords to determine if shared and/or generic accounts exist. If shared/generic accounts and/or passwords exist, inquire of management and inspect established policy and procedures to determine appropriateness—check whether users are sharing their credential with other not. If so check the company policy.
Control Activity: AC-4.1. Access to sensitive system resources is restricted and monitored.

Control Technique: AC-4.1.1. Access to sensitive/privileged accounts is restricted to individuals or processes having a legitimate need for the purposes of accomplishing a valid business purpose.

Topics covered include:

Observe, obtain, and inspect a listing of all production privileged accounts – check access to sensitive accounts are restricted or not.

Inspect a selection of privileged accounts and determine if access is reviewed and approved, and if the reason for access is captured through account request documents or another means – check whether if anybody is given access to privileges accounts its documented or not.
Control Activity: AC-4.1. Access to sensitive system resources is restricted and monitored.

Control Technique: AC-4.1.2. Use of sensitive/privileged accounts is adequately monitored.

Topics covered include:

• Observe, obtain, and inspect a listing of all production privileged accounts – gather a list of all the privilege accounts.

• Inspect a selection of privileged accounts and determine if access is being monitored, and evaluate the effectiveness of monitoring procedures – check whether the usage of privilege accounts are properly monitored or not.
• **Control Activity:** CM-2.1. Current configuration identification information is maintained.

• **Control Technique:** CM-2.1.1. A current and comprehensive baseline inventory of hardware, software, and firmware is documented, backed up, and protected.

Information system documentation describes security controls in sufficient detail to permit analysis and testing of controls. For Federal entities, baseline meets minimum configuration management standards as required by NIST standards and OMB.

Topics covered include:

• Obtain an inventory of all computer assets and determine if the inventory is accurate, complete, and whether duplicate copies are adequately protected – check whether all the hardware equipment's are properly entered in the inventory and there are no duplicate entries.

• Select items in the inventory and trace to the asset and verify that the configuration (model, settings, etc.) is accurate.

• Select assets at the entity and verify that they are accurately recorded in the inventory. (Note: Selections should be focused on areas that are most relevant to the audit.)
Control Activity: CM-2.1. Current configuration identification information is maintained.

Control Technique: CM-2.1.3. Configuration settings optimize the system’s security features.

Topics covered include:

- Observe/inspect the current system security configuration settings to determine if the security baseline deployed has been maintained – check whether the security is deployed according to the baselines or not.

- Determine if key component security settings conform with NIST SP 800-70 and vendor recommendations.
Control Activity: CM-4.1. The configuration is routinely audited and verified.

Control Technique: CM-4.1.1. Routinely validate that the current configuration information is accurate, up-to-date, and working as intended for networks, operating systems, and infrastructure applications.

Topics covered include:

- Obtain and inspect a selection of the configuration verifications and audits for compliance with applicable standards and determine whether vendor-supplied system software is still supported by the vendor – check whether the software company purchased is still supported by the vendor or not.

- Evaluate adequacy of the configuration audits based on the results of the IS control audit tests performed and determine whether configuration deviations are remediated timely – check whether the deviated configurations are remediated or not.
Control Activity: CM-4.1. The configuration is routinely audited and verified.

Control Technique: CM-4.1.3. Confirm compliance with applicable configuration management policy, plans, standards, and procedures.

Topics covered include:

Obtain and inspect a selection of configuration compliance reviews and determine whether configuration changes are in compliance with applicable configuration management policy, plans, standards, and procedures. Determine if findings are followed up and remediated timely – check whether configuration changes are according to its policy. Also findings are resolved quickly.
Questions??