We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Advanced IT Audit Techniques and Procedures

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Learning Objectives

At the end of this session, you will be able to:

- Identify Advanced Audit Techniques and Procedures to include:
  - Network and Operating Systems
  - Databases
  - Virtual Machines
  - Security
  - Applications
- Recognize Information Technology Controls to include:
  - IT Governance Controls
  - IT Security Controls
  - IT Operations Controls
  - Development Controls
  - Change Management Controls

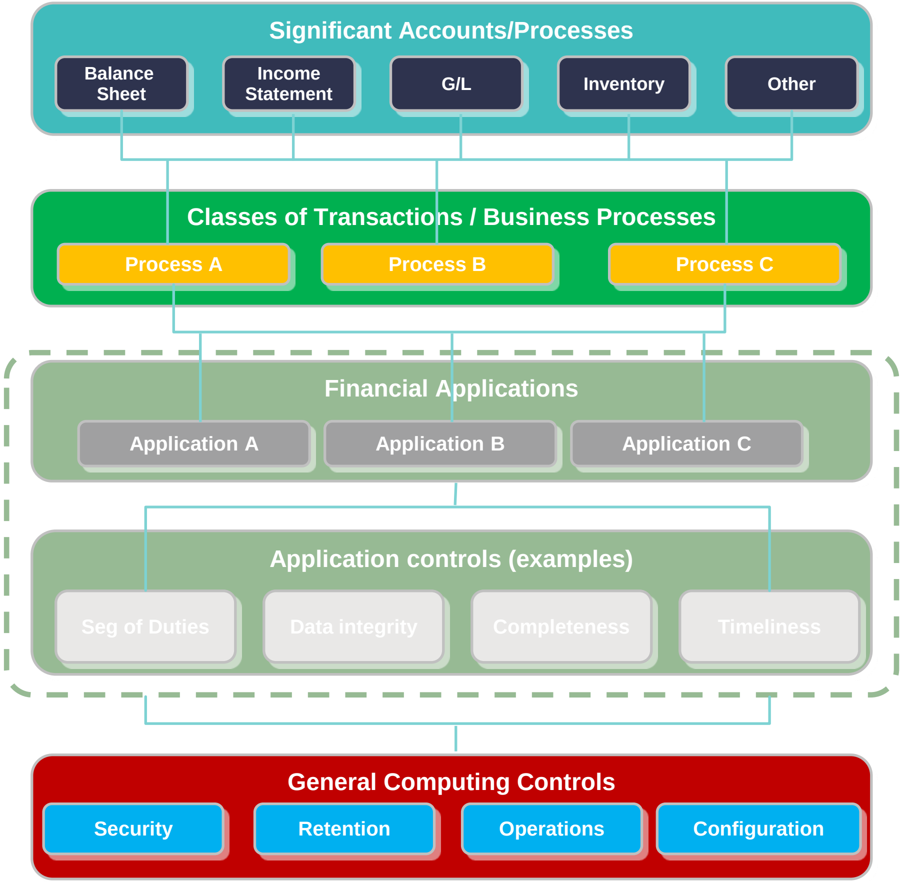
Agenda

- Overview of Information Technology Controls
- Advance IT Audit Techniques
  - Network and Operating Systems
  - Databases
  - Virtual Machines
  - Security
  - Applications

IT General Control Overview

Types of IT Controls

- General Controls
  - Foundation Controls
- Application Controls
  - Operational Controls
- IT Dependent Controls
  - Reports



Significant Accounts/Processes

Balance Sheet

Income Statement

G/L

Inventory

Other

Classes of Transactions / Business Processes

Process A

Process B

Process C

Financial Applications

Application A

Application B

Application C

Application controls (examples)

Seg of Duties

Data integrity

Completeness

Timeliness

General Computing Controls

Security

Retention

Operations

Configuration

IT General Controls (ITGC) Focus Area

- IT Governance Controls
- IT Security Controls
- IT Operations Controls
- Development Controls
- Change Management Controls

IT General Control - Considerations

- **Logical Security Controls**
- Authorization of user access (internal and external)
- Appropriateness of user rights
- Segregation of duties
- Security parameters in operating system
- Password parameters
- Security software settings
- Security violation logging

- **Program Change Controls**
- Authorization and Approval of program changes
- Testing/Quality Assurance
- User involvement and sign-off
- System Development Life Cycle (SDLC)
- Source Code Control software – access restrictions & version control
- Emergency Changes approvals
- Segregation of duties, including programmer access

IT General Control - Considerations

- **Backup and Recovery of Data and Programs**
  - Mechanism to track successful completion of backups
  - Population of backups
  - Periodic testing to establish the validity of backups
- **Incident Management**
  - Monitoring
  - Tracking and response
- **Job Scheduling**
  - May be governed by change control, but may also fall into operations
- **Physical/Environmental**

Logical Access Controls

- Administrative Access
  - Level of access above the normal user.
    - Configure the system
      - Inclusion of devices
      - Configuration of authentication protocols
      - Configuration of audit logging
    - Manage user
      - Creating/disabling users
      - Unlocking users
      - Managing access and permissions

Logical Access Controls

- Authentication of users
  - Local vs Network vs Identity Access Manager
    - Local: Operating System
    - Network: Active Directory, Novell
      - LDAP vs SSO
        - LDAP: Application protocol to crosscheck information
        - SSO: User authentication protocol
    - Identify Access Manager: Oracle, CA
      - Manages access for users at a single point for multiple applications, systems, services, etc.

Network and Operating System

- Monitoring of activity (logging)
  - Enabling of activities logged
  - Securing audit logs
  - Monitoring activities
    - Passive vs. Active vs. Automated
      - Passive: Logs reviewed when problem/incident occurs
      - Active: Reviewing logs for anomalous activity
        - Automated: Logic programmed in systems to alert for unusual activity

Administrative Access – Active Directory

Group or Account Name	Default Location	Description
Enterprise Admins	Users container	This group is automatically added to the Administrators group in every domain in the forest, providing complete access to the configuration of all domain controllers.
Schema Admins	Users container	This group has full administrative access to the Active Directory schema.
Administrators	Built-in container	This group has complete control over all domain controllers and all directory content stored in the domain, and it can change the membership of all administrative groups in the domain. It is the most powerful service administrative group.
Domain Admins	Users container	This group is automatically added to the corresponding Administrators group in every domain in the forest. It has complete control over all domain controllers and all directory content stored in the domain and it can modify the membership of all administrative accounts in the domain.

Administrative Access – Continued

Group or Account Name	Default Location	Description
Server Operators	Built-in container	By default, this built-in group has no members. It can perform maintenance tasks, such as backup and restore, on domain controllers.
Account Operators	Built-in container	By default, this built-in group has no members. It can create and manage users and groups in the domain, but it cannot manage service administrator accounts. As a best practice, do not add members to this group, and do not use it for any delegated administration.
Backup Operators	Built-in container	By default, this built-in group has no members. It can perform backup and restore operations on domain controllers.
DS Restore Mode Administrator	Not stored in Active Directory	This special account is created during the Active Directory installation process, and it is not the same as the Administrator account in the Active Directory database. This account is only used to start the domain controller in Directory Services Restore Mode. In Directory Services Restore Mode, this account has full access to the system and all files on the domain controller.

Administrative Access – Active Directory

- Request from the network administrator group member from each of the above groups and any custom administrative groups from the domain
  - Located in "Active Directory Users and Computers" screen under the "Users" tab. View the "Members" tab in the properties of each group under review
    - Single Head Icon – individual
    - Double Head Icon – group
      - Obtain member of any imbedded group listed in the group under review
- Review the membership with network architect to determine that access is appropriate.

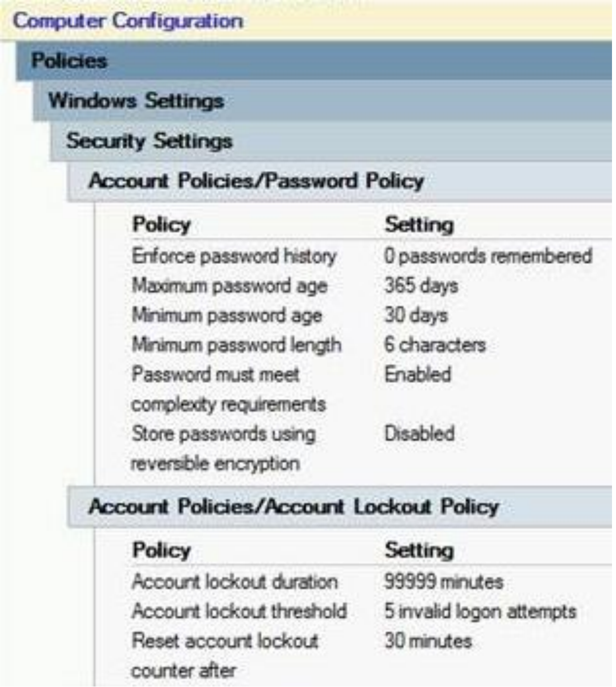
Active Directory – Authentication Controls

- Request from the Group Policies for Account Policy/Password Policy and Account Policy/Account Lockout Policy for the domain and each operating unit
    - Enforce Password History (Expiration) > 24 password remembered
    - Maximum password age (Expiration) < 90 days
    - Minimum Password age (Expiration) > 1day
    - Minimum Password Length > 8 characters
        - Leading practices 12+
    - Password must meet complexity requirements = Enabled
    - Store passwords in reversible encryption = Disabled
        - Storing **encrypted** passwords in a way that is **reversible** means that the **encrypted** passwords can be decrypted

Active Directory – Authentication Controls

- Account lockout duration > 15 minutes
  - Leading practice is to disable (‘0’), which requires administrative action to unlock
- Account lockout threshold between 3 and 5
- Reset account lockout counter after > 15 minutes
  - Automatically resets after successful login

Active Directory – Authentication Controls



Computer Configuration

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	0 passwords remembered
Maximum password age	365 days
Minimum password age	30 days
Minimum password length	6 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

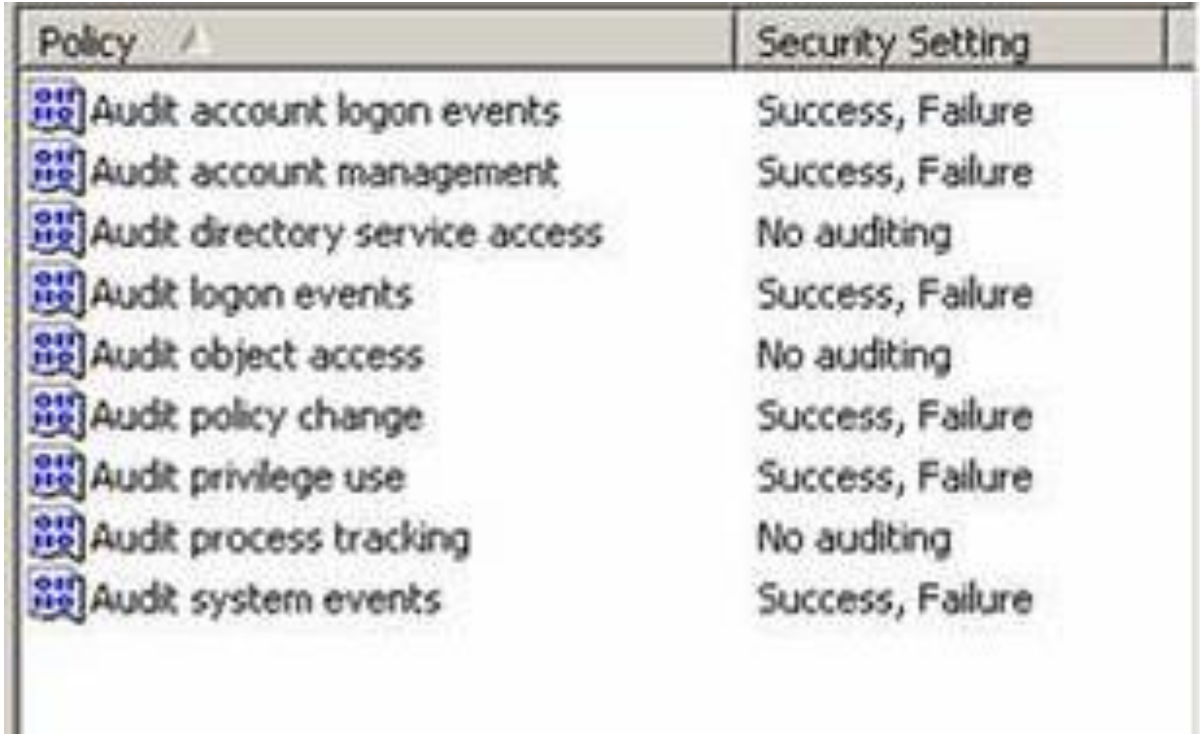
Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	99999 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Active Directory – Audit Logging

- Request from the Group Policies for Audit Policy
  - **Account logon events**. Audit this to see each instance of a user logging on to or logging off from another computer in which this computer is used to validate the account. Account logon events are generated in the domain controller's Security log when a domain user account is authenticated on a domain controller. These events are separate from Logon events, which are generated in the local Security log when a local user is authenticated on a local computer. Account logoff events are not tracked on the domain controller.
  - **Account management**. Audit this to see when someone has changed an account name, enabled or disabled an account, created or deleted an account, changed a password, or changed a user group.
  - **Directory service access**. Audit this to see when someone accesses an Active Directory® directory service object that has its own system access control list (SACL).
  - **Logon events**. Audit this to see when someone has logged on or off your computer (either while physically at your computer or by trying to log on over a network).
  - **Object access**. Audit this to see when someone has used a file, folder, printer, or other object. While you can also audit registry keys, we don't recommend that unless you have advanced computer knowledge and know how to use the registry.
  - **Policy change**. Audit this to see attempts to change local security policies and to see if someone has changed user rights assignments, auditing policies, or trust policies.
  - **Privilege use**. Audit this to see when someone performs a user right.
  - **Process tracking**. Audit this to see when events such as program activation or a process exiting occur.
  - **System events**. Audit this to see when someone has shut down or restarted the computer, or when a process or program tries to do something that it does not have permission to do. For example, if malicious software tried to change a setting on your computer without your permission, system event auditing would record it.

Active Directory – Audit Logging



Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	No auditing
Audit system events	Success, Failure

Windows – Audit Logging (Baseline)

- **Account logon events**
  - Audit Credential Validation (Success)
- **Account management**.
  - Audit Computer Account Management (Success)
  - Audit Other Account Management Events (Success)
  - Audit Security Group Management (Success)
  - Audit User Account Management (Success)
- **Directory service access**.
  - None
- **Logon events**.
  - Audit Logoff (Success)
  - Audit Logon (Success)
  - Audit Special Logon (Success)
- **Object access.**
  - **None**
- **Policy change**.
  - Audit Audit Policy Change (Success/Failure)
  - Audit Authentication Policy Change (Success)
- **Privilege use**.
  - None
- **System events**.
  - Audit IPsec Driver (Success/Failure)
  - Audit Security State Change (Success/Failure)
  - Audit Security System Extension (Success/Failure)
  - Audit System Integrity (Success/Failure)

https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

Administrative Access - Unix

- The default administrator account is “root”
  - User accounts can be granted root access by giving an account a user id number of ‘0’ or group id number of ‘0’
    - Obtain the etc/passwd file a review for any account with a ‘0’ user or group ID

```
root:!:0:0::/:/usr/bin/ksh
```

User Name	Password	User ID #	Group ID #	Full Name	Home Directory	Login Shell
Root	!	0	0		/	/usr/bin/ksh

  - The root account should be restricted from remote login
    - Obtain the etc/security/user and review that the rlogin configuration is set to ‘false’ for the root account

Administrative Access - Unix

```
default:
            admin = false
            login = true
            su = true
            rlogin = true

root:
            admin = true
            account_locked = false
            rlogin = false
            login = true
```

Administrative Access - UNIX

- Switch User (SU) vs SUDO
  - SU: allows convenient and secure access to the root account without having to log out of the current logged in user account
    - Switches are logged in the SU log (location: var/adm/sulog)
      - Log should be reviewed at an appropriate frequency
  - SUDO: tool for securing and logging the behavior of users who need to perform limited administrative tasks
    - Permissions are stored in the sudoers file (location: etc/sudoers)
      - Permissions should be reviewed with the server administrator for appropriateness
    - Commands are logged in the system log file (var/adm/messages)
      - Log should be reviewed at an appropriate frequency
      - Leading practice is to log in separate file

Authentication Controls - UNIX

- Obtain the /etc/security/user file from the UNIX administrator

- Histexpire: How long (weeks) before a password can be reused: >52
- Histsize: Number of password before reuse: 24
- Login: Restricts login to the system: True/False
- Logintimes: Restricts time of login
- Loginretries: Failed Attempts before account is locked: 3-5
- Maxage: Maximum password age (in weeks) before expiration: <12
- Maxexpired: Maximum time (in weeks) that a user can change an expired password: 2
- Maxrepeats: Maximum number of times character can be repeated in a password
- Minage: Minimum age (in weeks) before a password can be changed: .15
- Minalpha: Minimum alphabetic characters is a password: 1
- Mindiff: Minimum character difference of new password: 1
- Minlen: Minimum password length: 8
- Minother: Minimum non-alphabetic characters is a password: 1

Authentication Controls - UNIX

```
default:
        admin = false
                login = true
        logintimes =
        loginretries = 5
        histexpire = 13
        histsize = 10
                minage = 2
                maxage = 8
        maxexpired = 4
        minalpha = 1
        minother = 1
                minlen = 8
                mindiff = 3

        maxrepeats = 8
```

Administrative Access – AS/400 (OS/400)

- User permissions for the operating system are stored in the Display User Profiles Report (DSPUSRPRF)
  - The file is extract by using the following command DSPUSRPRF USRPRF(*ALL) OUTPUT(*OUTFILE) OUTFILE(QTEMP/<filename>)
  - Key fields to review:
    - Special Authority (UPSPAU)
      - * ALLOBJ: allows user to access any resource on the system
      - * SECADM: allows user to modify system security
      - * AUDIT: allows user to modify system audit configurations
    - Limit Capability (UPLTCP)
      - Users with *NO or *PARTIAL have the ability to change the initial menu, initial program, current library, or the attention key handling value. (To get access to the OS/400 command line.)

Authentication Controls AS/400

- System configurations for the operating system are stored in the Work System Value Report (WRKSYSVAL)
  - The file is extracted by using the following command WRKSYSVAL *ALL OUTPUT(*PRINT)
  - Key fields to review
    - QSECURITY
      - 10: No system-enforced security
      - 20: Sign-on security
      - 30: Sign-on and resource security (Baseline)
      - 40: Sign-on and resource security; integrity protection
      - 50: Sign-on and resource security; enhanced integrity protection.

Authentication Controls AS/400 (OS/400)

- Password Configurations
  - QPWDMINLEN (Password minimum length): 8
  - QPWDRQDDGT (Numeric character requirements): 1
  - QPWDLMTREP (Character repetition limit):
    - 1: No repeats in password
    - 2: No consecutive repeats in password
  - QPWDLMTREP (Password Expiration): <90
  - QMAXSIGN (Maximum of failed login attempts): 3-5
  - QMAXSGNAC N(Action to take when max failed long in attempts is reached):
    - 1: Disable the device only
    - 2: Disable the user profile only (Baseline)
    - 3: Disable both the user profile and device

Authentication Controls AS/400 (OS/400)

- QPWDRQDDIF (Minimum character difference of new password): 1
- QINACTITV (Inactive Session Timeout): 60
- QDSPSGNINF (Display login information): 1

Administrative Access – RACF (z/OS)

- User permission for the operating system are included in the “Selected User Attribute Report” of the Data Security Monitor Report (DSMON)
    - Review the list of accounts with the “SPECIAL” (security administrator), “OPERATIONS” (computer operations), or “AUDITOR” (logging configuration)

Authentication Controls – RACF (z/OS)

- System configurations for the operating system are included in the Set RACF Options Report (SETROPS)

Authentication Controls – RACF (z/OS)

```
PASSWORD PROCESSING OPTIONS:
 PASSWORD CHANGE INTERVAL IS 90 DAYS.
 PASSWORD MINIMUM CHANGE INTERVAL IS 1 DAYS.
 MIXED CASE PASSWORD SUPPORT IS IN EFFECT.
 24 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
 AFTER 4 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS, A USERID WILL BE
 REVOKED.
  PASSWORD EXPIRATION WARNING LEVEL IS 14 DAYS.
 INSTALLATION PASSWORD SYNTAX RULES:
  RULE 1 LENGTH(4:5) LLLLL
  RULE 2 LENGTH(5) AAAAA
  RULE 3 LENGTH(6:8) LLLLLLLL
  RULE 4 LENGTH(6:8) NNNNNNNN
  RULE 5 LENGTH(6:8) AAAAAAAA
 LEGEND:
  A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL
  *-ANYTHING c-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL $-NATIONAL
```

Administrative Access - Oracle

- User accounts are located in the DBA_USER table
    - Number of accounts indicates:
        - Few – application account interfaces updates to the database
            - Lower Risk
        - Many – user accounts interface updates to the database
            - Higher Risk
    - Defaults Accounts (SYS, SYSTEM, SCOTT, DBSNMP, OUTLN)
        - Validate that default password has been change and determine how access to the account is controlled

Administrative Access - Oracle

- DBA Access
  - Role access is granted through the ROLE_PRIVS table
    - Determine that accounts (Grantee) with the ‘DBA’ or custom role (GRANTED_ROLE) and validate that access is appropriate
      - Review that the “admin_option” (ability to assign the role) is appropriate
  - System privileges are granted through the SYS_PRIVS table
    - Account Administration: Determine that accounts granted the “CREATE USER” privilege are appropriate
    - Table Administration: Determine that accounts granted the following privileges are appropriate

- ALTER ANY TABLE
- CREATE ANY TABLE
- CREATE TABLE
- DELETE ANY TABLE
- DROP ANY TABLE
- INSERT ANY TABLE
- UPDATE ANY TABLE

Authentication Controls - Oracle

- Authentication configurations are located in the DBA_Profiles table
  - Configurations are set for each profile listed in the DBA_USER table
  - FAILED_LOGIN_ATTEMPTS
  - PASSWORD_LIFE_TIME
  - PASSWORD_REUSE_TIME
  - PASSWORD_REUSE_MAX
  - PASSWORD_VERIFY_FUNCTION
  - PASSWORD_LOCK_TIME
  - PASSWORD_GRACE_TIME

Virtual Machines

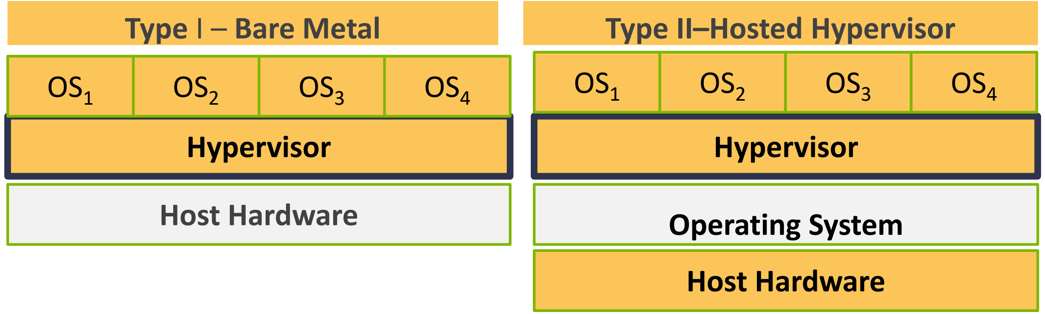
Virtual Machine - Overview

- Virtualization is a software technology
- Divides a physical resource into multiple virtual resources
- Consolidates physical resources
- Separates Operating systems from hardware
- Enables multiple operating systems and applications to share the resources of a single physical machine
- Risk is not that different from physical environments

- Configuration
- Access Management

- Change Management
- Patch Management

Virtual Machine - Diagram



Type I – Bare Metal

OS_1 OS_2 OS_3 OS_4

Hypervisor

Host Hardware

Type II–Hosted Hypervisor

OS_1 OS_2 OS_3 OS_4

Hypervisor

Operating System

Host Hardware

Hypervisor installed directly onto the hardware	Host OS is installed onto the physical hardware
Instances of OS installed onto the hypervisor	Hypervisor is the second layer installed onto the host OS
Needs a management console	Host OS provides the management functions

Virtual Machines

- Governance
  - Established objectives/goals
  - Ongoing risk assessment monitoring and reporting
  - Documentation of service level agreements
  - Documented policies/procedures
- Infrastructure
  - Hypervisor (VMWare) vs. HyperV (MicroSoft)
  - Partitions/Zones/Environments/Operating Systems

Virtual Machines

- Access Management
  - How is access to management controls controlled/monitored?
  - Who has access to:
    - Change configurations
    - Create new images
    - Modify template images

Virtual Machines

- Change Management (Image Management)
  - Has a standard image template been defined?
    - Are existing images updated with the changes to the template?
    - Are existing images audited for compliance with the template?
      - Are exemptions/deviations documented/approved?
  - Has a hardening guide been established?
    - Is it actively used when deploying new images?
    - Are existing images audited for compliance with the guide?
      - Are exemptions/deviations documented/approved?
  - Are consoles and systems patched on a regular basis
    - Are system reviewed from missing patches?

Network Devices - Overview

- What Comprises your network
  - Firewalls
  - Switches
  - Routers
  - Services
  - Desktops

- But Also
  - Printers
  - Faxes
  - Copiers
  - Internet of Things
    - Lightbulbs
    - Thermostats
    - Home Automation

Security

Network Devices - Risks

- Capture data crossing the network (sniffing)
- Redirect traffic
- Drop or interrupt network traffic
- Basis for distributed denial of services (DDOS) attacks

Network Devices – Access Controls

- Verify that default passwords are changed
- Verify that passwords are secured and only known to those that need access
- Use central authentication controls (identify management systems)

Network Devices – Change Management

- Verify that infrastructure changes are processed through a process as vigorous as software or program change management
  - Includes hardening guides for deployment
  - Includes SLDC standards of end of life management
- Firewall/Router/Switch Rule Sets
  - Changes to rule sets have an established change management process
  - Changes to rule sets are monitored
  - Rule sets are periodically assessed against standards

Security/Incident Response Preparedness

- Internal Vulnerability/External Penetration
  - Use to validate internal management/configuration management
  - Should be supplemented with internal assessments
    - Scanning Tools – To identify missing patches
      - Microsoft Baseline Security Analyzer
      - Nessus
    - Scripting – To identify configuration not agreeing to hardening guidelines

Security/Incident Response Preparedness

- Incident Response Testing
    - Natural/Technical Disaster vs. Breach (suspected)
        - Table top vs simulated
        - Technical vs Non-technical

Application Controls

Application Controls

- Application controls are automated processes that effect business transactions. There are two types of application controls:
  - Inherent to the application
  - Configured within the application
- Inherent controls include the Software logic defined by the software vendor (“Out of the Box Functionality”)
- Configured controls rely upon management to determine the parameters or possible values (e.g. tolerance levels in the Accounts Payable approval authority)

Link of ITGC and Application Controls

- In order to rely on, and utilize/assess, application controls, effective IT General Controls need to be present. Given that General Controls support Application controls, tests of both and effective conclusions of both are necessary for reliance.

Application Controls - Access

- Sensitive Access – Access to privileged functions are retracted to authorized individuals
  - Maintain vendor master records
  - Entry general ledger transactions
- Review Procedures:
  - Work with the application administrator to extract accounts with access to the function(s)
    - Pitfall: Basing on group description

Application Controls - Access

- Segregation of Duties – A single user cannot process multiple functions of the same transactions
  - Enter invoice vs. Maintain vendor master
  - Enter general ledger transaction vs approve general ledger transactions
  - Process purchase order vs. enter goods receipt vs. process invoice
- Types
  - Procedural vs. Technical
  - Segregation of access vs system inquiry

Application Controls - Access

- Review Procedures
  - In complex ERPs separate modules or third-party tools
    - SAP>GRC
  - Work with the application administrator to extract accounts with access to the functions
    - Manual compare for incompatible duties

Application Controls Thresholds

- System configuration to warn or stop transaction when certain parameters are met
    - Expense request exceeds available budget
    - Cash receipt does not meeting billed amount
    - Invoice amount exceeds purchase order
- Review Procedures
    - Design: Validate that configuration meets design of the control
    - Operational: Perform positive/negative tests to validate that system operates as expected

Application Controls – Workflow Approval

- System configuration to require approval on a transaction before processing
  - Purchase requisition/order
  - General ledger postings
  - Adjustments
    - Inventory
    - Write off

Application Controls – Workflow Approval

- Review Procedures
  - Design: Validate that configuration meets design of the control
  - Operational: Perform positive/negative tests to validate that system operates as expected
  - Access: Work with the application administrator to extract accounts with access to the function(s)

Thank you!

Joel Eshleman
Phone: 717-558-0860
Email: joel.eshleman@CLAconnect.com
Baltimore, MD

Brian Boguski
Phone: 215-371-4785
Email: brian.Boguski@CLAconnect.com
Philadelphia, PA

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS