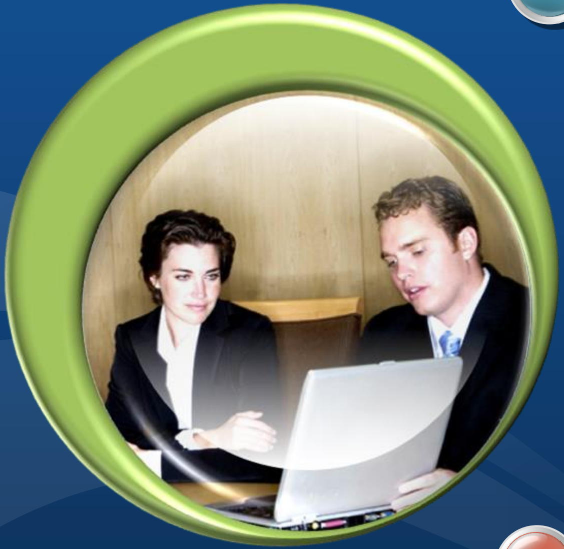
Securely Yours LLC

IT Hot Topics

Sajay Rai, CPA, CISSP, CISM
sajayrai@securelyyoursllc.com

Contents



- Background
- Top Security Topics
- What auditors must know?
- What auditors must do?
- Next Steps

Background

Movement towards Cloud

- More Applications in Cloud
- More Critical Data in Cloud

Smart Devices Influx

- Critical data on Smart Devices
- Increased Data Leakage

SECURELY YOURS LLC

SECURING YOUR INFORMATION WORLD

Intensity of Attacks

- C to C (Country to Country)
- C to C (Company to Company)
- C to C (Consumer to Consumer)

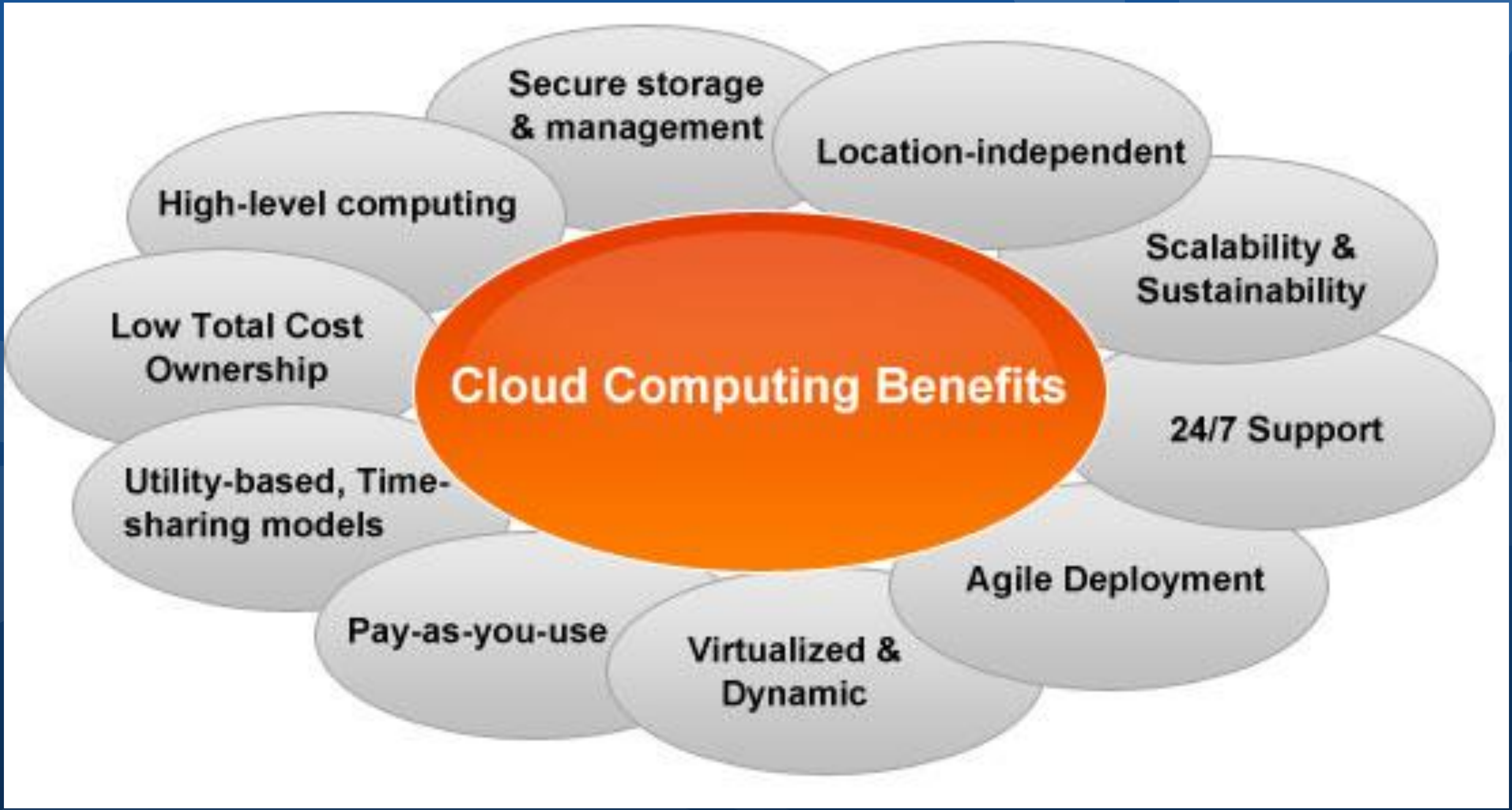
Increased Regulations

- More scrutiny by Federal & State
- More demands by customers/clients

Top Security Topics

1. Public Cloud

1. Public Cloud

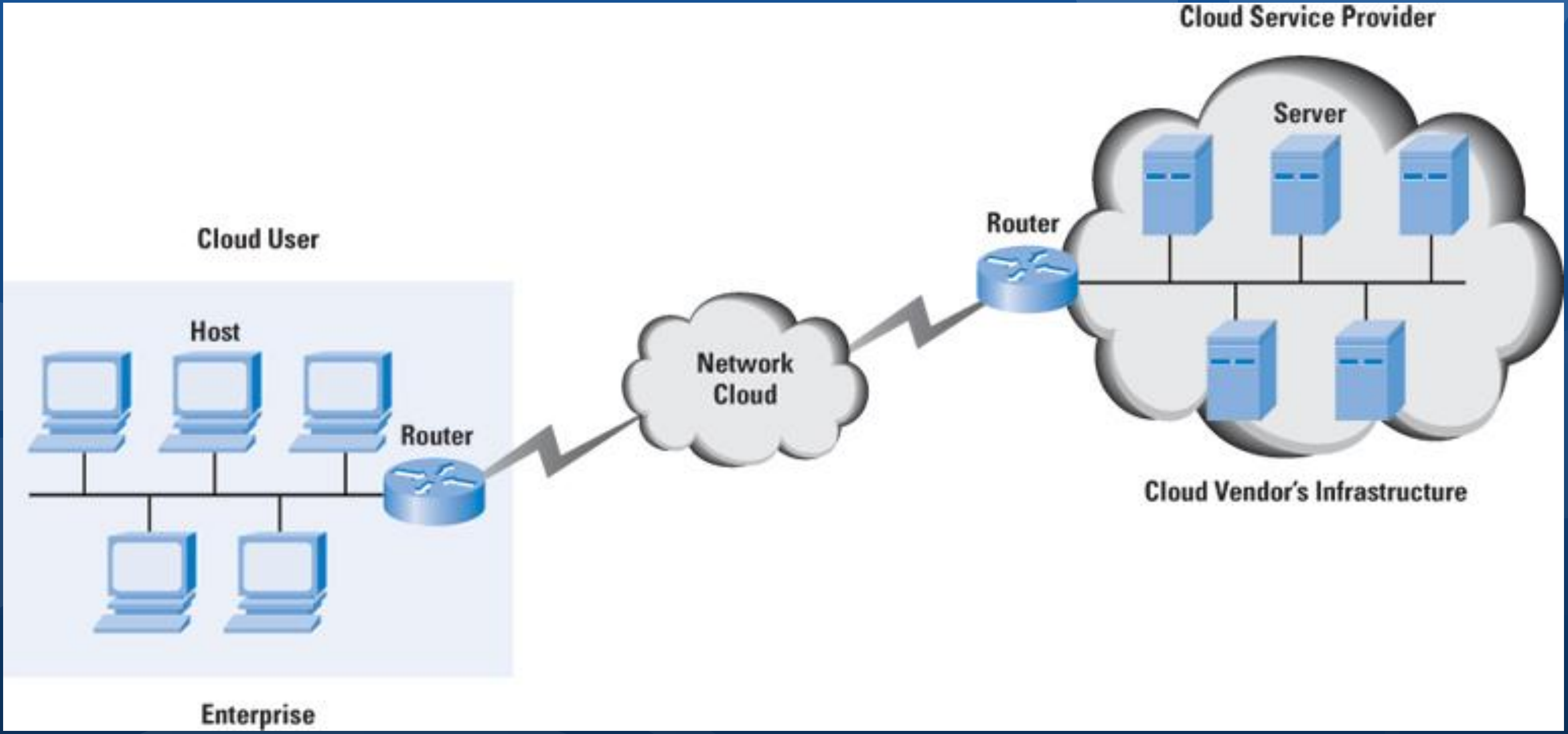


1. Public Cloud

What is it?

- Organizations are starting to use public clouds for many critical applications
  - Sharing of folders e.g. Box.net
  - Email e.g. Google mail
  - Marketing and Sales e.g. Salesforce.com
- Organizations either access these applications in the cloud by creating a separate account or link to their identity stores like Active Directory or LDAP
- Organizations usually nominate an administrator within their organization to manage the users (addition, deletion and changes)

1. Public Cloud



1. Public Cloud

What auditors must know?

- How the users within your organization access the application
  - How are they authenticated?
  - How the access to resources are provided?
- How the activities are logged and monitored?
- What data breach procedures does the service provider has?
- What access protocols does the service provider has in place to prohibit their employees to look at your critical data?
- What Disaster Recovery and continuity procedures does the service provider has?
- Does your organization use Single Sign-on (SSO) vendors in the public cloud to make access easier to cloud applications (e.g. Ping Identity, OneLogin)?
- Does the organization have a right to audit the provider?

1. Public Cloud

What auditors must do?

1. If using SSO vendors, verify that the passwords are not being copied or stored in the service provider systems. If they are, a verification test should be performed that the passwords are encrypted (using appropriate encryption protocols) at all times.
2. Verify that the appropriate documents are provided by cloud application providers (vulnerability scan reports, SOC2 type 2 etc.)
3. If possible, conduct periodic audits of the service provider (big companies probably won't let you conduct audits)
4. Verify that your IAM process extends to the cloud service providers as well (getting rid of ids when employee leaves)
5. Verify that the logs are being reviewed either by service providers or by your organization (monitor activity and anomalies)

Top Security Topics

1. Public Cloud
2. Smart Devices

2. Smart Devices

What is it?

- Proliferation of smart devices across the organization
- Started out as a replacement of blackberry but now major applications are being developed
- The smart devices are starting to replace laptops and connecting to the corporate network
- Mobile applications are being downloaded from Apple and Google stores at record pace
- IT has implemented Mobile Device Management (MDM) solutions
- Majority of Internal Audit departments are now starting to include auditing of smart devices in their audit plans

2. Smart Devices

What auditors must know?

- MDM software allows to enforce security policies on the smart device
- If your organization does not have an MDM software, there are built-in features in Activesync which can be utilized
  - E.g. Unlock, lock and wipe out devices
- Is confidential data residing on users smart devices
- Is your organization writing mobile apps and deploying on users devices?
- Are smart devices connecting with corporate network to access internal folders and files?
- Understand the new features of operating systems which run the smart devices

Security Features of iOS7

Feature 1

Single Sign-on

- Previously available for multiple apps developed by same developer (e.g. Google Apps)
- Now available for all Apps
- Some constraints:
  - Kerberos enabled platform and application
  - Still have to provision the device and send profile

Feature 2

Restricting opening of attachments

- Restrict attachments to open within approved apps (e.g. you can open an attachment in corporate email vs. personal email)
- Restricts data leakage
- Prevents users to take a picture of confidential information and post it on facebook

Feature 3

Default Data Protection

- When a passcode is configured, Apple used to protect the data using hardware encryption, but it was left for developers to protect application data (choice of encryption)
- Now, by default everything is encrypted

Feature 4

Per App VPN

- Instead of a VPN for the IP address, now the VPN is per App.
- Different Apps can connect to different VPNs
- Not fully tested yet, but I think we would be able to VPN to a payroll provider for payroll app and a bank for a banking application and both apps could be used interchangeably

Feature 5

Activation Lock

- Currently, the Find My iPhone feature allows you to locate and secure your lost iOS device using the Find My iPhone app on another iPhone, iPad or iPod touch, or by visiting iCloud.com on your computer.
- Unfortunately, it has a major drawback. The thief can turn off your iOS device and restore it to prevent you from using the Find My iPhone features.
- iOS 7 includes a new feature called Activation Lock. In iOS 7, turning off Find My iPhone or erasing your device requires Apple ID and password. It will also continue to display the custom message displaying your contact number, even after your device is erased. This should make it a major deterrent for thieves and make the Find My iPhone feature fool proof.

Feature 6

iCloud Key Chain

- In iOS 7, Safari’s AutoFill feature has been extended to remember account names, passwords, and credit card numbers. Safari will automatically enter them when you visit a site to sign in or shop online. The keychain will also be synced via iCloud to all your iOS devices running iOS 7 and Macs running OS X Mavericks. Apple says the information will be stored using 256-bit AES encryption.
- Safari will also be able to generate a unique, hard-to-guess password like password management apps like 1Password.
- Unfortunately, this feature will be extremely useful only for users who use Safari on their computers and iOS devices. If you prefer using Chrome, then this feature is useless

Other Features

- Private Browsing
  - Easy to set private browsing on Safari
- Fingerprinting
  - Two factor Authentication
  - Still issues with it
    - Hackers
    - Ease of use
- Recent news of SIRI bug unlocking the phone

2. Smart Devices

What auditors must do?

1. Review the following documents:
   - Smart Device Use Policy
   - Smart Device security Policy
   - IT Infrastructure architecture documents
   - MDM procedures
   - Reports produced from MDM
2. Verify that the security policy is implemented on the device
3. Verify that the appropriate reports from MDM are being reviewed
4. Verify that appropriate authentication protocols are in place if the device is connecting to the corporate network
5. Verify that appropriate anti-virus scan is performed to download apps from stores and/or appropriate SDLC process is in place to review the source code

Top Security Topics

1. Public Cloud
2. Smart Devices
3. Cyber Insurance Policy

3. Cyber Insurance Policy

What is it?

- Designed to mitigate losses due to cyber incidents
- Vehicle to insure against cyber expenses
- Some policies cover regulatory penalties
- Some policies require minimum controls before the claims are paid
- The positive is that it is a good tool to be part of your overall security program and promotes security awareness
- The negative is that it is very expensive

3. Cyber Insurance Policy

What auditors must know?

- What is covered? What is not?
- What are the requirements of compliance?

What auditors must do?

1. Review the cyber security insurance policy as part of your overall risk assurance program
2. Understand the requirements of the policy for insurance coverage and the state of security required to file claim
3. Communicate the requirements to security group

Top Security Topics

1. Public Cloud
2. Smart Devices
3. Cyber Insurance Policy
4. Extended Enterprise

4. Extended Enterprise

What is it?

- Service providers outside of your network
- Typically have access to OR store your confidential information
- May even have access to OR store HIPAA related or PII information
- May or may not have an agreement in place
- May or may not have a Business Associate Agreement
- May provide the following services:
  - Cloud (e.g. Salesforce.com)
  - Backup and Recovery (e.g. Iron Mountain)
  - Delivery (e.g. Fedex etc.)
  - Smart devices (e.g. iCloud, apps which save your information in cloud)
- Potentially your weakest link

4. Extended Enterprise

What auditors must know?

- Identify third parties which provide KEY services
- The responsibilities of the service providers in terms of security
- Third party compliance with the contracted terms (including BAA)
- What steps are taken before bringing in a new service provider (cloud, hosting etc.)

What auditors must do?

1. Identify the KEY service providers
2. Ensure that the contracts with key service providers have security requirements and if needed BAA agreements
3. Review the process of risk analysis for new service providers

Top Security Topics

1. Public Cloud
2. Smart Devices
3. Cyber Insurance Policy
4. Extended Enterprise
5. Security Information Event Management

5. SIEM

What is it?

- Data Aggregation: Logs from various sources
- Correlation: Looking for common attributes
- Alerts: Automated analysis and alerts
- Retention: Ability to retain past history
- Automate Compliance: by collecting compliance data
- Commonly known software (Gartner top right Quadrant)
  - HP's Arcsight
  - IBM's Q1 Labs
  - McAfee (Nitro Security)
  - Novell's LogRhythm
- Other known software
  - Splunk
  - LogLogic
  - Symantec and RSA

5. SIEM

What auditors must know?

- What activity is going on?
- Are their risks which are being ignored or not known?
- What action is taken once an incident is reported or discovered?
- Is appropriate information recorded to understand the activities taking place within the organization?

What auditors must do?

1. Understand the process of log management, logging, log reviewing and incident reporting
2. Identify the technologies whose logs are not reviewed or recorded
3. Are their correlation analysis done on the log data to identify advanced persistent threats

Top Security Topics

1. Public Cloud
2. Smart Devices
3. Cyber Insurance Policy
4. Extended Enterprise
5. Security Information Event Management
6. Data Leakage

6. Data Leakage

What is it?

- Allows organization to understand the data which is coming inside the organization AND which data is leaving the organization
  - We want to know if unwanted data is coming in (e.g. malware)
  - We want to know if confidential data is leaving (e.g. PHI or PII)
- DLP: assist with data leakage:
  - Data Loss Prevention
  - Symantec
  - McAfee
  - Websense
  - RSA
- NGFW (Next Generation Firewall)
  - Deep packet scanning
  - Sees the content before it comes in
  - Sees the content before it goes out

6. Data Leakage

What auditors must know?

- What sensitive data is leaving the organization?
- In what form the data is leaving?
- What regulatory requirements does your organization have or what agreements you have with your clients (Encryption etc.)
- Focus on Data Classification

What auditors must do?

1. Review the process of data leaving the organization via different vehicles: emails, Flash drives, FTP, website etc.
2. Understand the technology implemented to assist with data leakage
3. Verify that regulatory or contractual requirements are met
4. Review the data classification policy and procedures

Top Security Topics

1. Public Cloud
2. Smart Devices
3. Cyber Insurance Policy
4. Extended Enterprise
5. Security Information Event Management
6. Data Leakage
7. Appropriate Access

7. Appropriate Access

What is it?

- Knowing the identities
- Knowing the roles
- Knowing the access
- Reviewing the access
- Logging the violations
- Technologies which can help:
  - Work flow
  - Identity and Access Management
  - Password sync and password management
  - Single Sign-on
  - Federated Id

7. Appropriate Access

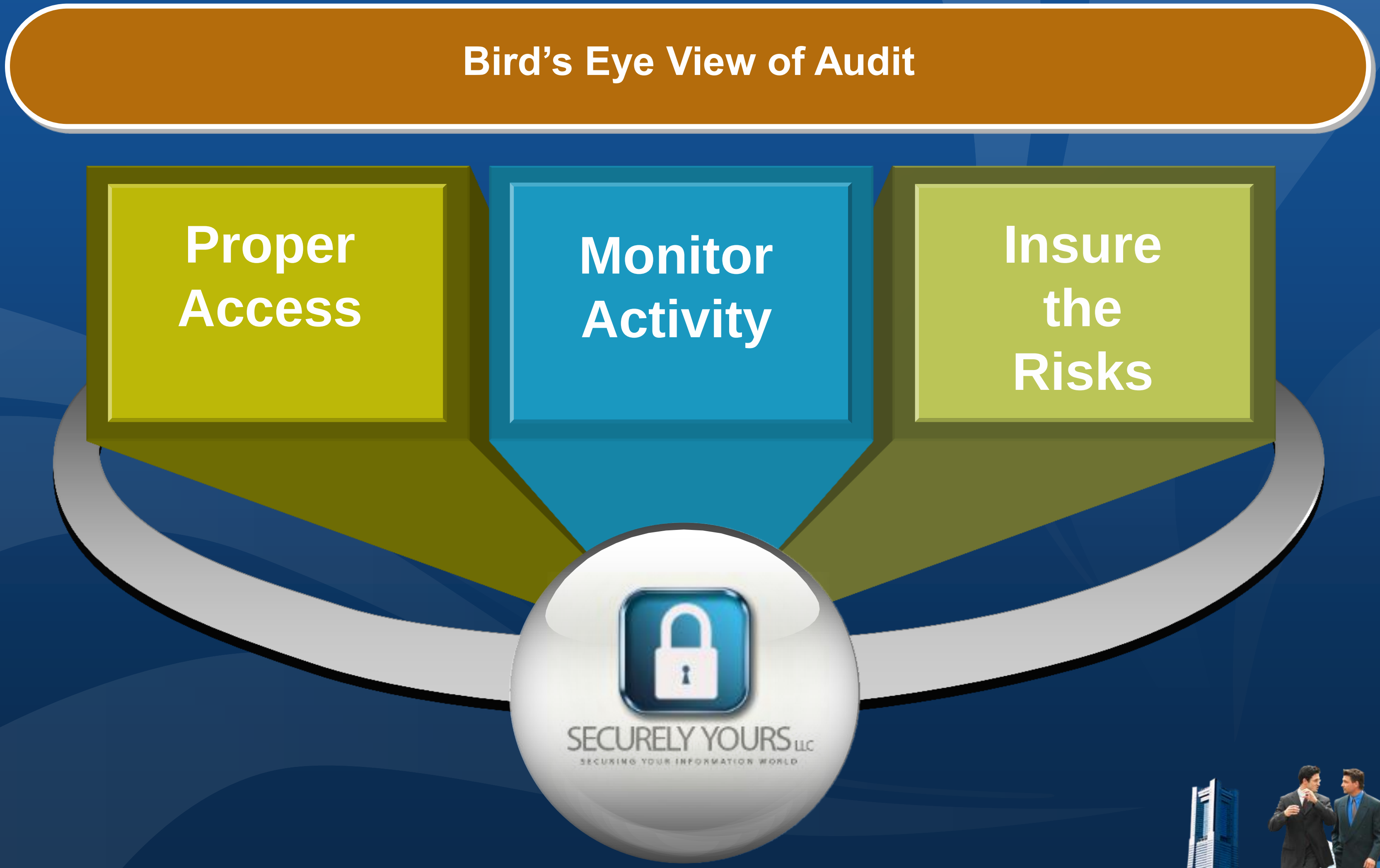
What auditors must know?

- Does sensitive data have appropriate access?
- Is Access to sensitive data reviewed by appropriate owners?
- Is Identity and Access managed appropriately within the organization?
- Are sensitive data protected through a layered defense?

What auditors must do?

1. Ensure that the access review is performed periodically
2. Review the provisioning and de-provisioning process for accuracy
3. Review how third party service providers get access to sensitive data
4. Understand how the system logs are reviewed and managed

Next Steps



Bird's Eye View of Audit

Proper Access

Monitor Activity

Insure the Risks

Thank You!

Sajay Rai 248-723-5224 sajayrai@securelyyoursllc.com