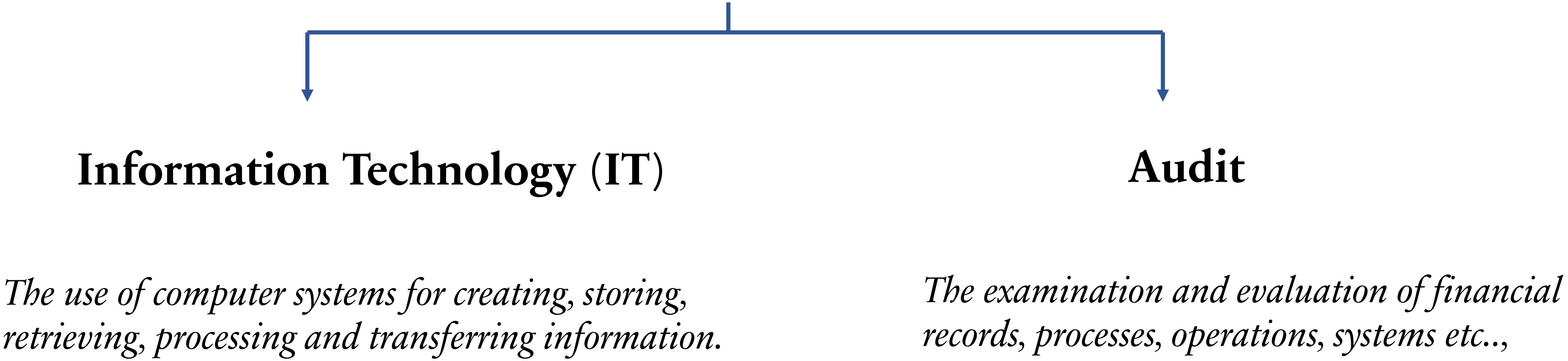
# IT Audit



**Information Technology (IT)**

*The use of computer systems for creating, storing, retrieving, processing and transferring information.*

**Audit**

*The examination and evaluation of financial records, processes, operations, systems etc..,*

**IT Audit** is the examination and evaluation of an IT infrastructure, applications, data, policies and operations.

# Importance of IT Audit

- Availability of Computer Systems
- Security
- Confidentiality
- Reliability
- Compliance With The Law

The main objective of an IT audit is to identify inaccuracies and inefficiencies in the management and use of the IT systems.

# Sarbanes - Oxley (SOX) Act

# Sarbanes Oxley (SOX) Act 2002

Enacted in 2002:

- Financial scandals involving – Enron, Tyco International, Adelphia, Worldcom, etc..,
- Billions of dollars lost in the US stock market
- Eroded confidence in the US stock market

Sarbanes-Oxley Act of 2002 passed by the US Congress to protect investors by improving the accuracy and reliability of corporate disclosures.

- Reduce potential fraud
- Ensure financial systems are accurate
- Protect investors
- Restore faith in the US stock market

# Sarbanes-Oxley (SOX) Act 2002

**Section 302:** Corporate Responsibility for Financial Reports

- CEO and CFO are directly responsible and personally attest that the financial information is accurate and reliable

**Section 404:** Management Assessment of Internal Controls

- Management is responsible for implementing adequate internal controls
- Assessment of the effectiveness of the internal control structure and any shortcomings in the controls.
- Independent external auditors' attestation

Section 302 & 404 mandates a controlled environment for financial reporting that includes designing, implementing, testing, and certifying internal controls' effectiveness.

# Who Must Comply With SOX?

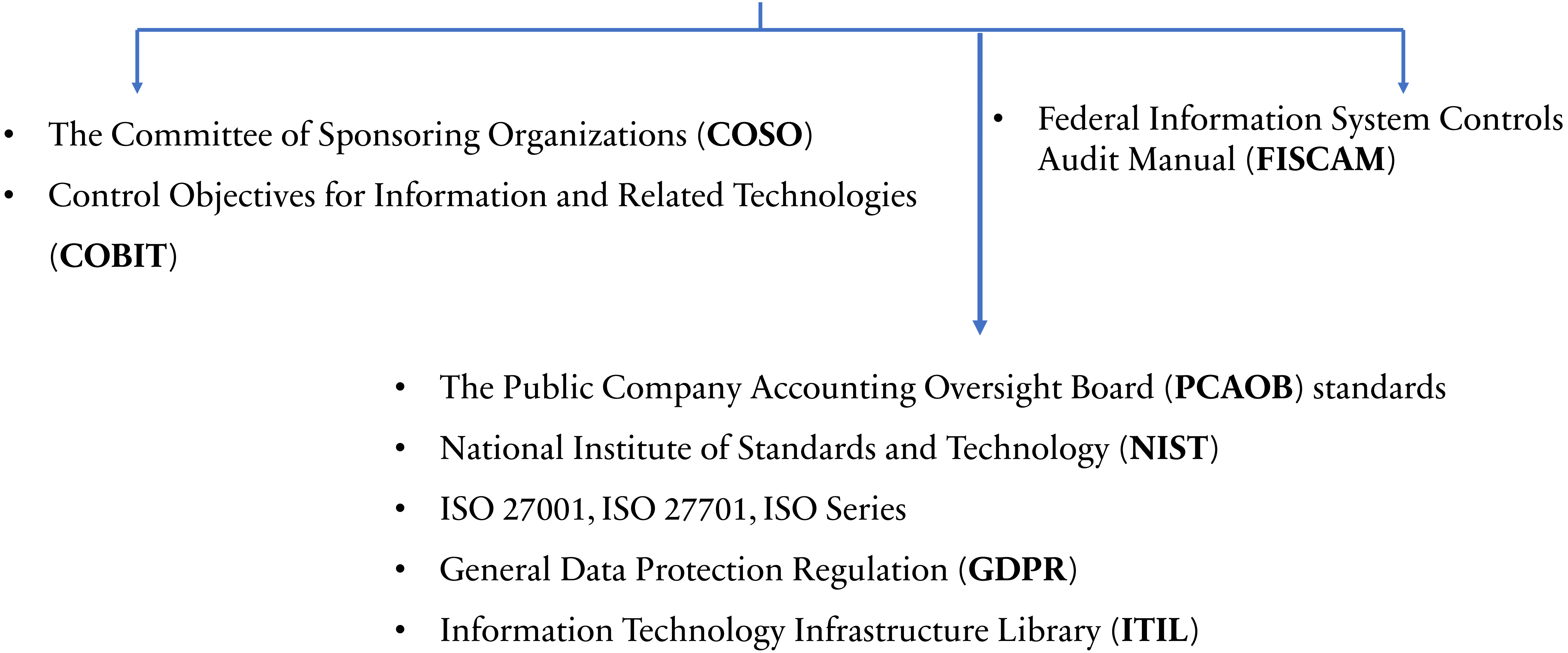
- All publicly traded companies in the United States
- All foreign companies that are publicly traded and do business in the United States
- Accounting firms that offer services to any of the above companies

To comply with the Sarbanes-Oxley Act of 2002, organizations are required to conduct a yearly audit of financial statements.

Note: Private companies are not mandated to comply with SOX, however some of its provision may directly affect them.

# IT Audit Frameworks

# IT Audit Frameworks



- The Committee of Sponsoring Organizations (**COSO**)
- Control Objectives for Information and Related Technologies (**COBIT**)

- Federal Information System Controls Audit Manual (**FISCAM**)

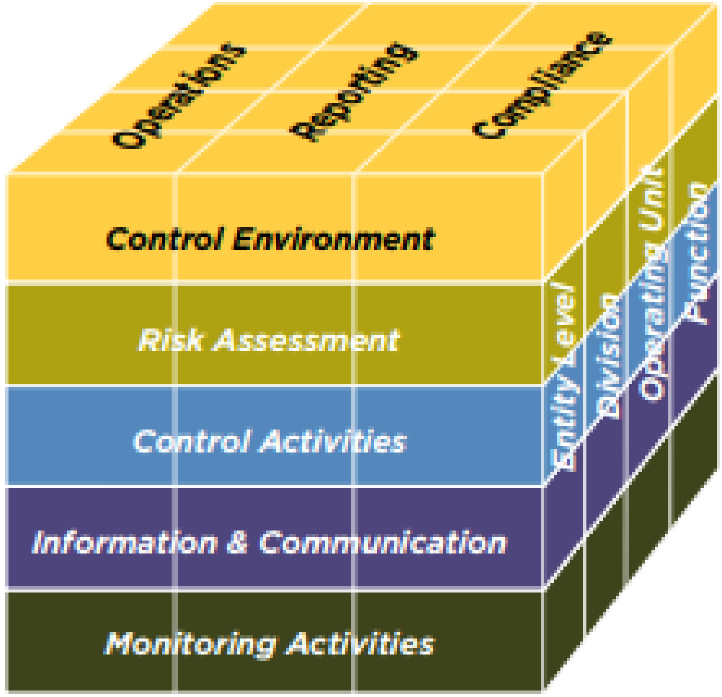
- The Public Company Accounting Oversight Board (**PCAOB**) standards
- National Institute of Standards and Technology (**NIST**)
- ISO 27001, ISO 27701, ISO Series
- General Data Protection Regulation (**GDPR**)
- Information Technology Infrastructure Library (**ITIL**)

# COSO Framework

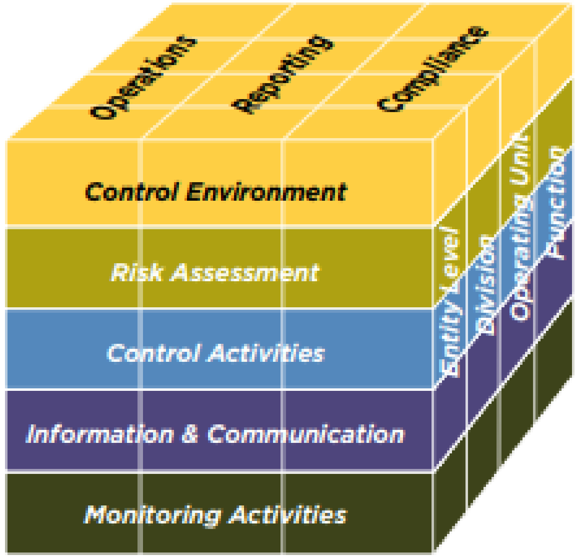
- System used to establish integration of internal controls into business processes.
- Focuses on Section 404 of SOX Act – Internal controls over financial reporting

# COSO Framework Objective

- **Operations:** Effectiveness and efficiency of business operations
- **Reporting:** Reliable financial & non-financial reporting
- **Compliance:** Compliance with laws and regulations and industry standards



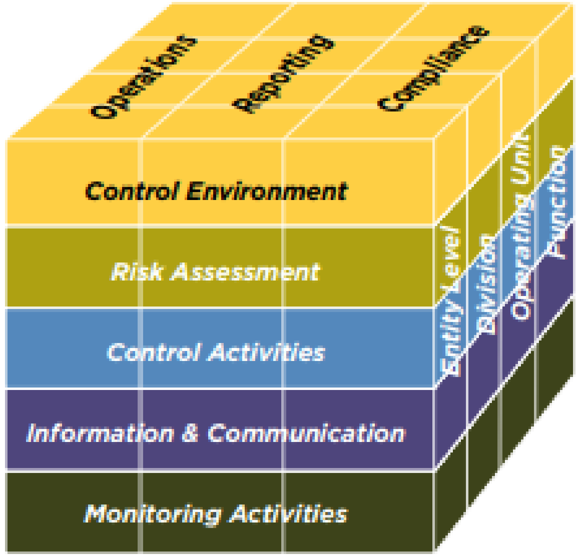
# COSO Framework Components



- **Control Environment:** Policies & procedures that guide the organization
- **Risk Assessment:** Adoption of risk management plans
- **Control Activities:** Internal controls in place & operating effectively over a period of time
- **Information & Communication:** Communicating expectations to internal & external users
- **Monitoring Activities:** Overseeing the functioning of the entire organization, identifying gaps and correcting deficiencies

# COSO Framework Entity Structure

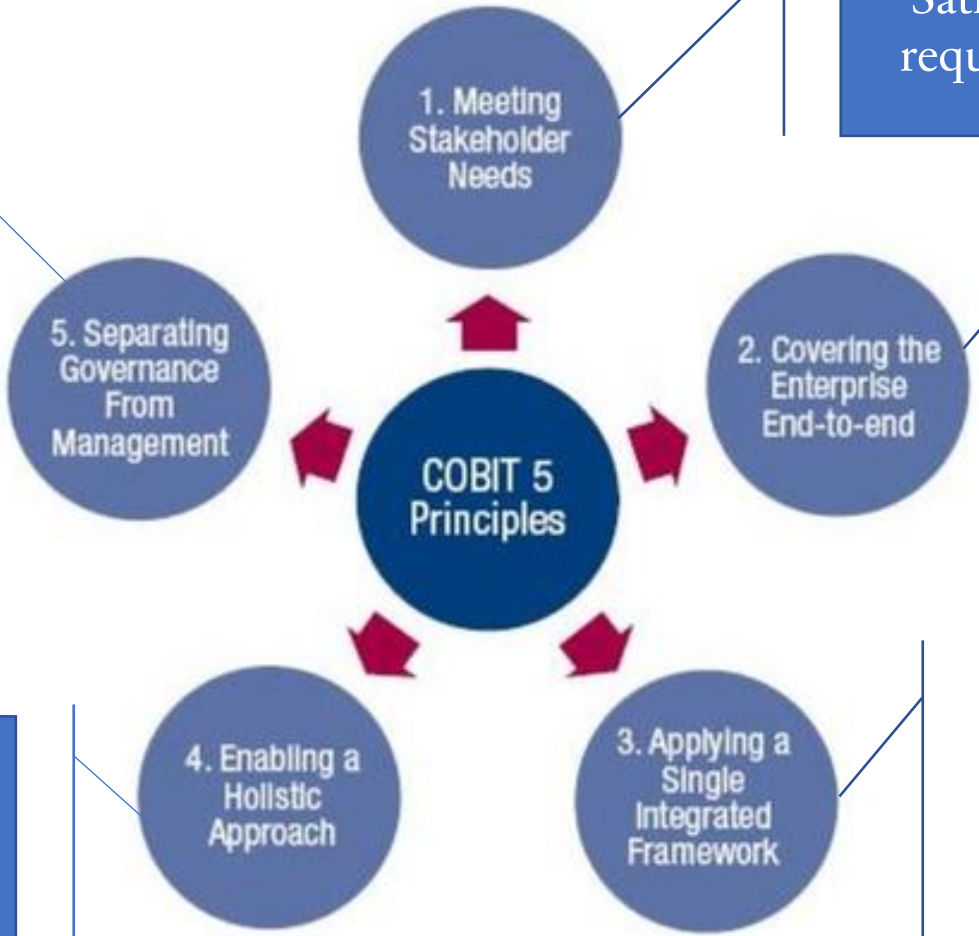
- Operating units
- legal entities
- Other structures



# COBIT Framework

- The COBIT Framework provides detailed instructions for how to design and implement a secure IT infrastructure related to business management and governance.
- Created by ISACA (Information Systems Audit & Control Association).
- It is a mixture of frameworks, resources and standards.

# COBIT Framework Key Principles


1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

Satisfy customer needs and requirement of stakeholders

Manage and operate every section of the business planning

Integration of relevant frameworks and governance standards – COSO, ITIL, ISO series, GDPR, PMBOK e.t.c.

Entire organization should work as a single unit.

Separate governance implementation and management in your organization.

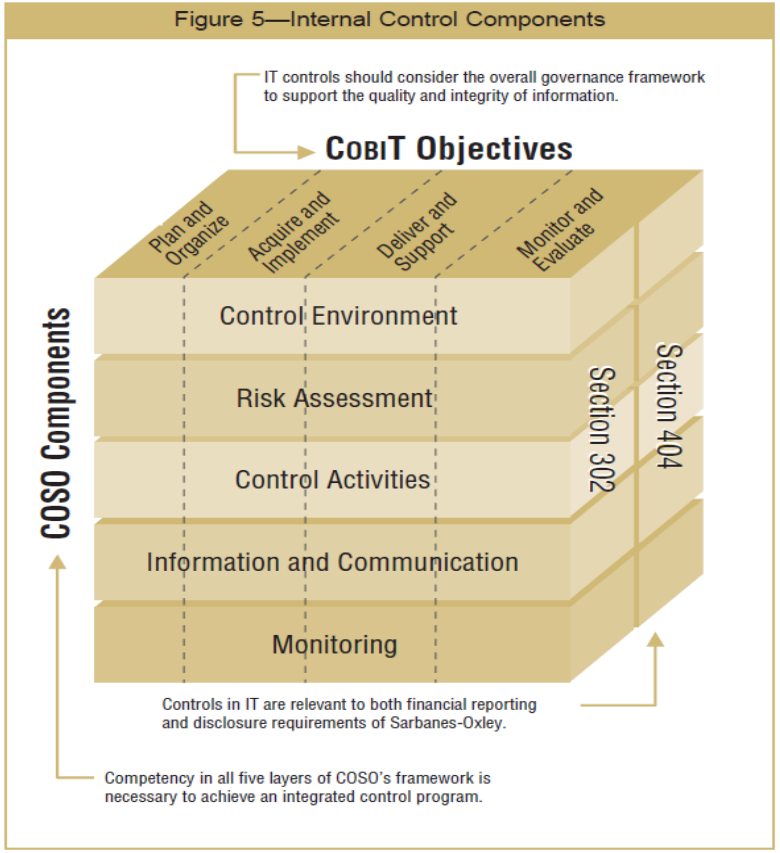
# COSO & COBIT Frameworks

- Both frameworks help in creating, managing and maintaining internal controls for fraud prevention and risk management.

- COSO provides framework for fraud prevention through implementing effective internal controls and risk management .

- COBIT helps ensure that organization's IT system enhances and strengthens internal controls.

Figure 5—Internal Control Components



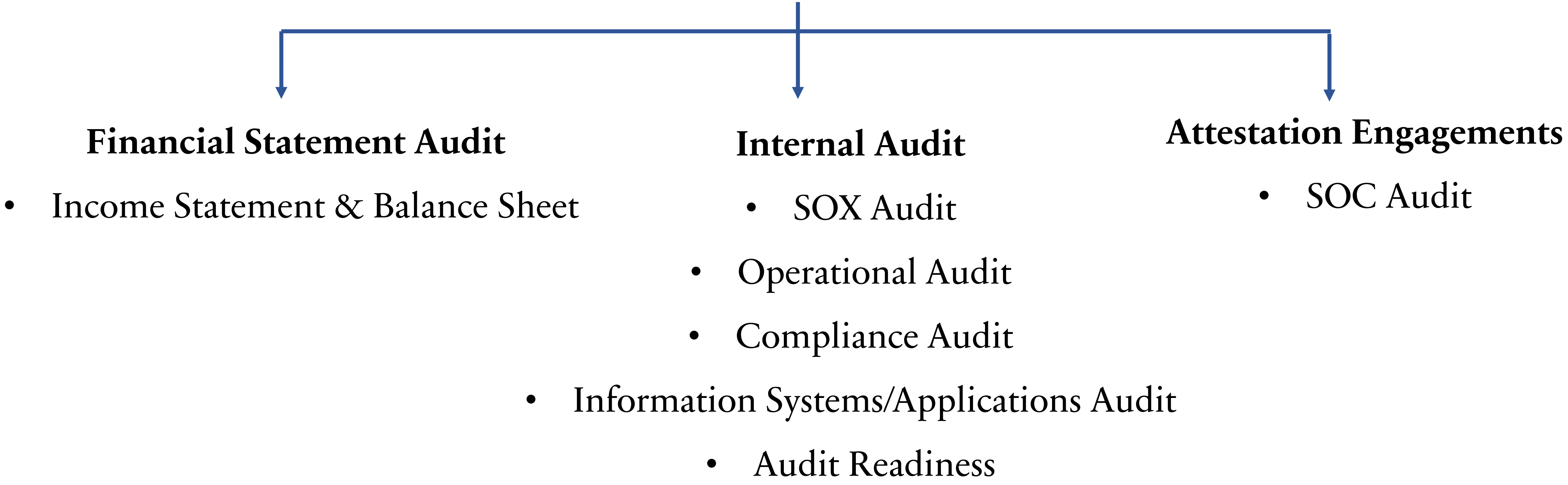
IT controls should consider the overall governance framework to support the quality and integrity of information.

Controls in IT are relevant to both financial reporting and disclosure requirements of Sarbanes-Oxley.

Competency in all five layers of COSO's framework is necessary to achieve an integrated control program.

# Types of IT Audit

# Types of IT Audit



**Financial Statement Audit**

- Income Statement & Balance Sheet

**Internal Audit**

- SOX Audit
- Operational Audit
- Compliance Audit
- Information Systems/Applications Audit
- Audit Readiness

**Attestation Engagements**

- SOC Audit

# Types of IT Audit – Financial Statement Audit

- Primarily the audit of Income Statement and Balance Sheet.

- Purpose: Ensure adherence to standard accounting principles – Generally Accepted Accounting Principles (GAAP).

- Determine if the IT controls are effective & financial systems reliable for generating accurate financial controls.

- Performed by Accounting firms – Certified Public Accountants (CPA). Only CPA firms are authorized to perform financial statement audit

# Types of IT Audit – Internal Audit

**Audit Projects**

- **SOX Audit:** Assessment of internal controls in compliance with sections 303 & 404 of the SOX Act.

- **Operational Audit:** Evaluates process changes, procedures, pricing, resource allocation and associated internal control activities  to determine impact on attaining organizational goals & objectives.

- **Compliance Audit:** Adherence to laws, regulations, internal & external policies, terms of contracts.

- **Information Systems Audit:** Information & transaction processing systems and how people use those systems.

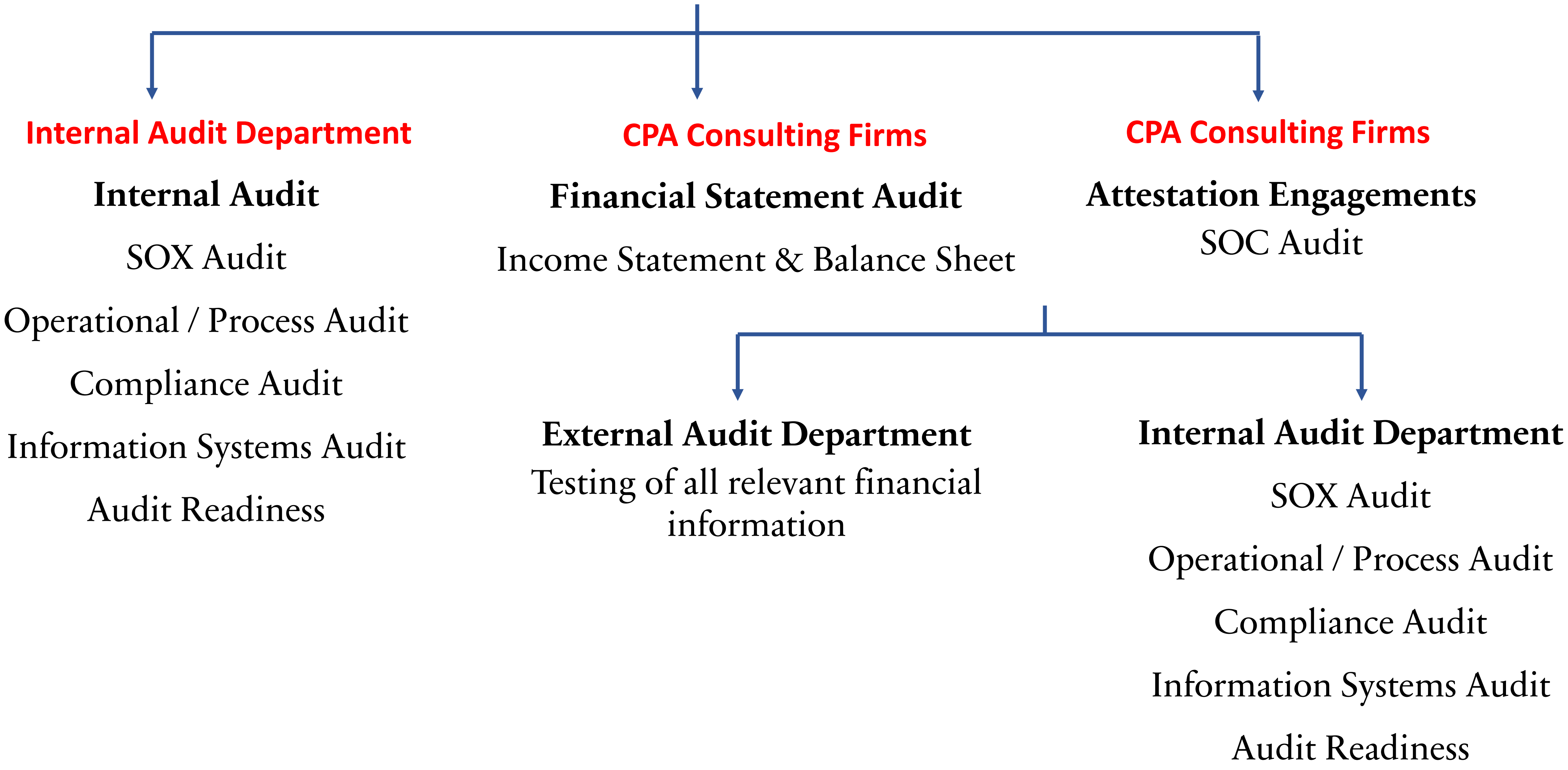
- **Audit Readiness:** Identify gaps in systems, internal controls, processes before an external audit.

# Types of IT Audit – Attestation Engagement

- **Service Organization Control** (**SOC**) **Audit:** Attest or confirm internal controls at service organizations are in place and are properly designed and operating effectively

# Internal Auditor
# vs
# External Auditor

# Internal Auditor vs External Auditor



**Internal Audit Department**

**Internal Audit**

SOX Audit

Operational / Process Audit

Compliance Audit

Information Systems Audit

Audit Readiness

**CPA Consulting Firms**

**Financial Statement Audit**

Income Statement & Balance Sheet

**External Audit Department**

Testing of all relevant financial information

**Internal Audit Department**

SOX Audit

Operational / Process Audit

Compliance Audit

Information Systems Audit

Audit Readiness

**CPA Consulting Firms**

**Attestation Engagements**

SOC Audit

# Functions of the Internal Audit Department

- Perform IT Audit - Monitor/test the effectiveness of the internal controls (SOX 404 requirement)
- Monitor and assist the company with risk management
- Assist with documentation and development of the company's internal controls
- Monitor/test the company's operational process for compliance, efficient and fraud detection

Internal Audit is an independent and consulting activity whose basic task is to provide assurance that the organization's control and operations are efficient and effective

# IT Auditor – Internal vs External Auditor

**ABC Company**

**Internal Audit Department**

**CPA Firm (Deloitte, KPMG, BDO etc.)**

**Internal & External Audit Department**

**IT Audits**

Financial Statement Audit

SOC Audit

SOX Audit

Operational / Process Audit

Compliance Audit

Information Systems Audit

Audit Readiness

# IT Auditor – Internal vs External Auditor

| Internal Auditors | External Auditors |
|---|---|
| Company employees | Outside audit firm |
| Hired by the company | Appointed by a shareholder vote |
| CPA designation not mandatory | Must have CPA designation |
| Reports are used by management | Used by stakeholders – investors, creditors, lenders |
| Internal audits are conducted throughout the year | External auditors conduct a single annual audit. |

# IT Controls

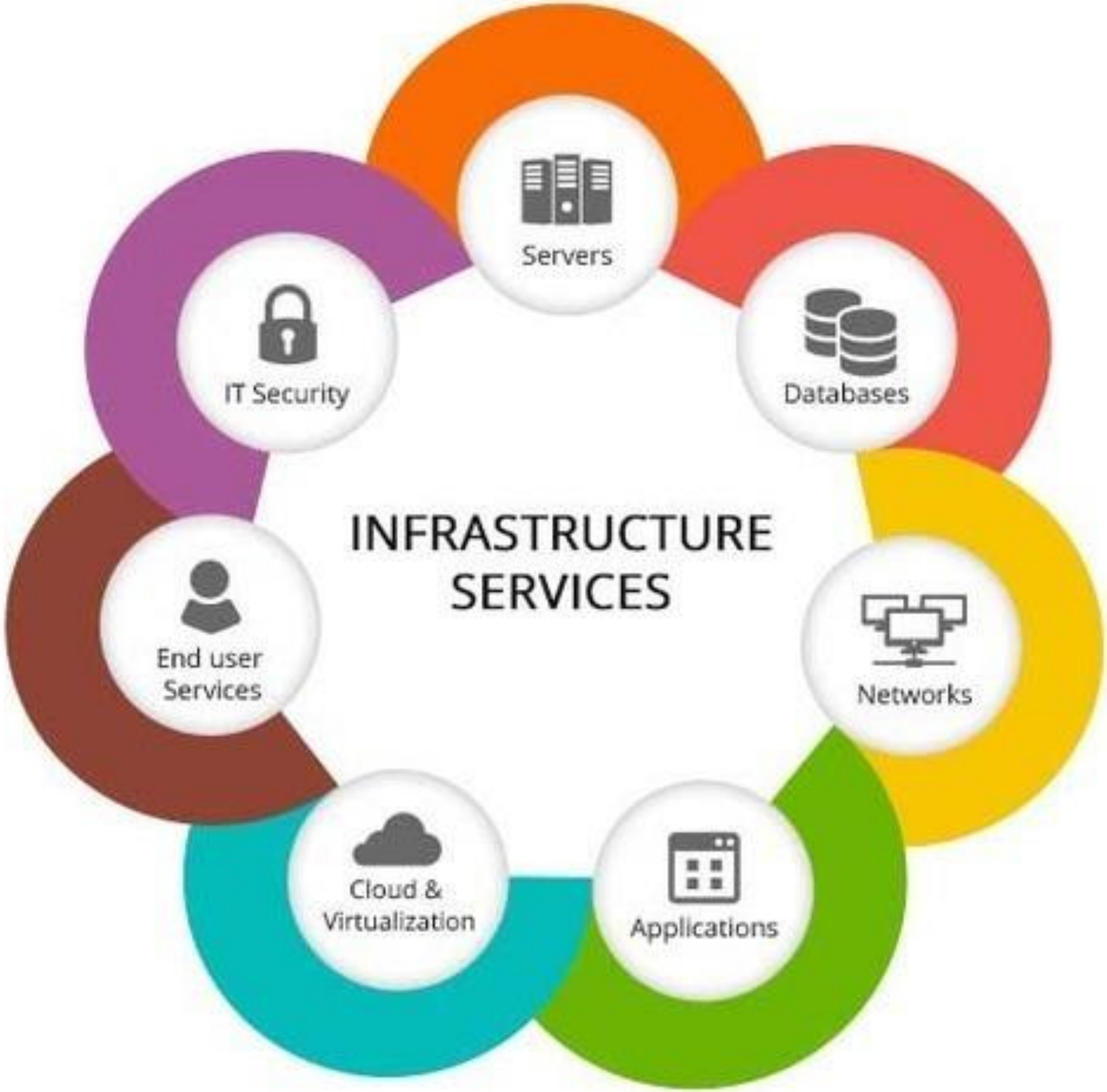
# IT Controls

- An IT control is a procedure or policy that provides a reasonable assurance that an IT environment operates as intended, that data is reliable, and that the organization comply with applicable laws and regulations.
  - An IT control is any action, policy, procedure
  - Controls only provides reasonable assurance
  - Operating as intended
  - Data reliability
  - Compliance with laws

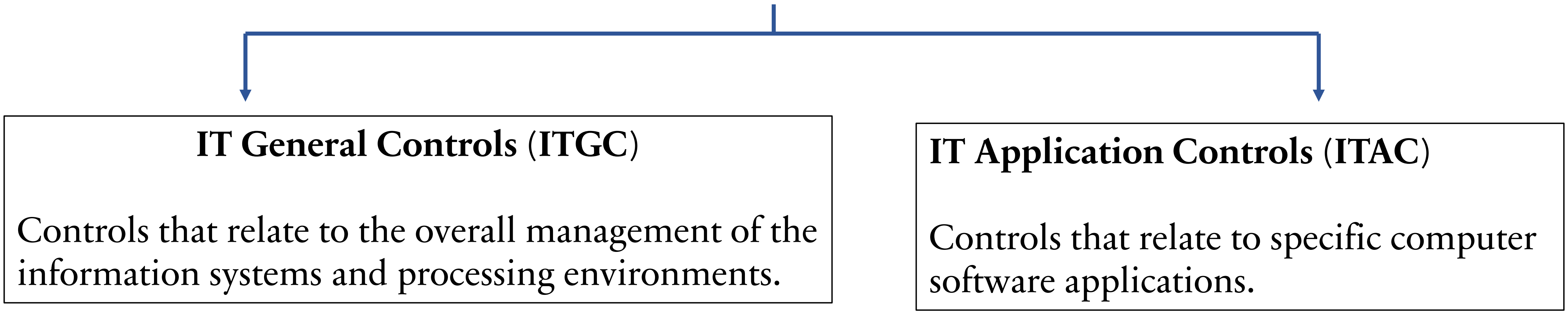
**Note: A control can be automated or human activities or a combination of both.**

# Controls

# IT General Controls (ITGC)
# &
# IT Application Controls (ITAC)


INFRASTRUCTURE SERVICES
Servers
Databases
Networks
Applications
Cloud & Virtualization
End user Services
IT Security

# IT Controls



**IT General Controls (ITGC)**

Controls that relate to the overall management of the information systems and processing environments.

**IT Application Controls (ITAC)**

Controls that relate to specific computer software applications.

IT Audit is the examination and evaluation of an organization’s IT infrastructure, applications, data, policies and operations.

IT Audit is the examination of IT General and Application controls of an organization’s IT infrastructure to determine if those controls are **designed appropriately** and **operating effectively**.

# IT General Controls (ITGC)

# IT General Controls (ITGC)

1. Access Controls – Logical & Physical
2. Change Management Controls
3. IT Operations – Backup & Recovery
4. System Development Life Cycle (SDLC)

# Access Controls (ITGC)

# Access Controls – Logical & Physical (ITGC)

**Objective:** Only authorized persons have access to data & applications; and can perform only specifically authorized functions.

- Determine if user access is authorized and appropriately established
- Password parameters are appropriate & compliant with policies/best practices
- Access provisioning and de-provisioning
- Physical access to IT resources is appropriately restricted
- Logical access process is monitored
- Access to privileged IT functions is limited to appropriate individuals
- Segregation of incompatible duties (SOD) within access control environment

# Change Management Controls (ITGC)

# Change Management Controls - (ITGC)

**Objective:** Only authorized, tested and approved changes are made to applications, databases and operating systems.

- Ensure changes are appropriately requested
- Ensure changes are appropriately authorized
- Ensure changes are appropriately tested and approved before deployment to production environment
- Assess vulnerability scans to determine if vulnerabilities are being remediated in a timely manner
- Segregation of incompatible duties (SOD)

# IT Operation Controls (ITGC)

# IT Operations – Backup- & Recovery (ITGC)

**Objective:** Ensure the availability of information systems and that its operations is correct.

- Data is appropriately backed-up
- Disaster recovery plan
- Production errors are identified and resolved
- Only approved and tested changes are deployed

# System Development Life Cycle (ITGC)

# System Development Life Cycle / Program Development  (ITGC)

**Objective:** Ensure the development of new systems or upgrades does not lead to data corruption

- Ensure changes to systems are appropriately requested & documented
- Ensure changes to systems are appropriately authorized & documented
- Ensure changes are appropriately tested and approved before deployment to production environment
- Issues encountered during the development of the program are monitored and resolved
- Segregation of incompatible duties

# Segregation of Duties (SOD) - IT General Controls (ITGC)

**5. Segregation of Duties** (**SOD**)

Objective: Minimize the occurrence of errors or fraud

- Determine individuals performing control activities do not have conflicting duties
- Determine if incompatible duties have been identified and documented
- Determine if any conflicting roles have been allowed by management and if so, have compensating controls been implemented to minimize the risk?

# IT Application Controls (ITAC)

# IT Application Controls (ITAC) Classification

**Input Controls**

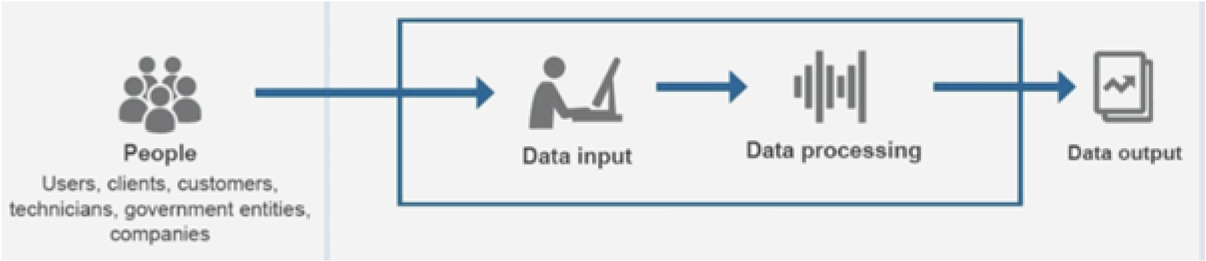
Authenticate information entered into a system.

**Processing Controls**

Verifies information transmitted within systems

**Output Controls**

Validates information being sent out of the system.


People
Users, clients, customers, technicians, government entities, companies
Data input
Data processing
Data output

Controls embedded in applications such as ERP systems (SAP, Oracle, Workday, Microsoft Dynamics)

# IT Application Controls (ITAC)

**Input Controls**

- Check for data accuracy and completeness
  - Data input authorization
  - Data conversion
  - Data editing
  - Error handling

**Processing Controls**

- Rules for processing data
- Data accuracy and completeness

**Output Controls**

- Data accuracy and completeness
- Access authorization

# Testing IT General Controls (ITGC)

# 1. Access Controls Testing

# Access Controls Testing

1. **Test Password Configuration:**

   Determine and obtain evidence of the organization's setting for the following configurations:

   - Minimum password length
   - Initial log-on uses a one-time password
   - 2 Factor Authentication
   - Password complexity (alpha/numeric characters)
   - Frequency of forced password
   - Password reuse history
   - Number of unsuccessful log-on attempts allowed before lockout

# Access Controls Testing

## 2. Test User Access authorization:

- **Access Provisioning for New Users:** Determine that employees are only granted access to data that is appropriate based on their job function and their access approval and obtain evidence of authorization and approval.
- **Access De-Provisioning for Terminated Users:** Determine that terminated users have been removed timely from the systems to prevent unauthorized access to data.
- **Test Transferred Users:** Determine that transferred users are only granted access that is appropriate based on their new job function and that access for their previous function has been removed and deactivated.

# Access Controls Testing

## 3. Test Privilege User Rights:

- Determine if users' sensitive access is appropriate based on their job description/function.
- Determine if activity of high privilege accounts, administrators and sensitive generic accounts are regularly monitored.
- Monitor login attempts, user updates and role changes
- Collect and save audit logs from all sessions
- Host session logs outside of the database they are monitoring
- Who to Evaluate – IT admins and developers, contractors and third -party vendors

# Access Controls Testing

**4. Test Segregation of Incompatible Duties:**

- Determine those individuals performing the control activities over user access do not have conflicting duties.
- Determine that different individual perform the following duties related to logical access – requesting access, approving access, setting up access and monitoring access.

**5. Test that Logical access process is monitored:** Identify relevant monitoring controls and test that the controls functioned as expected.

- Periodic logical access review for continues appropriateness
- Violation or violation attempts reporting and review
- Review of logs (surrounding privilege user access)

# 2. Change Management Controls Testing

# Change Management Controls Testing

**Types of Change Management Controls**

- **System Development/Acquisition (SDLC- system development lifecycle):** Development and implementation of new systems and applications.
- **Program Change:** Changes being made to existing applications, interfaces and DBMS (Database management systems)
- **Maintenance:** Technical changes to DBMS, operating systems and system software
- **Emergency Changes:** Changes made in an emergency. The changes are mostly made directly in production environment and therefor may not have evidence of testing. Change documentation and approval are usually obtained after the fact

# Change Management Controls Testing

- Obtain evidence of change request
- Obtain evidence of authorization and approval before changes are migrated into production environment
- Obtain evidence of testing (UAT Test, Manual and automated tests are performed to validate change functions)
- Test segregation of incompatible duties: Determine that different individuals are performing the following duties:
  - Request /Approve the development or change
  - Program the development or change
  - Move changes in and out of production

# 3. IT Operations - Backup and Recovery

# IT Operations – Backup & Recovery Controls Testing

- **Test Backup:** Data is backed up daily according to a documented schedule and process.
- **Recovery:** Recovery plans for critical systems are in place and tested.
- **Access Restriction:** Access is properly restricted, assuring data is not deleted or altered through the data management process.
- Production errors are identified and resolved
- Physical security measures are in place

# 4. Software Development Life Cycle (SDLC)

# Software Development Life Cycle (SDLC) Controls Testing

- Major improvement to ERP systems is properly tested and approved before migration to production
- Evidence of appropriate requests and approvals
- The new system has the appropriate controls (Access, application, backup)
- Issues encountered during the development of the program are monitored and resolved
- Final signoffs are obtained prior to going live in production

# 5. Segregation of Incompatible Duties (SOD)

# Segregation of Incompatible Duties (SOD) Controls Testing

Generally, the primary incompatible duties that need to be segregated are:

- Authorization or approval
- Custody of assets
- Recording transactions
- Reconciliation/Control Activity

Note: When duties cannot be sufficiently segregated, it is important that mitigating controls such as detailed supervisory review of activities, be put in place to reduce risks.

# Testing IT Application Controls (ITAC)

# IT Application Controls (ITAC) Controls Testing

**There are 3 main types of Application Controls tested:**

- **Input Controls**
  - Controls that governs data input in an application
  - Controls preventing users from entering unvalidated information into the system
  - Controls that ensure data accuracy and integrity
- **Processing Controls**
  - Controls verifying that incoming data is correctly processed before it's added to the information system
  - Establishing rules for processing data
  - Ensuring relevant rules are followed every time data is transmitted

# IT Application Controls (ITAC) Controls Testing

- **Output Controls**
  - Controls safeguarding data when transmitting between applications
  - Controls that ensures data gets sent to the right destination
  - Controls that ensures/confirms data is complete at final destination

**Other Controls**

- Access Controls
- Integrity Controls

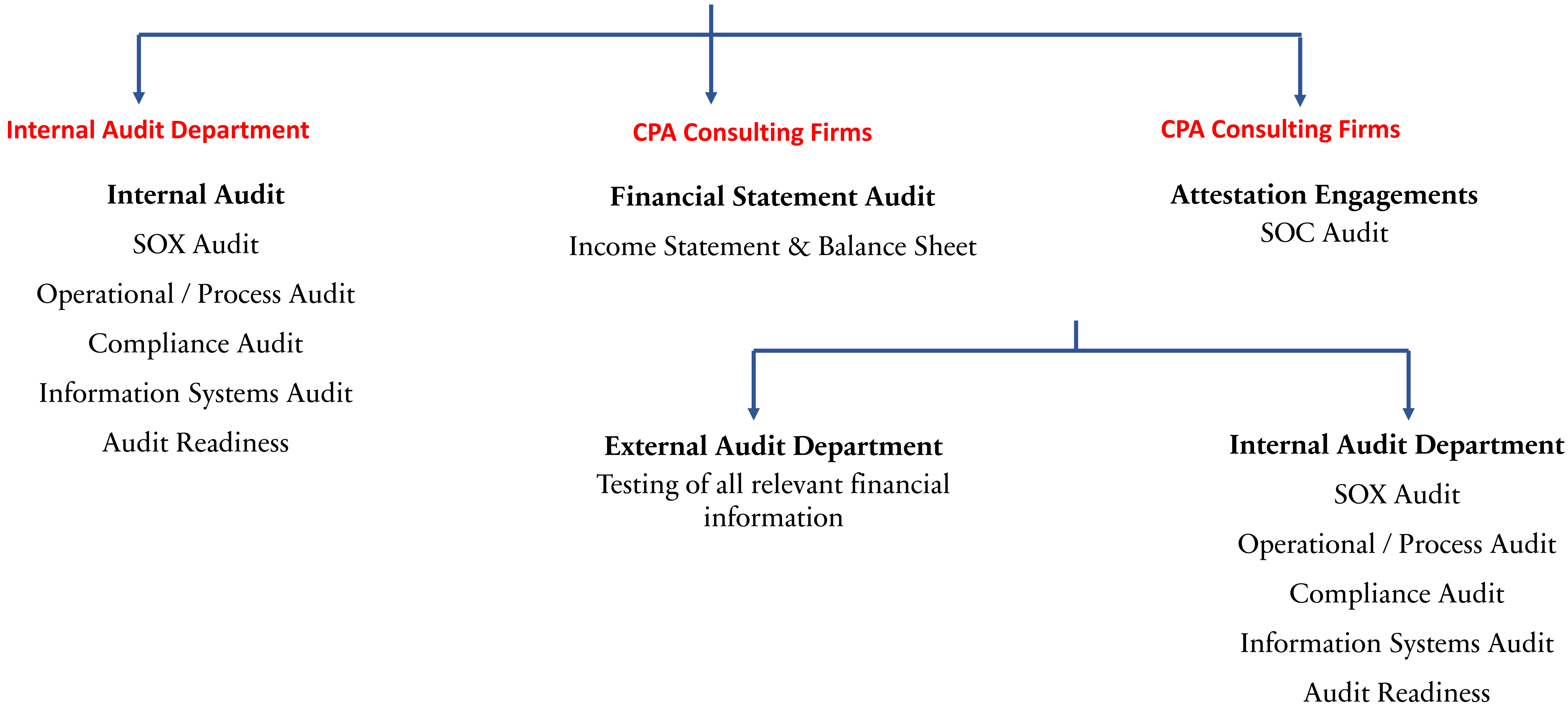
# Internal Audit Department

# Internal Audit – Need to Know

- Internal Audit Department Size: 10 – 25 (depends on the company size)
- Internal Audit Plan: Contains all the types of audits/projects the internal audit plans to execute during the year. Including:
  - Period & priority based on risk assessment of the activities considered for audit
  - Resources needed for the audit
- Audit Program: Detailed step required to test or audit a control
- Audit Committee: An arm of the board of directors generally composed of 3 to 5 members.
- Internal Audit Charter: A formal document that defines internal audit's purpose, authority, responsibility, and position within the organization.
- Engagement Letter: Informs department on what audit will be performed, duration of test
- Risk and Control Matrix: list of controls that will be tested, control objective and description of the client control, risk rating (high, moderate, low)
- Substantive Testing: Conducted when in doubt about the accuracy of information
- Prepared by Client (PBC) List

# IT Audit Process

# IT Audit Process



Internal Audit Department

**Internal Audit**

SOX Audit

Operational / Process Audit

Compliance Audit

Information Systems Audit

Audit Readiness

CPA Consulting Firms

**Financial Statement Audit**

Income Statement & Balance Sheet

CPA Consulting Firms

**Attestation Engagements**

SOC Audit

**External Audit Department**

Testing of all relevant financial information

**Internal Audit Department**

SOX Audit

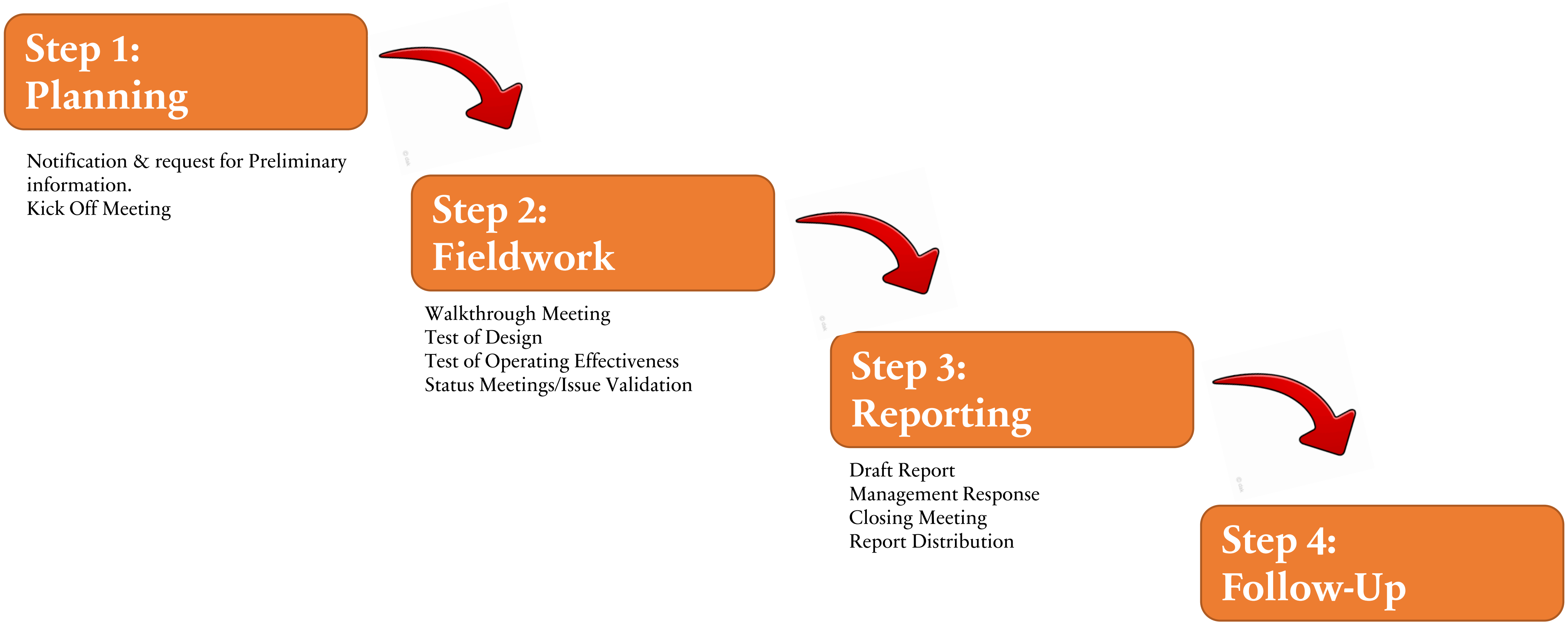
Operational / Process Audit

Compliance Audit

Information Systems Audit

Audit Readiness

# IT Audit Process



**Step 1: Planning**

Notification & request for Preliminary information.
Kick Off Meeting

**Step 2: Fieldwork**

Walkthrough Meeting
Test of Design
Test of Operating Effectiveness
Status Meetings/Issue Validation

**Step 3: Reporting**

Draft Report
Management Response
Closing Meeting
Report Distribution

**Step 4: Follow-Up**

# Planning Stage

- Determine the audit **objective**, **scope**, risk considerations and evidence to be collected

**Objective** – Why are we conducting this review?

To evaluate, to determine, to assess that there is:

- Compliance with policies
- Achievement of goals
- Reliability of data or documents
- Efficient use of resources
- Safeguard of assets

**Scope** – Where and when?

- Remote / On-premise
- Time period / duration of audit
- Parameters - Specific areas of review
- Sample size
- Sampling methodology

# Planning Stage

- Determine the audit objective, scope, risk considerations and evidence to be collected
- Controls to be tested are selected from established internal control program or control matrix
- Review past audit workpaper
- Selecting testing team members and assigning of work and responsibilities
- Create Audit request / PBC List (Prepared by Client List) from controls being tested
- Notification & request for preliminary information & documents
- Conduct Audit Kick-off meeting:
  - Audit period
  - Questions about the PBC List / requested documents
  - Concerns needed to be addressed

**Note:** We can obtain/pull some or most of the requested items ourselves during fieldwork.

# Fieldwork Stage

- Schedule meetings with department personnel or head to discuss the audit request
- Conduct a **Walkthrough** to understand the process/system
- **Test the design of the controls**
- **Test effectiveness of the controls** by selecting a sample (usually 10% of the transactions up to a maximum of 25 samples)
- Conduct status meetings with client/department – progress/delays/needs/audit findings validation
- Conduct weekly internal status meeting within internal audit (IA) team – status/progress/deliverables

# Walkthrough - Fieldwork Stage

- Walkthrough is the examination of a process from initiation to completion
- Examine if internal controls are properly designed
- Identify risk of material misstatement
- As we perform a walkthrough, we:
    - Make inquiries
    - Inspect process or documents
    - Make observations

# Reporting Stage

- Prepare a draft report - list of audit findings or control weaknesses found with related risk statement
- Conduct exit meeting / exit memo
- Request response from management
- Distribute final audit report

# Follow-Up Stage

- Follow-up to determine if control weaknesses have been corrected
- Obtain evidence / re-test control
- Close the deficiency

# Identifying Control Weaknesses

# Identifying Control Weaknesses

**Control Gap**

**No Control in place -** i.e., No one at the cash registry

**Control Design**

**Control not Designed Appropriately** – i.e., Surveillance camera not capturing night image

**Control Effectiveness**

**Control not Operating Effectively** – i.e., Procedures not consistently followed

# Key Control
# vs
# Non-Key Control

# Key Control vs Non-Key Control (Secondary Control)

**Key Control**

Material impact on the financial statement

**Non-Key Control**

Non-material impact on the financial Statement

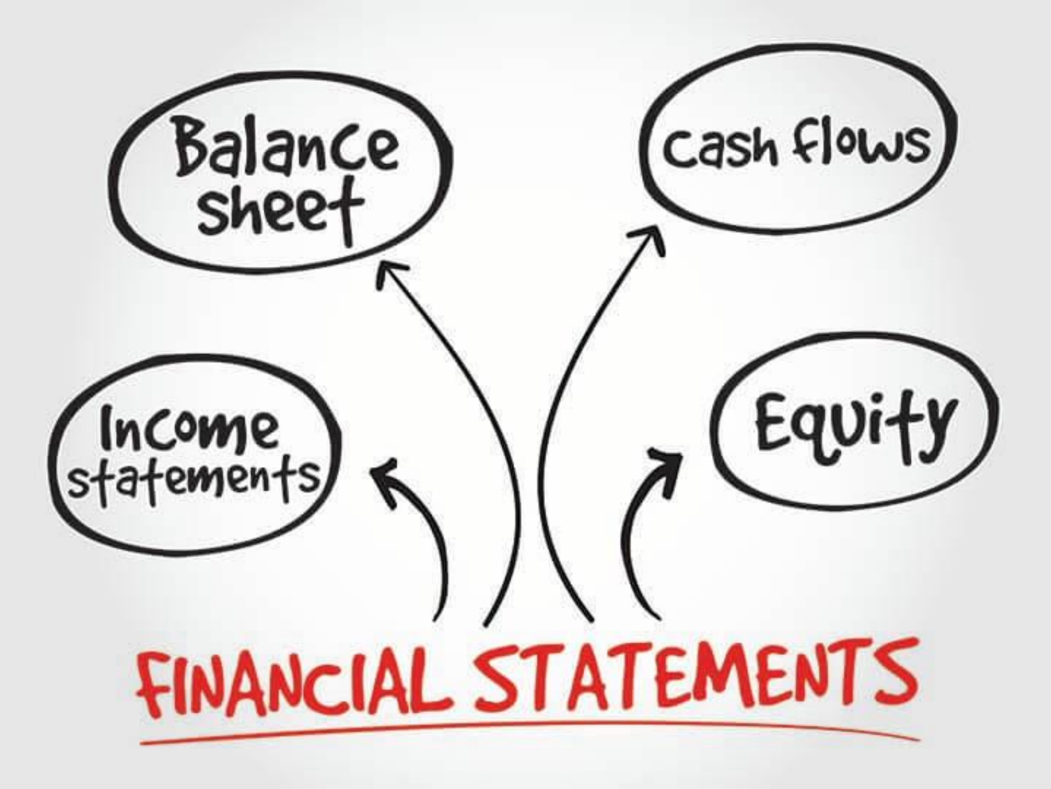
A material misstatement is information in the financial statements that is sufficiently incorrect that it may impact the economic decisions of someone relying on those statements.

# Key Control vs Non-Key Control (Secondary Control)

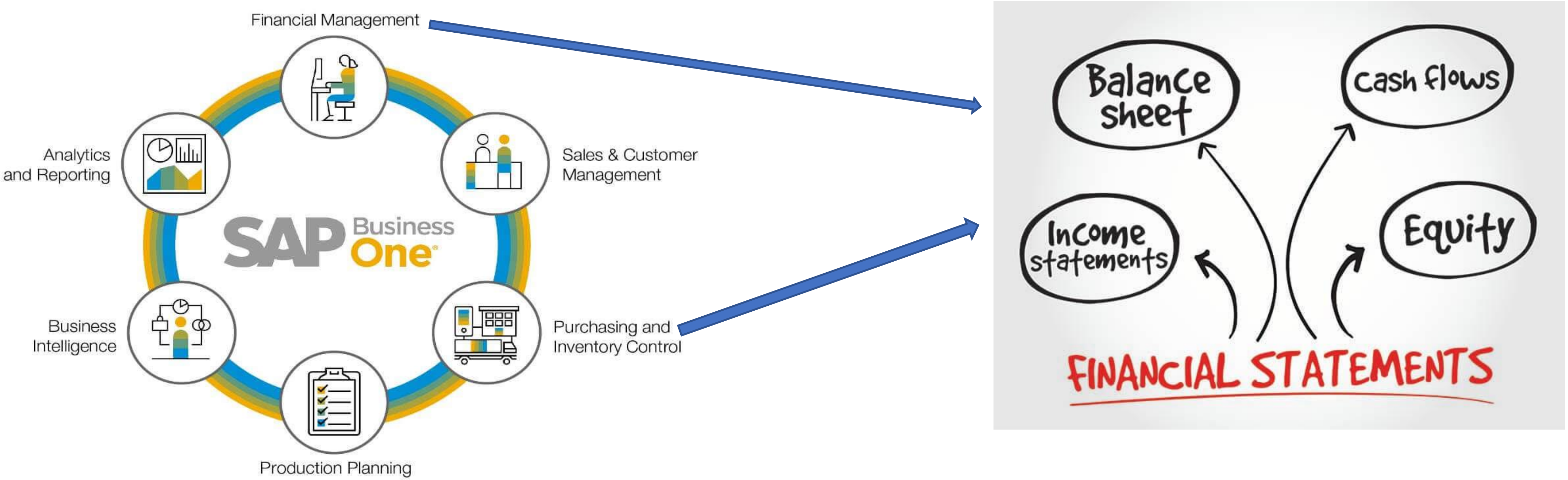
- Follow-up to determine if control weaknesses have been corrected
- Obtain evidence / re-test control
- Close the deficiency

# Financially Significant Applications/Controls

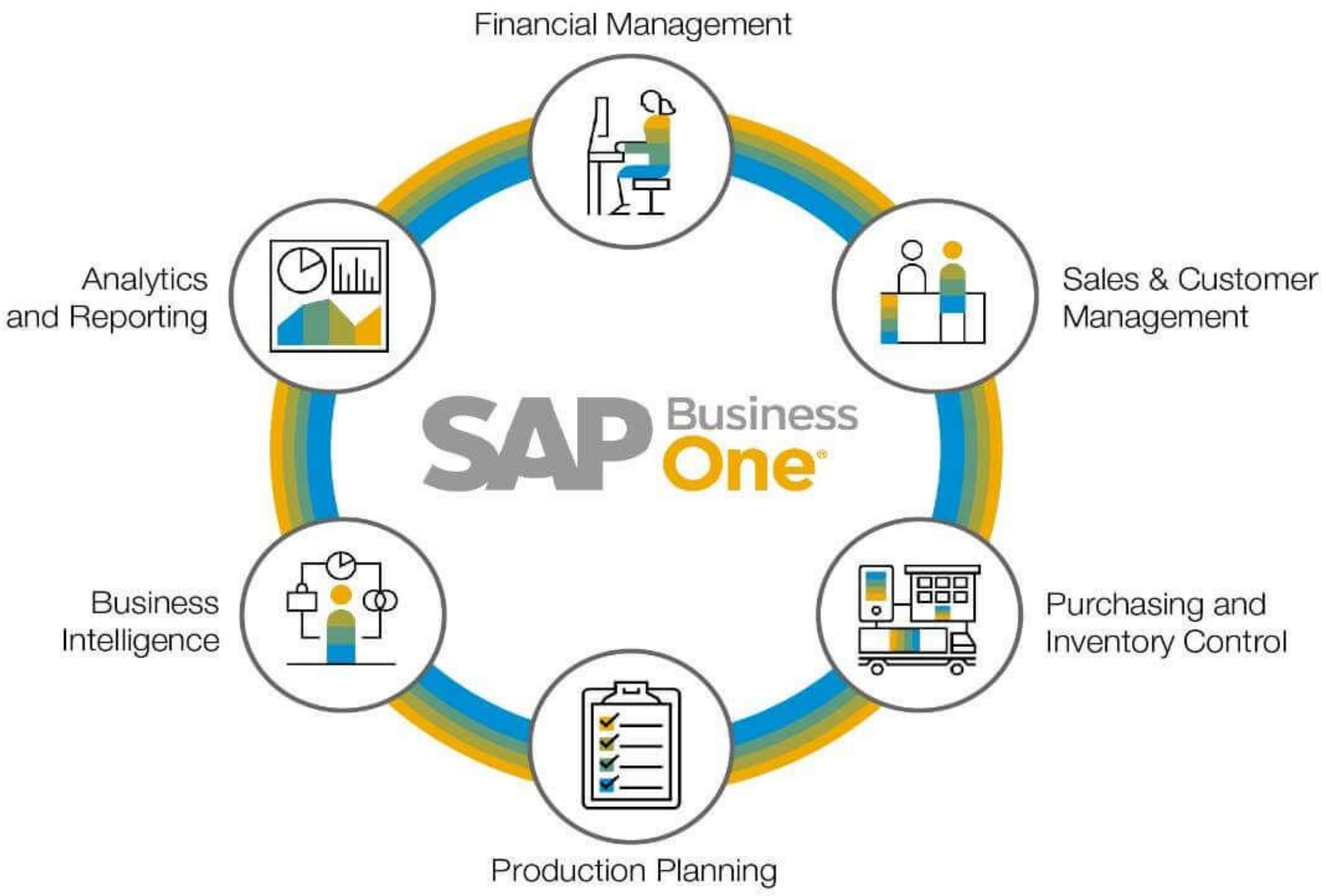
# Financially Significant Applications/Controls



# Financially Significant Applications/Controls



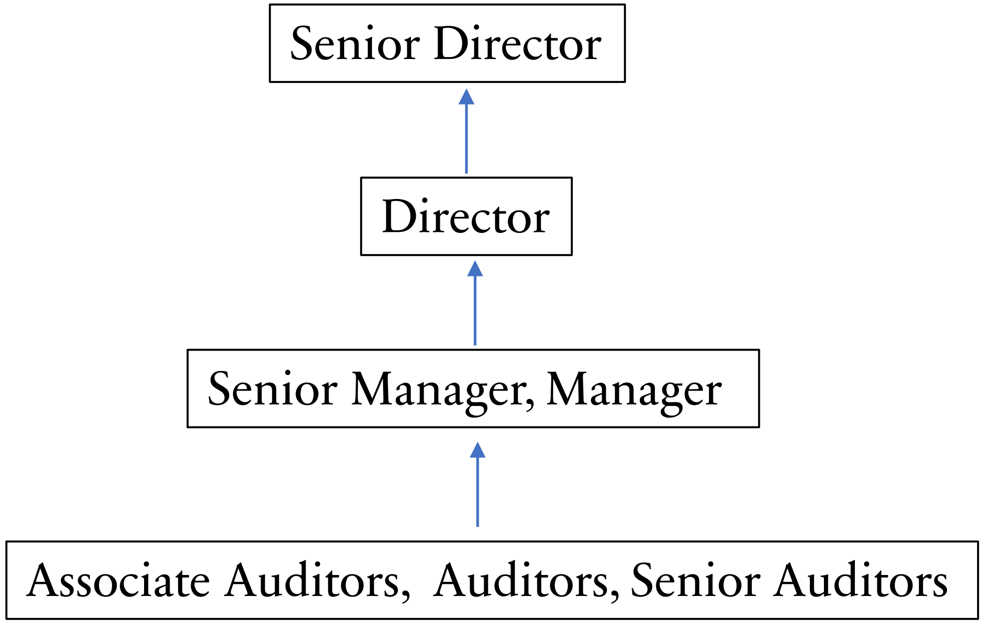
# Financially Significant Applications/Controls



# Internal Audit Team

# Internal Audit Team

- Team Size: 10 to 25 Auditors



Senior Director

Director

Senior Manager, Manager

Associate Auditors, Auditors, Senior Auditors

# Working Papers

# Working Papers

Documentation/Evidence of :

- Auditors' process
- Auditors' findings
- Auditors' conclusion

Importance:

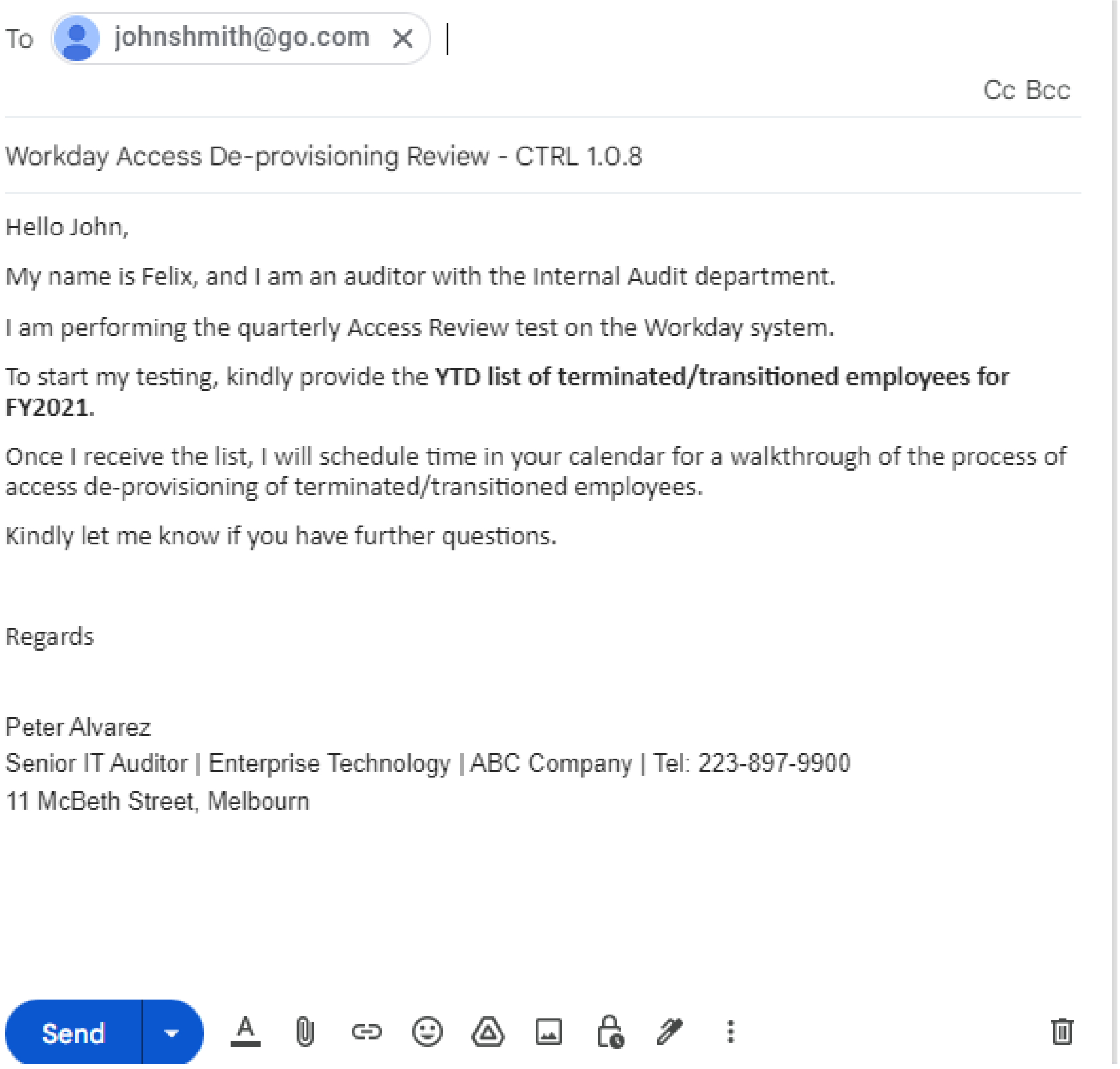
- Support the audit final report
- Used for future audits

# Performing an IT Audit

# Planning

# Planning Phase

- Determine the audit objective, scope and other considerations
- Controls to be tested are selected from established internal control program or control matrix
- Selecting testing team members and assigning of work and responsibilities
- Review past audit workpaper and test steps
- Notification & request for preliminary information & documents / PBC List (Prepared by Client List)
- Conduct Audit Kick-off meeting:
    - Audit Objectives
    - Audit Scope
    - Questions about the PBC List / requested documents
    - Concerns needed to be addressed



To johnshmith@go.com

Workday Access De-provisioning Review - CTRL 1.0.8

Hello John,

My name is Felix, and I am an auditor with the Internal Audit department.

I am performing the quarterly Access Review test on the Workday system.

To start my testing, kindly provide the **YTD list of terminated/transitioned employees for FY2021.**

Once I receive the list, I will schedule time in your calendar for a walkthrough of the process of access de-provisioning of terminated/transitioned employees.

Kindly let me know if you have further questions.

Regards

Peter Alvarez
Senior IT Auditor | Enterprise Technology | ABC Company | Tel: 223-897-9900
11 McBeth Street, Melbourn

# Fieldwork

# Fieldwork Phase

- Schedule meetings with department personnel or head to discuss the audit request
- Conduct a **Walkthrough** to understand the process/system
- **Test effectiveness of the controls** by selecting a sample (usually 10% of the transactions up to a maximum of 25 samples)
- Conduct status meetings with client/department – progress/delays/needs/audit findings validation
- Conduct weekly internal status meeting within internal audit (IA) team – status/progress/deliverables

# Walkthrough - Fieldwork Phase

- Walkthrough is the examination of a process from initiation to completion
- As we perform a walkthrough, we:
  - Inspect process or documents
  - Ask questions
  - Make observations
- Examine if internal controls are properly designed
- Identify control gaps and risk of material misstatement
- Test a single transaction
- In person or remotely (Zoom, Teams, Google Meet)

**Note:** Walkthrough is not always done during fieldwork

# Access Controls Testing

# Access Controls Testing

IT Audit

Testing IT General & IT Application Controls

Test the Design & Effectiveness of the Controls

Reasonable Assurance of no Financial Misstatements

# IT General Controls (ITGC)

1. Access Controls – Logical & Physical
2. Change Management Controls
3. IT Operations – Backup & Recovery
4. System Development Life Cycle (SDLC)

# Access Controls Testing

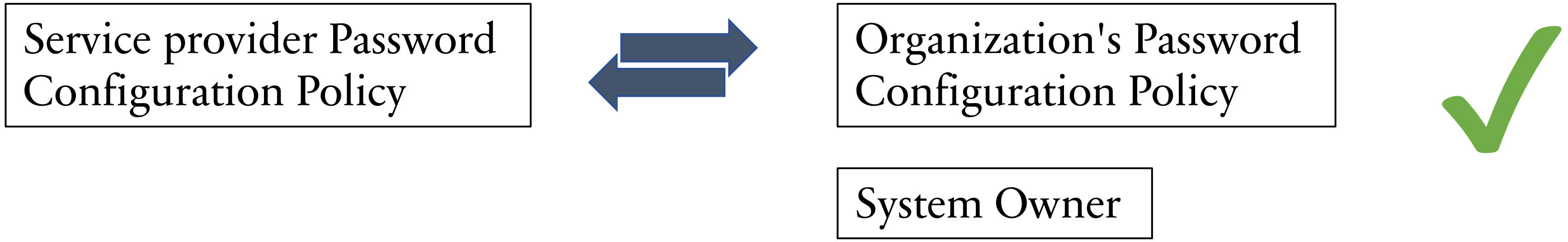
- Test passwords are correctly configured
- Test User Access authorization
  - Access provisioning
  - Access deprovisioning
- Test Privileged Users & Generic Ids
- Test Segregation of Duties (SOD)

# Password Configuration - Access Controls Testing

**Test Password Are Correctly Configured:**

- Confirm one-time password for initial log on to application
- Verify password length has a minimum of 8 characters
- Verify password composition contains alpha/numeric characters
- Determine if Multi-Factor Authentication (MFA) is used to login
- Confirm password history prior to reusing a password
- Determine limit on the number of unsuccessful attempts to sign on

# Password Configuration Test Result



Service provider Password Configuration Policy

Organization's Password Configuration Policy

System Owner

✓

Service Provider Policy:
**Password length minimum of 6 characters**

Organization’s Policy:
**Password length must have a minimum of 8 characters**

# User Access Authorization

## User Access Authorization - Access Controls Testing

# Test of Control Design

# User Access Authorization - Access Controls Testing

**Access Provisioning:**

- Determine access approval process
- Obtain evidence of access request/approval from appropriate persons
- Determine who can grant access to system/application i.e., System Administrator, manual or automated
- Verify that employees are only granted access to systems/application in line with job function
- Verify that access granted by the system administrator is in line with approval
- Inform the system owner on the next steps in the audit process

# User Access Authorization - Access Controls Testing

## Test of Control Effectiveness

# User Access Authorization - Access Controls Testing

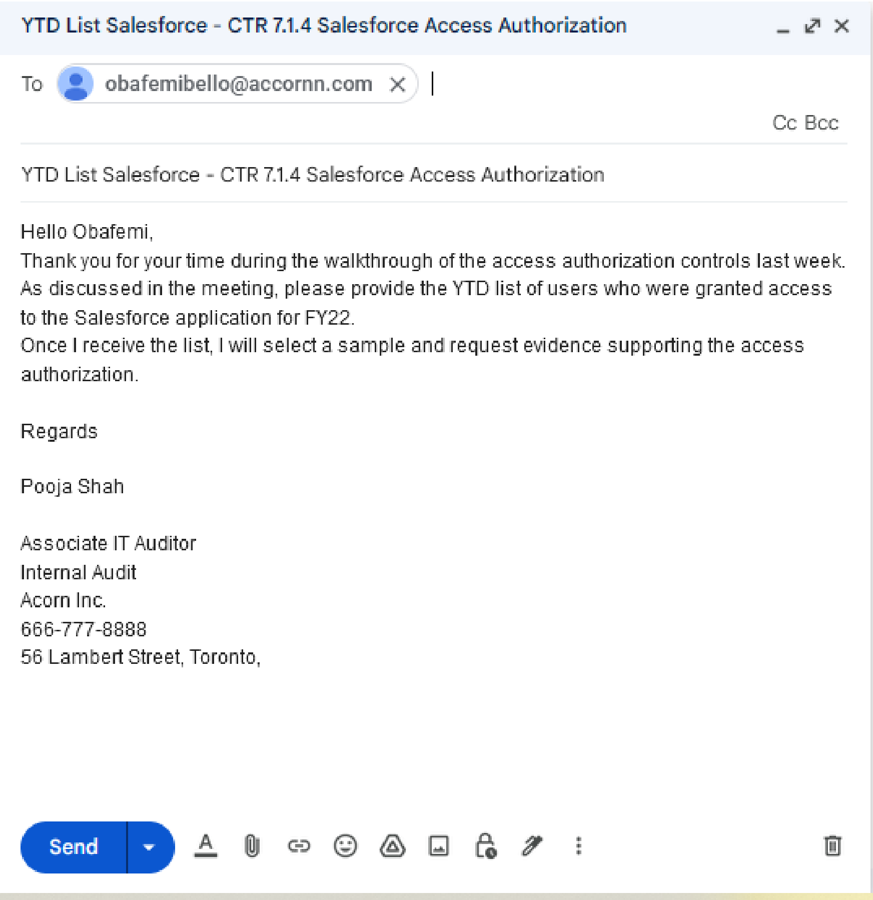
**Access Provisioning:**

- Request list of access granted within audit period
- Select sample from population to test (10% to max of 25 transactions)
- Obtain evidence of access request/approval from appropriate persons
- Verify that employees were only granted access to systems/application in line with job function
- Verify that access granted by the system administrator is in line with approval

# User Access Authorization - Access Controls Testing

## Access Provisioning Test:

- Request list of access granted within audit period



YTD List Salesforce - CTR 7.1.4 Salesforce Access Authorization

To obafemibello@accornn.com

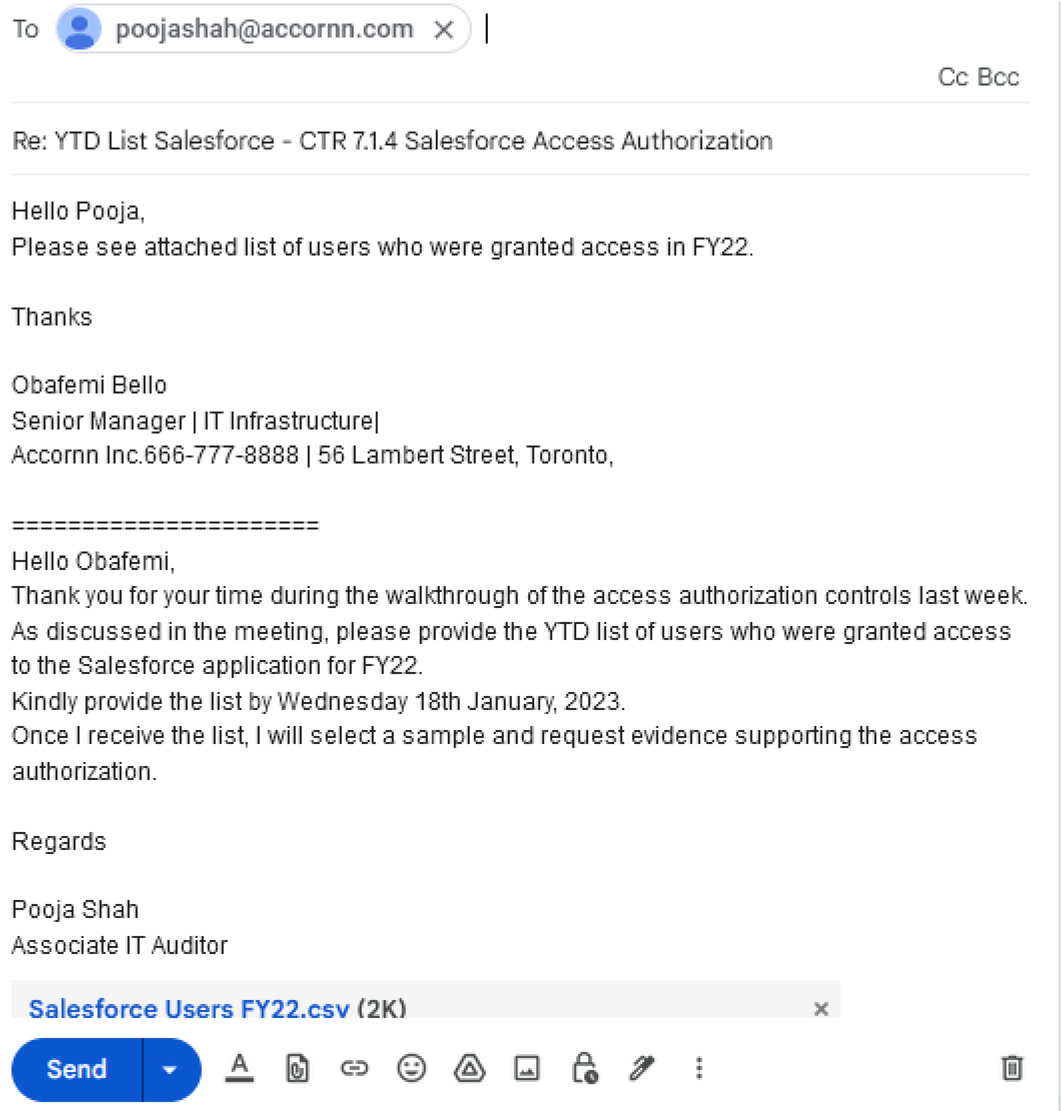
YTD List Salesforce - CTR 7.1.4 Salesforce Access Authorization

Hello Obafemi,
Thank you for your time during the walkthrough of the access authorization controls last week.
As discussed in the meeting, please provide the YTD list of users who were granted access to the Salesforce application for FY22.
Once I receive the list, I will select a sample and request evidence supporting the access authorization.

Regards

Pooja Shah

Associate IT Auditor
Internal Audit
Acorn Inc.
666-777-8888
56 Lambert Street, Toronto,



To poojashah@accornn.com

Re: YTD List Salesforce - CTR 7.1.4 Salesforce Access Authorization

Hello Pooja,
Please see attached list of users who were granted access in FY22.

Thanks

Obafemi Bello
Senior Manager | IT Infrastructure|
Accornn Inc.666-777-8888 | 56 Lambert Street, Toronto,

======================
Hello Obafemi,
Thank you for your time during the walkthrough of the access authorization controls last week.
As discussed in the meeting, please provide the YTD list of users who were granted access to the Salesforce application for FY22.
Kindly provide the list by Wednesday 18th January, 2023.
Once I receive the list, I will select a sample and request evidence supporting the access authorization.

Regards

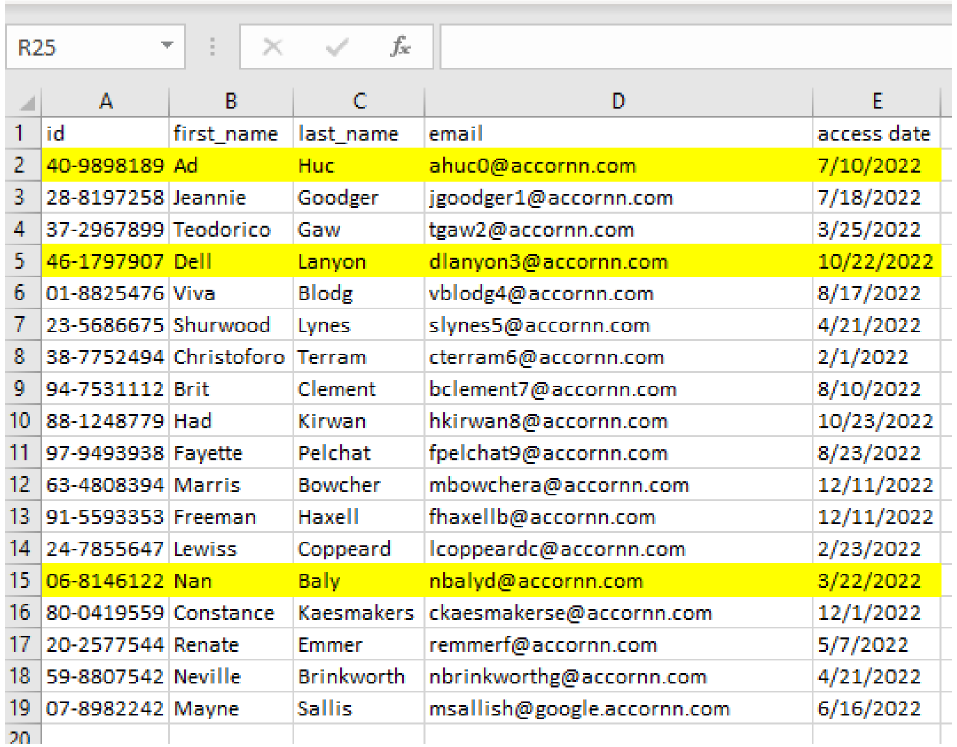
Pooja Shah
Associate IT Auditor

Salesforce Users FY22.csv (2K)

# User Access Authorization - Access Controls Testing

## Access Provisioning:

- Select sample from population to test (10% to max of 25 transactions)

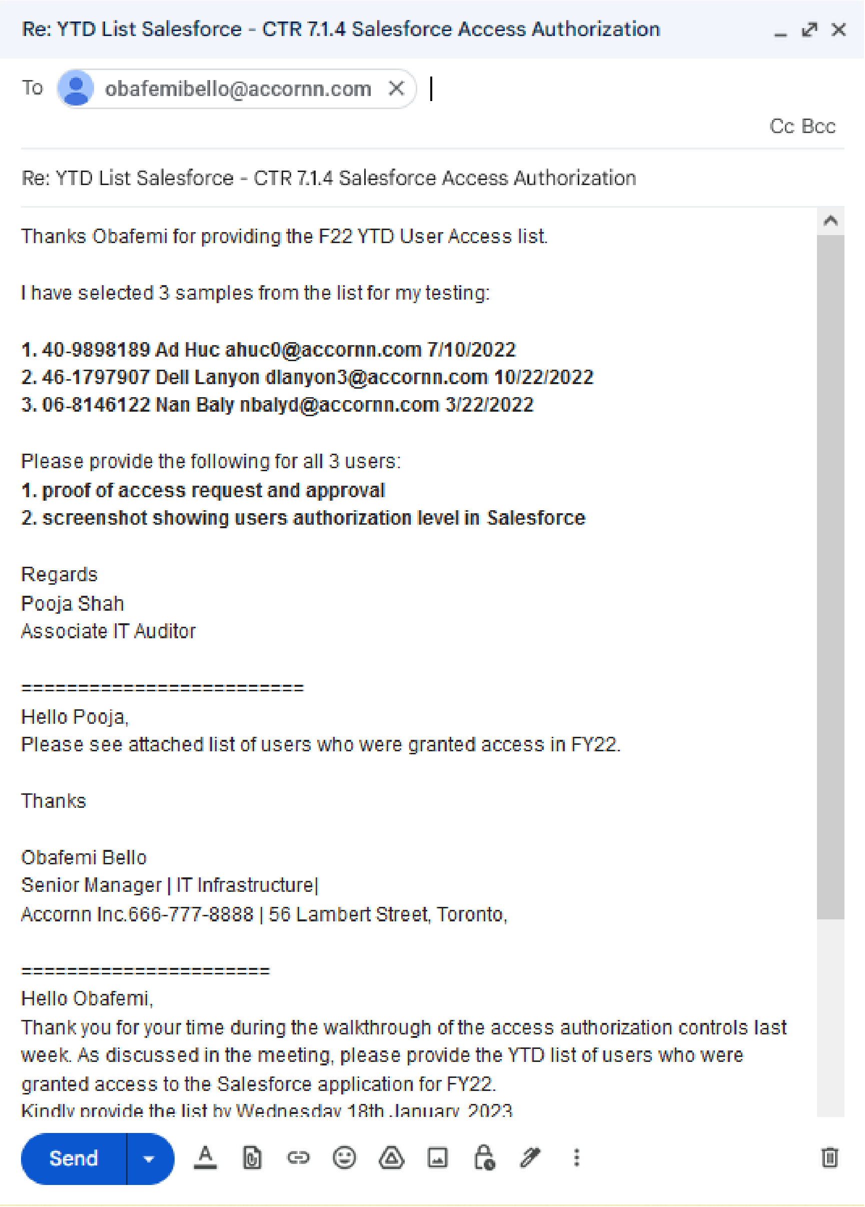


| | A | B | C | D | E |
|---|---|---|---|---|---|
| 1 | id | first_name | last_name | email | access date |
| 2 | 40-9898189 | Ad | Huc | ahuc0@accornn.com | 7/10/2022 |
| 3 | 28-8197258 | Jeannie | Goodger | jgoodger1@accornn.com | 7/18/2022 |
| 4 | 37-2967899 | Teodorico | Gaw | tgaw2@accornn.com | 3/25/2022 |
| 5 | 46-1797907 | Dell | Lanyon | dlanyon3@accornn.com | 10/22/2022 |
| 6 | 01-8825476 | Viva | Blodg | vblodg4@accornn.com | 8/17/2022 |
| 7 | 23-5686675 | Shurwood | Lynes | slynes5@accornn.com | 4/21/2022 |
| 8 | 38-7752494 | Christoforo | Terram | cterram6@accornn.com | 2/1/2022 |
| 9 | 94-7531112 | Brit | Clement | bclement7@accornn.com | 8/10/2022 |
| 10 | 88-1248779 | Had | Kirwan | hkirwan8@accornn.com | 10/23/2022 |
| 11 | 97-9493938 | Fayette | Pelchat | fpelchat9@accornn.com | 8/23/2022 |
| 12 | 63-4808394 | Marris | Bowcher | mbowchera@accornn.com | 12/11/2022 |
| 13 | 91-5593353 | Freeman | Haxell | fhaxellb@accornn.com | 12/11/2022 |
| 14 | 24-7855647 | Lewiss | Coppeard | lcoppeardc@accornn.com | 2/23/2022 |
| 15 | 06-8146122 | Nan | Baly | nbalyd@accornn.com | 3/22/2022 |
| 16 | 80-0419559 | Constance | Kaesmakers | ckaesmakerse@accornn.com | 12/1/2022 |
| 17 | 20-2577544 | Renate | Emmer | remmerf@accornn.com | 5/7/2022 |
| 18 | 59-8807542 | Neville | Brinkworth | nbrinkworthg@accornn.com | 4/21/2022 |
| 19 | 07-8982242 | Mayne | Sallis | msallish@google.accornn.com | 6/16/2022 |
| 20 | | | | | |

# User Access Authorization - Access Controls Testing

## Access Provisioning:

- Obtain evidence of access request/approval from appropriate persons
- Verify that employees were only granted access to systems/application in line with job function
- Verify that access granted by the system administrator is in line with approval



Re: YTD List Salesforce - CTR 7.1.4 Salesforce Access Authorization

To obafemibello@accornn.com

Re: YTD List Salesforce - CTR 7.1.4 Salesforce Access Authorization

Thanks Obafemi for providing the F22 YTD User Access list.

I have selected 3 samples from the list for my testing:

**1. 40-9898189 Ad Huc ahuc0@accornn.com 7/10/2022**
**2. 46-1797907 Dell Lanyon dlanyon3@accornn.com 10/22/2022**
**3. 06-8146122 Nan Baly nbalyd@accornn.com 3/22/2022**

Please provide the following for all 3 users:
**1. proof of access request and approval**
**2. screenshot showing users authorization level in Salesforce**

Regards
Pooja Shah
Associate IT Auditor

=========================
Hello Pooja,
Please see attached list of users who were granted access in FY22.

Thanks

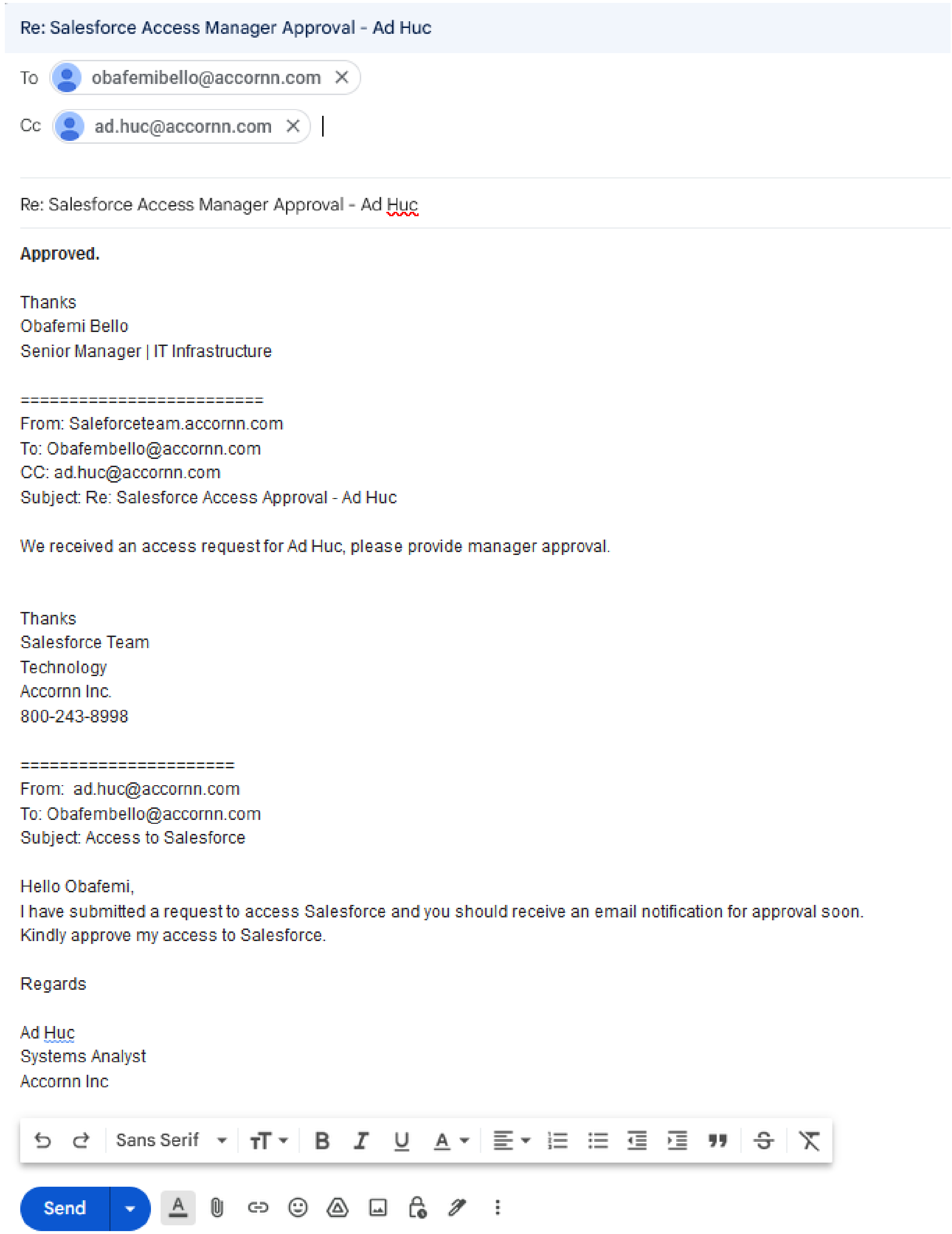
Obafemi Bello
Senior Manager | IT Infrastructure|
Accornn Inc.666-777-8888 | 56 Lambert Street, Toronto,

======================
Hello Obafemi,
Thank you for your time during the walkthrough of the access authorization controls last week. As discussed in the meeting, please provide the YTD list of users who were granted access to the Salesforce application for FY22.
Kindly provide the list by Wednesday 18th January 2023

# User Access Authorization - Access Controls Testing

## Access Provisioning:

- Obtain evidence of access request/approval from appropriate persons
- Verify that employees were only granted access to systems/application in line with job function
- Verify that access granted by the system administrator is in line with approval



Re: Salesforce Access Manager Approval - Ad Huc

To obafemibello@accornn.com

Cc ad.huc@accornn.com

Re: Salesforce Access Manager Approval - Ad Huc

**Approved.**

Thanks
Obafemi Bello
Senior Manager | IT Infrastructure

========================
From: Saleforceteam.accornn.com
To: Obafembello@accornn.com
CC: ad.huc@accornn.com
Subject: Re: Salesforce Access Approval - Ad Huc

We received an access request for Ad Huc, please provide manager approval.

Thanks
Salesforce Team
Technology
Accornn Inc.
800-243-8998

=====================
From:  ad.huc@accornn.com
To: Obafembello@accornn.com
Subject: Access to Salesforce

Hello Obafemi,
I have submitted a request to access Salesforce and you should receive an email notification for approval soon.
Kindly approve my access to Salesforce.

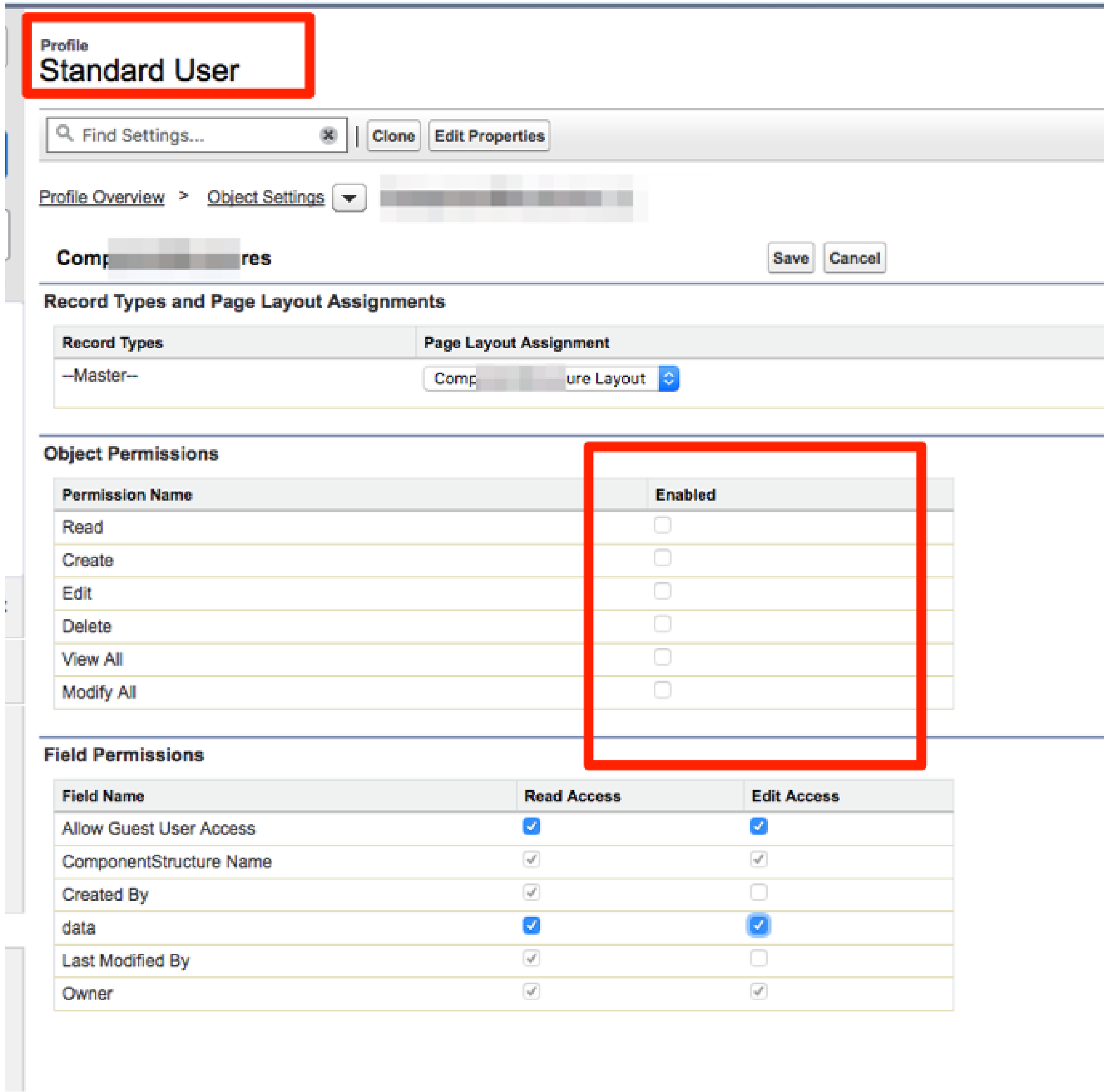
Regards

Ad Huc
Systems Analyst
Accornn Inc

# User Access Authorization - Access Controls Testing

## Access Provisioning:

- Obtain evidence of access request/approval from appropriate persons
- Verify that employees were only granted access to systems/application in line with job function
- Verify that access granted by the system administrator is in line with approval



Profile
Standard User

Profile Overview > Object Settings [redacted]

Comp[redacted]res

Record Types and Page Layout Assignments

| Record Types | Page Layout Assignment |
|---|---|
| --Master-- | Comp[redacted]ure Layout |

Object Permissions

| Permission Name | Enabled |
|---|---|
| Read | □ |
| Create | □ |
| Edit | □ |
| Delete | □ |
| View All | □ |
| Modify All | □ |

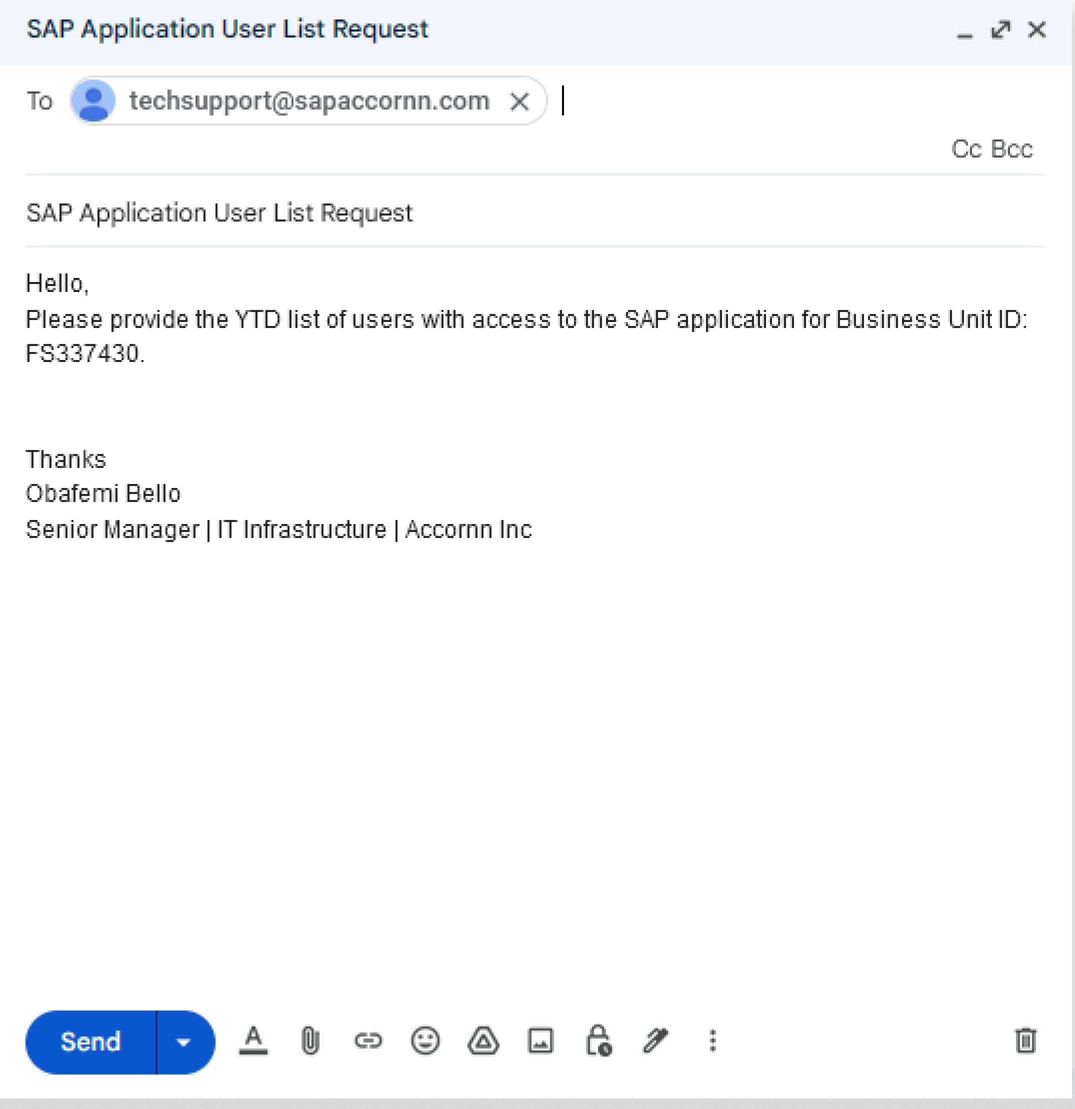
Field Permissions

| Field Name | Read Access | Edit Access |
|---|---|---|
| Allow Guest User Access | ☑ | ☑ |
| ComponentStructure Name | ✓ | ✓ |
| Created By | ✓ | □ |
| data | ☑ | ☑ |
| Last Modified By | ✓ | □ |
| Owner | ✓ | ✓ |

# User Access Authorization - Access Controls Testing

## Access Deprovisioning:

- Request evidence of review of application user list



SAP Application User List Request

To techsupport@sapaccornn.com

SAP Application User List Request

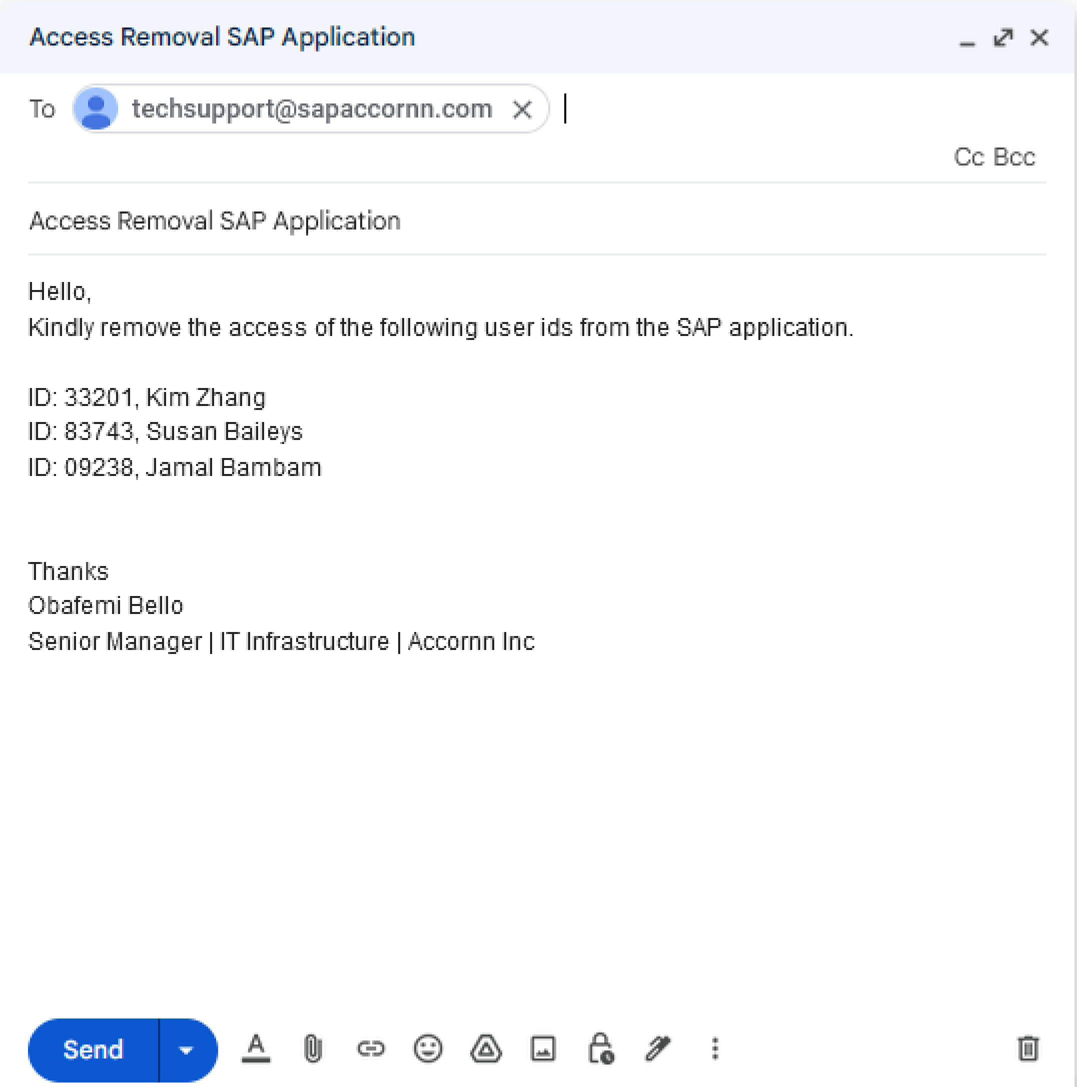
Hello,
Please provide the YTD list of users with access to the SAP application for Business Unit ID: FS337430.

Thanks
Obafemi Bello
Senior Manager | IT Infrastructure | Accornn Inc

# User Access Authorization - Access Controls Testing

## Access Deprovisioning:

- Obtain evidence user access to be removed was identified
- Obtain evidence of access removal request



Access Removal SAP Application

To techsupport@sapaccornn.com

Access Removal SAP Application

Hello,
Kindly remove the access of the following user ids from the SAP application.

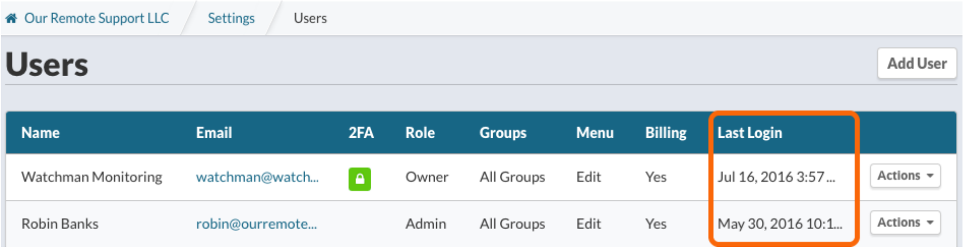
ID: 33201, Kim Zhang
ID: 83743, Susan Baileys
ID: 09238, Jamal Bambam

Thanks
Obafemi Bello
Senior Manager | IT Infrastructure | Accornn Inc

# User Access Authorization - Access Controls Testing

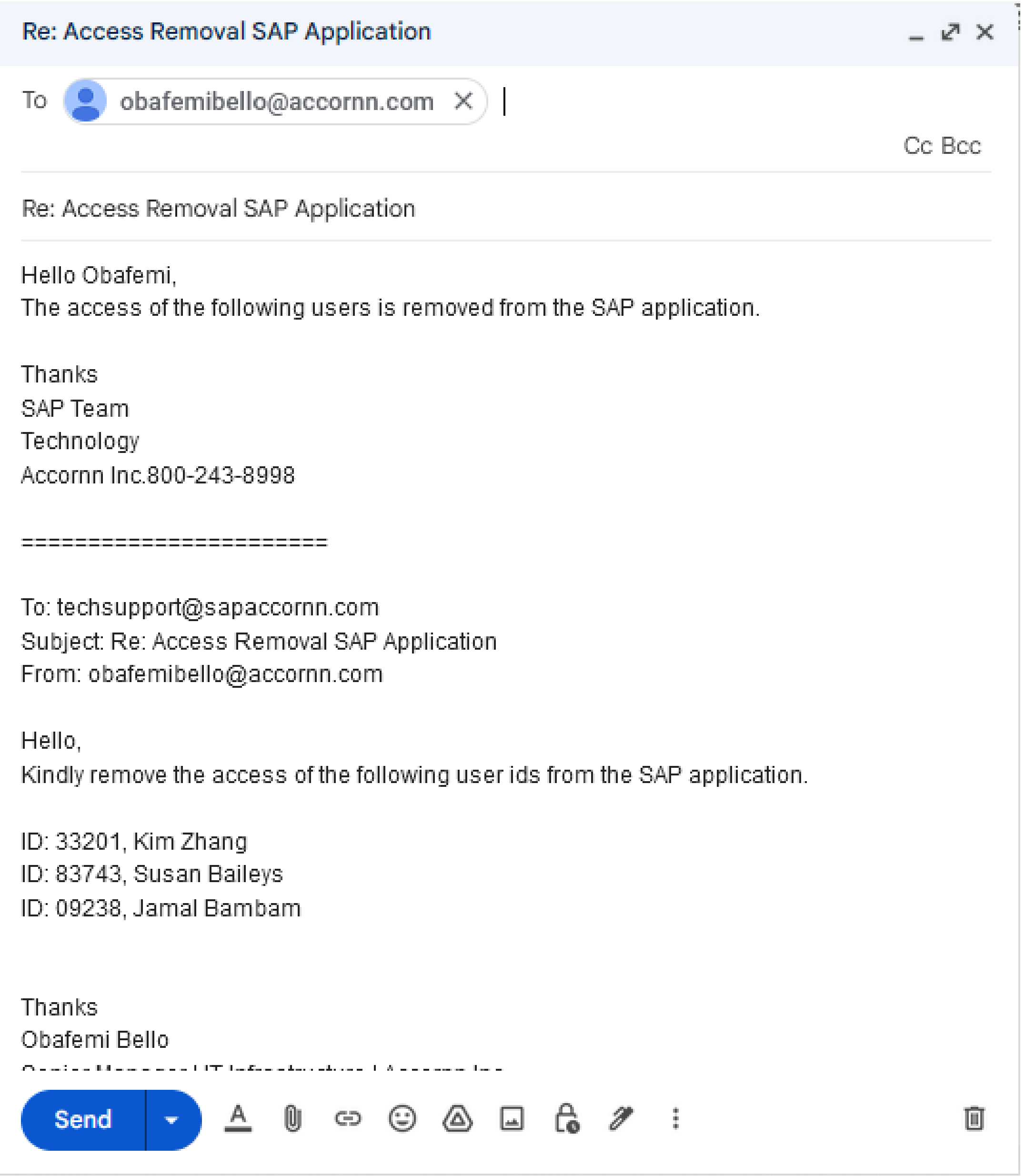
## Access Deprovisioning:

- Obtain evidence that the right access was removed



### Users

| Name | Email | 2FA | Role | Groups | Menu | Billing | Last Login | |
|---|---|---|---|---|---|---|---|---|
| Watchman Monitoring | watchman@watch... | 🔒 | Owner | All Groups | Edit | Yes | Jul 16, 2016 3:57... | Actions |
| Robin Banks | robin@ourremote... | | Admin | All Groups | Edit | Yes | May 30, 2016 10:1... | Actions |



Re: Access Removal SAP Application

To obafemibello@accornn.com

Re: Access Removal SAP Application

Hello Obafemi,
The access of the following users is removed from the SAP application.

Thanks
SAP Team
Technology
Accornn Inc.800-243-8998

=======================

To: techsupport@sapaccornn.com
Subject: Re: Access Removal SAP Application
From: obafemibello@accornn.com

Hello,
Kindly remove the access of the following user ids from the SAP application.

ID: 33201, Kim Zhang
ID: 83743, Susan Baileys
ID: 09238, Jamal Bambam

Thanks
Obafemi Bello

# Privileged Access -

## Privileged Users & Generic IDs

# Privileged Access

**Privileged Access:** Special access or abilities above and beyond a standard user

**Privileged User:**

Systems Administrator

Database Administrators

IT Administrator

Developers

**Generic ID/Privileged Account:**

System configuration

Application configuration

Administrative actions

# Privileged Access Testing

- Human are your weakest link
- Systems Network
- Access sensitive data
- Cyber Attacks

Privileged Access Testing

# Test of Control Design

# Privileged Access Testing

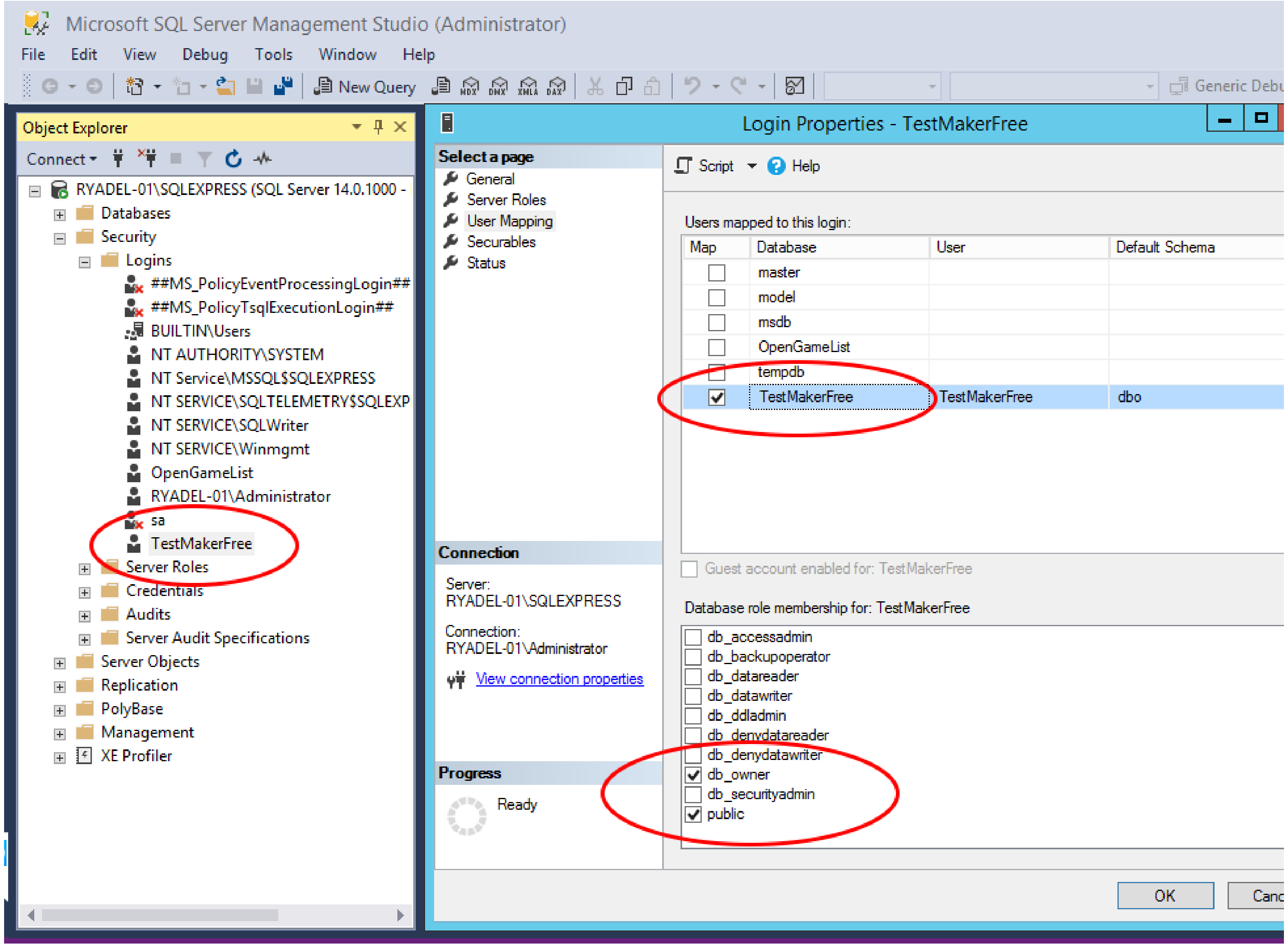
**Privileged User Access & Generic ID:**

- Determine Access approval process

# Privileged Access Testing

**Privileged User Access & Generic ID:**

- Determine Access approval process
- Select 1 privileged user



Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Generic Debu
Object Explorer
Connect

- RYADEL-01\SQLEXPRESS (SQL Server 14.0.1000 -
  - Databases
  - Security
    - Logins
      - ##MS_PolicyEventProcessingLogin##
      - ##MS_PolicyTsqlExecutionLogin##
      - BUILTIN\Users
      - NT AUTHORITY\SYSTEM
      - NT Service\MSSQL$SQLEXPRESS
      - NT SERVICE\SQLTELEMETRY$SQLEXP
      - NT SERVICE\SQLWriter
      - NT SERVICE\Winmgmt
      - OpenGameList
      - RYADEL-01\Administrator
      - sa
      - TestMakerFree
    - Server Roles
    - Credentials
    - Audits
    - Server Audit Specifications
  - Server Objects
  - Replication
  - PolyBase
  - Management
  - XE Profiler

Login Properties - TestMakerFree

Users mapped to this login:

| Map | Database | User | Default Schema |
|---|---|---|---|
| □ | master | | |
| □ | model | | |
| □ | msdb | | |
| □ | OpenGameList | | |
| □ | tempdb | | |
| ☑ | TestMakerFree | TestMakerFree | dbo |

□ Guest account enabled for: TestMakerFree

Database role membership for: TestMakerFree

□ db_accessadmin
□ db_backupoperator
□ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter
☑ db_owner
□ db_securityadmin
☑ public

Connection

Server:
RYADEL-01\SQLEXPRESS

Connection:
RYADEL-01\Administrator

View connection properties

Progress

Ready

# Privileged Access Testing

**Privileged User Access & Generic ID:**

- Determine Access approval process
- Select 1 privileged user
- Determine if users' sensitive access is appropriate based on their job description/function
- Obtain evidence of access request/approval from appropriate persons
- Determine if activity of high privilege accounts, administrators and sensitive generic accounts are regularly monitored
    - Monitor login attempts, user updates and role changes
    - Collect logs from all sessions
    - Track privileged activities
    - Monitor and analyze threats
    - Multi Factor Authentication (MFA)

## Privileged Access Testing

# Test of Control Effectiveness

# Privileged Access Testing

**Privileged User Access & Generic ID :**

- Request list of privileged access granted within audit period
- Select sample from population to test (10% to max of 25 transactions)
- Obtain evidence of formal request for privileged access
- Obtain evidence of privileged access approval from appropriate persons
- Verify that employees were only granted access to systems/application in line with job function
- Verify that access granted by the system administrator is in line with approval

# Segregation Of Duties (SOD)

# Segregation of Duties (SOD)

- Applicable to all aspect of ITGC & ITAC
- Individuals performing certain control activities should not have conflicting duties.
- Segregation of Duties help minimize error or fraud
- Segregation of Duties involves separating three main functions:
  - Having custody of assets
  - Being able to authorize the use of assets
  - Recordkeeping of assets

# Segregation of Duties (SOD) Testing

- Determine that individuals performing the control activities over user access do not have conflicting duties
- Determine that different individual perform the following duties related to logical access:
  - Requesting access
  - Approving access
  - Setting up access
  - Monitoring access
- Obtain evidence of compensating controls where Segregation of Duties cannot be achieved

# Change Management Controls Testing

# Change Management

- Change Management: Process by which changes (application code and infrastructure) are introduced into a production IT environment.
- Performed in a controlled and repeatable manner
- Changes include bug fixes, new features, system upgrades and patching

# Change Management Controls Testing

- Determine the process to make changes
- Determine what type of change is being tested i.e.  Emergency Change or Maintenance
- Obtain evidence of change request
- Obtain evidence of authorization and approval before changes are migrated into production environment
- Obtain evidence of testing (UAT signoff, QA signoff)
- Test segregation of incompatible duties: Determine that different individuals are performing the following duties:
    - Request /Approve the development or change
    - Program the development or change
    - Move changes in and out of production

# IT Operations – Backup & Recovery Testing

# IT Operations – Backup & Recovery Controls Testing

- Confirm if backups are done
- Determine the frequency of data backups
- Obtain evidence of completeness and accuracy of data
- Determine if recovery plans for critical systems are in place and tested
- Determine if there is adequate access restriction for backup data
- Production errors are identified and resolved

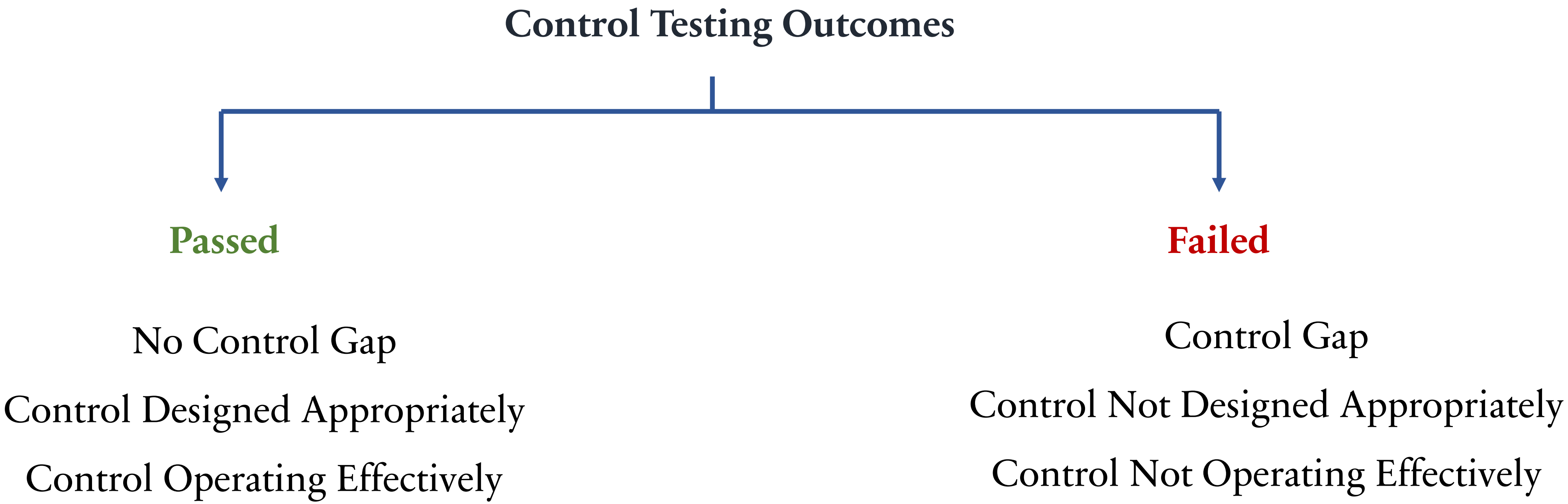
# System Development Life Cycle (SDLC) Controls Testing

# System Development Life Cycle (SDLC) Controls Testing

- Inquire about the process of SDLC
- Obtain evidence of formal request and approval for improvement to ERP systems
- Obtain evidence of testing and approval before migration to production
- Obtain evidence that the new system has the appropriate controls (Access, Application, Backup)
- Obtain evidence that issues encountered during the development of the program are monitored and resolved
- Obtain evidence of final signoffs prior to going live in production

# IT Audit Testing Outcomes

# IT Audit Testing Outcomes



**Control Testing Outcomes**

**Passed**

No Control Gap

Control Designed Appropriately

Control Operating Effectively

**Failed**

Control Gap

Control Not Designed Appropriately

Control Not Operating Effectively

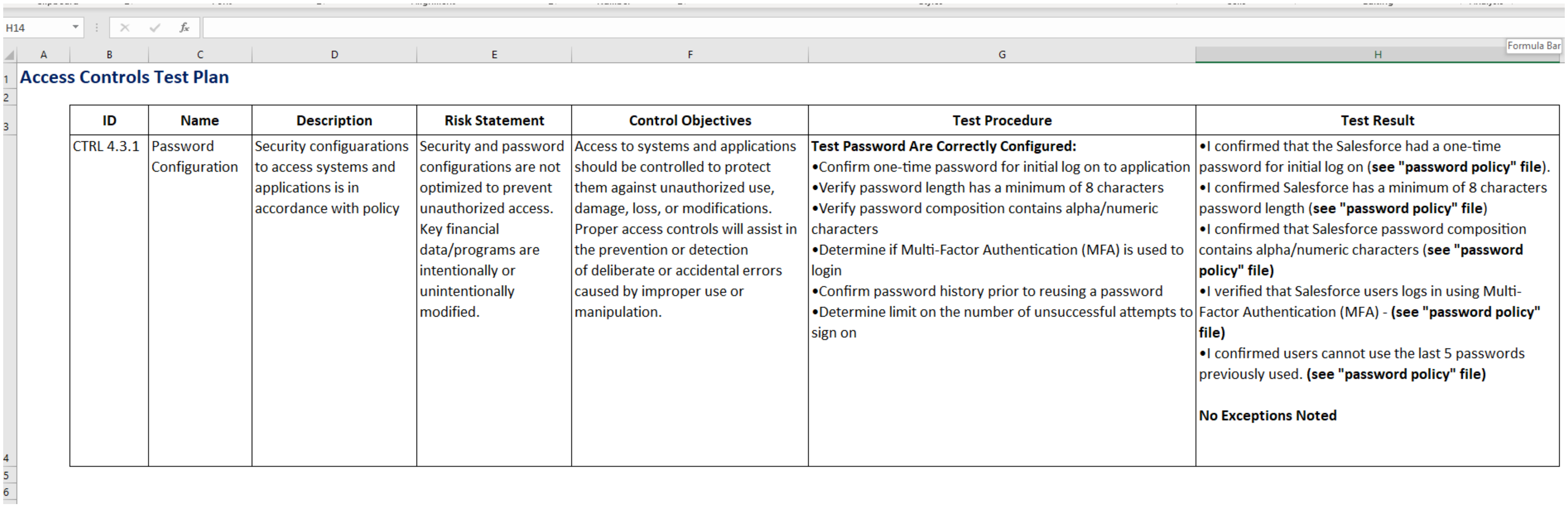
**Control Deficiency**

Control deficiency exists when the design or operation of a control is incapable of preventing or detecting errors on a timely basis (This may lead to a financial misstatement).

# Reporting Phase

# Reporting Format – Internal Audit Department

- Document test steps & results using Excel, Google Sheets, Word, PowerPoint
- IT Audit software applications – Auditboard, monitorQA, iAuditor, Highbond etc..



## Access Controls Test Plan

| ID | Name | Description | Risk Statement | Control Objectives | Test Procedure | Test Result |
|---|---|---|---|---|---|---|
| CTRL 4.3.1 | Password Configuration | Security configuarations to access systems and applications is in accordance with policy | Security and password configurations are not optimized to prevent unauthorized access. Key financial data/programs are intentionally or unintentionally modified. | Access to systems and applications should be controlled to protect them against unauthorized use, damage, loss, or modifications. Proper access controls will assist in the prevention or detection of deliberate or accidental errors caused by improper use or manipulation. | **Test Password Are Correctly Configured:**<br>•Confirm one-time password for initial log on to application<br>•Verify password length has a minimum of 8 characters<br>•Verify password composition contains alpha/numeric characters<br>•Determine if Multi-Factor Authentication (MFA) is used to login<br>•Confirm password history prior to reusing a password<br>•Determine limit on the number of unsuccessful attempts to sign on | •I confirmed that the Salesforce had a one-time password for initial log on (**see "password policy" file**).<br>•I confirmed Salesforce has a minimum of 8 characters password length (**see "password policy" file**)<br>•I confirmed that Salesforce password composition contains alpha/numeric characters (**see "password policy" file)**<br>•I verified that Salesforce users logs in using Multi-Factor Authentication (MFA) - **(see "password policy" file)**<br>•I confirmed users cannot use the last 5 passwords previously used. **(see "password policy" file)**<br><br>**No Exceptions Noted** |

# Reporting Control Deficiency

# Examples of Deficiencies

- **Access Controls**
  - Poor user access review
  - Password not properly configured
  - Inadequate role-based access control
  - User access not revoked at all or not revoked timely
  - No segregation of duties between approver and implementer
- **Change Management Controls**
  - Lack of documented change management policies and procedures
  - Inadequate change approval process
  - Lack of testing and validation
  - Inadequate monitoring and reporting
  - No segregation of duties between approver and implementer

## Examples of Deficiencies

- IT Operations – Backup & recovery Controls
  - No backup procedures
  - Inadequate backup frequency
  - Insufficient backup retention
  - Lack of backup testing
  - No disaster recovery plan

- System Development Life Cycle (SDLC) Controls
  - Lack of Formal SDLC Process
  - Insufficient Testing
  - Lack of Code Review
  - Inadequate Change Management processes
  - Poorly Managed Dependencies

## Types of Control Deficiencies

**Control Deficiency:** Shortcoming in some aspects (principle, attribute, components) of the system of internal control, and no compensating controls and has the potential to adversely affect the ability of the organization to achieve its objectives.

**Material Weakness:** Deficiency or combination of deficiencies, in internal control such there is a reasonable possibility that a material misstatement of financial statements will not be prevented, detected, or corrected on a timely basis.

**Significant Deficiency:** A deficiency or combination of deficiencies less severe than a material weakness, yet may be important enough to merit attention by the board of directors. Multiple significant deficiencies when considered collectively may result in a determination that a material weakness exists.

# Risk Level of Control Weaknesses

| **Control Weakness** | **Risk Level** | **Action** |
|---|---|---|
| Control Deficiency | Low | Client can take time to correct |
| Significant Deficiency | Medium | Need to be corrected as soon as possible & management needs to know about it |
| Material Weakness | High | Need to be corrected immediately & management needs to know about it |

# Audit Report

- Prepare a draft report - list of audit findings or control weaknesses found with related risk statement
- Audit team reviews the audit report
- Draft report sent to management
- Conduct exit meeting or request response from management
- Final changes made to audit report
- Distribute final audit report

# Deficiency Remediation Process

- Identify the control deficiency
- Evaluate the severity of the deficiency
- Audit team notifies management of control weaknesses
- Management develops a remediation plan
- Assign corrective tasks – Control owner
- Establish timelines
- Management & relevant stakeholders implement remediation plan.
- Management monitors the effectiveness of the remediation
- Management reports on the remediation
- Audit team retest the control
- Audit team closes the deficiency
- Audit team documents or issues a report on the operation and effectiveness of the control

# Service Organization Controls (SOC) Audit

# Service Organization Controls (SOC) Audit

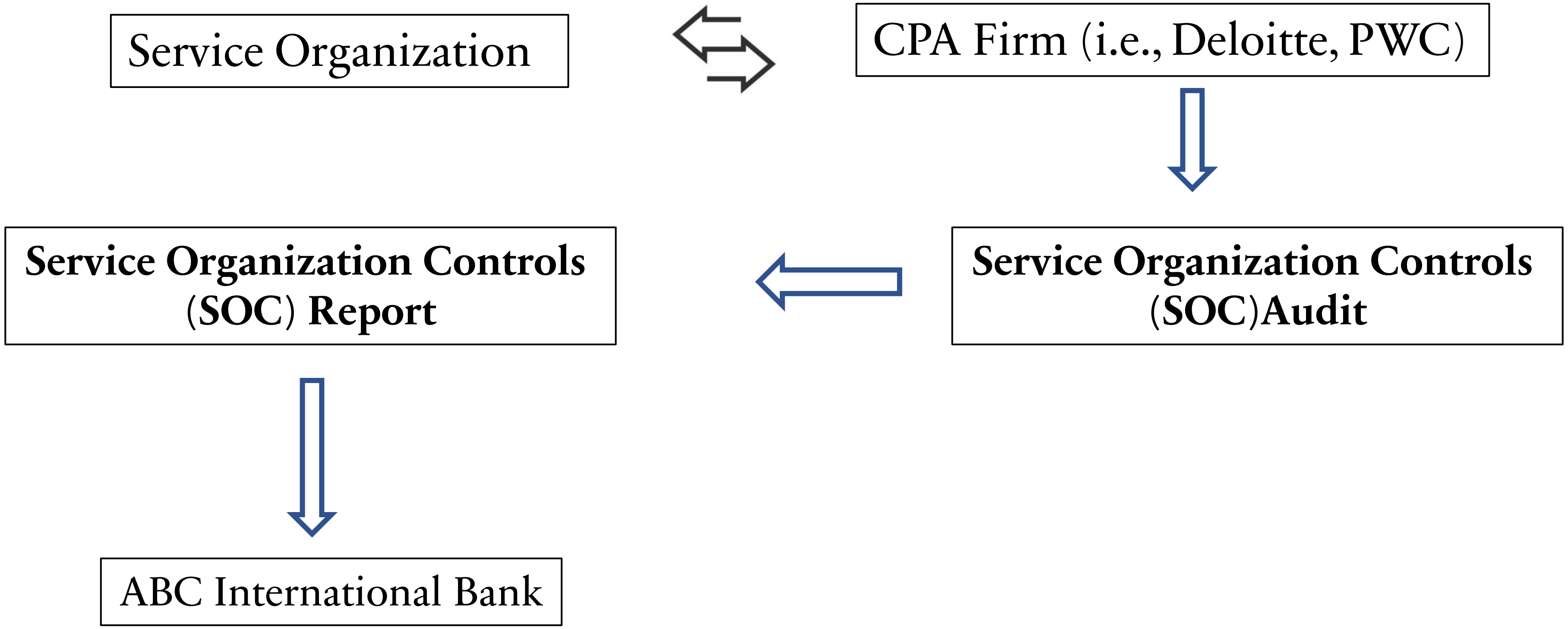
ABC Intercontinental Bank

Cloud
APP
APPLICATION

# Service Organization Controls (SOC) Audit

- What reasonable assurance do we have to rely on the service providers?
  - Ans: Test their internal controls X

# Service Organization Controls (SOC) Audit



Service Organization

CPA Firm (i.e., Deloitte, PWC)

**Service Organization Controls (SOC)Audit**

**Service Organization Controls (SOC) Report**

ABC International Bank

# Categories of SOC Audit

SOC 1

SOC 2

SOC 3

# SOC Audit Categories

- **SOC 1**: Test internal controls over financial reporting (ICFR)
- **SOC 2:** Test internal controls relevant to:
  - Security
  - Availability
  - Privacy
  - Confidentiality
  - Processing integrity

Contains sensitive information and not shared widely or shared under “Non-Disclosure Agreements” (NDA’s)

- **SOC 3:** Test controls relevant:
  - Security
  - Availability
  - Privacy
  - Confidentiality
  - Processing integrity.

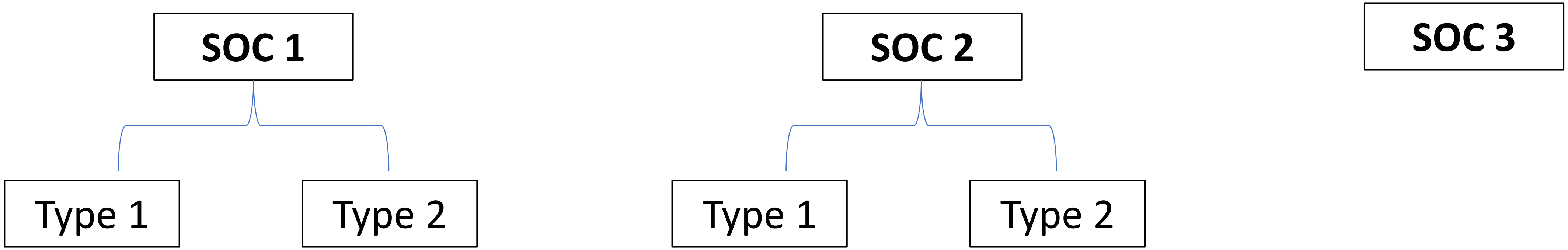
Provides high level information and shared publicly

# SOC Audit Types

**Type I:** Describe the controls the service providers have in place and report the auditor's opinion on the suitability of the controls. Testing is not done on the controls. The auditor does not give an opinion on whether the controls are working effectively.

**Type II:** Test the design and operating effectiveness of controls over a period – Typically 12 consecutive calendar months. More rigorous and intensive than Type I as it covers a greater span of time and requires a more thorough investigation of system designs and processes.

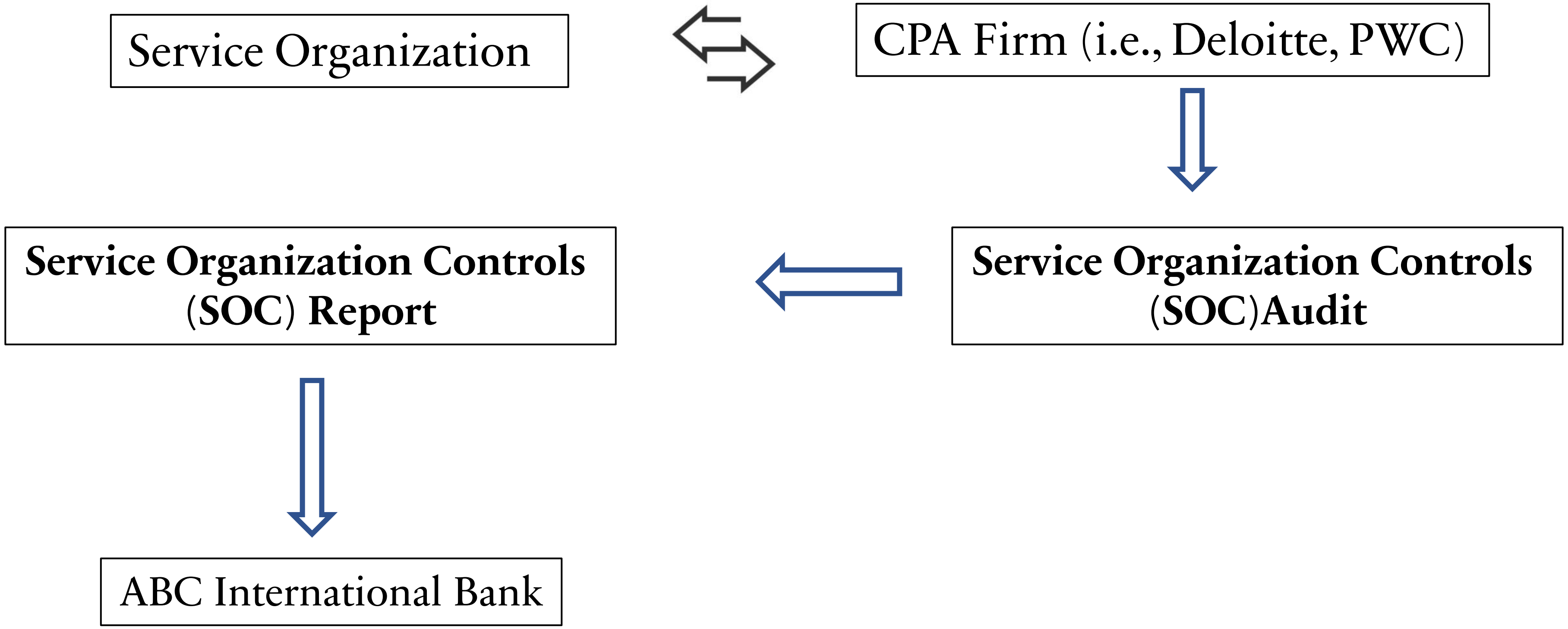
# SOC Audits/SOC Reports



| Category | Scope |
|---|---|
| SOC 1 | Financial statement controls |
| SOC 2 | Security, Availability, Privacy, Confidentiality, Integrity (**Private report**) |
| SOC 3 | Security, Availability, Privacy, Confidentiality, Integrity (**Public report**) |

| Report Type | Tests |
|---|---|
| Type 1 | Suitability of controls |
| Type 2 | Suitability & effectiveness of controls |

# Service Organization Controls (SOC) Audit



Service Organization

CPA Firm (i.e., Deloitte, PWC)

**Service Organization Controls (SOC)Audit**

**Service Organization Controls (SOC) Report**

ABC International Bank

# Service Organization Controls (SOC) Testing

# SOC 2 Requirements

- **Security:** Access controls, firewalls, and other operational/governance controls to protect data and applications.
- **Availability:** Focuses on minimum downtime and requires demonstrating that systems meet operational uptime and performance standards.
- **Privacy:** Protection of Personal Identifiable Information (PII) from breaches and unauthorized access .
- **Confidentiality:** Requires demonstrating ability to identify and safeguard confidential information throughout its life cycle.
- **Process Integrity:** Assesses whether cloud data is processed accurately, reliable and on time and if the systems achieve their purpose.

# SOC 2 Controls Testing

## Security Controls Testing

- Access Controls - Logical & Physical Access Controls
- Systems & Operational Controls
- Change Management Controls
- Risk Mitigation Controls
- Intrusion Detection Systems
- Anti-virus/malware
- Firewalls

# SOC 2 Controls Testing

## Availability Controls Testing

- **Test controls around:**
  - Infrastructure & Capacity Monitoring
  - Backups & Replication
  - Business Continuity & Disaster Recovery Plan

# SOC 2 Controls Testing

## Confidentiality Controls Testing

- **Test controls around:**
  - Identify and maintains confidential information
  - Disposes confidential information to meet objectives related to confidentiality
- Possible internal controls to test:
  - Encryptions
  - Access controls
  - Network/Application firewalls

# SOC 2 Controls Testing

## Privacy Controls Testing

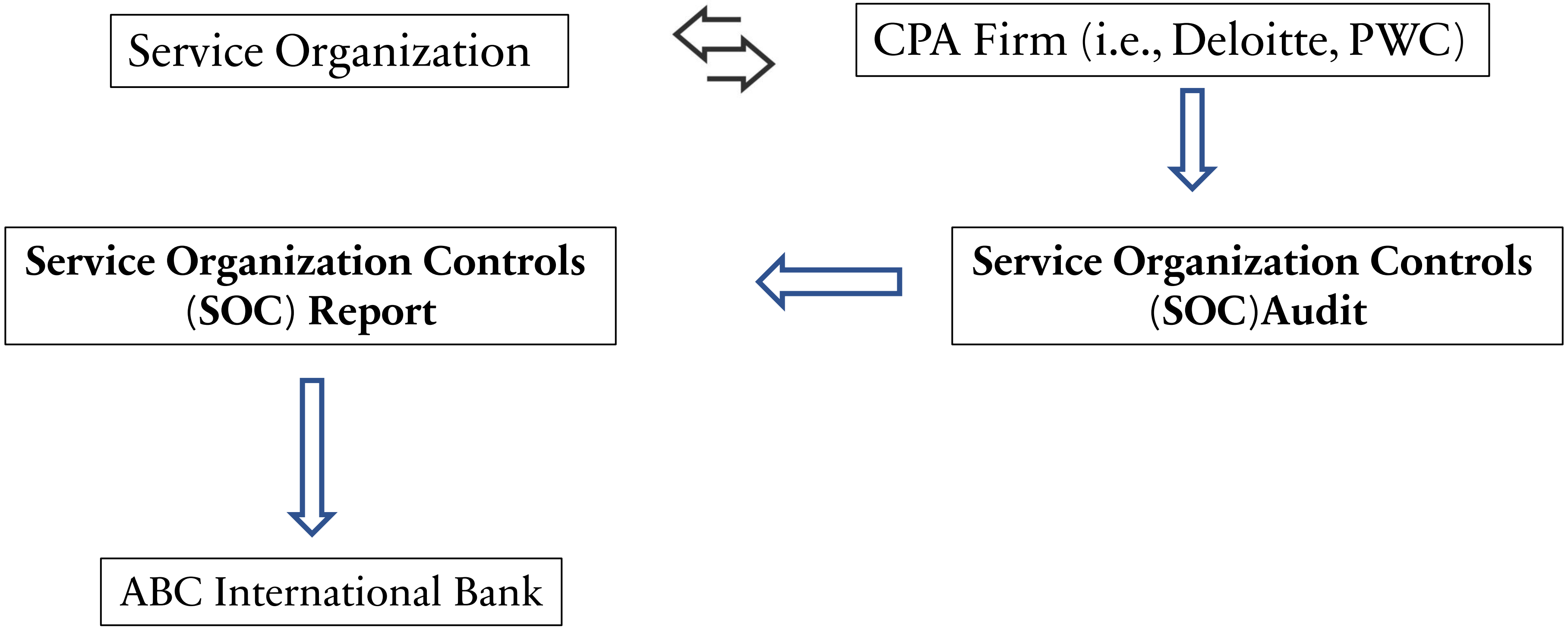
- **Test controls around:**
  - Encryption
  - Multiple Factor Authentication (MFA)
  - Access Controls

# SOC 2 Controls Testing

## Process Integrity Controls Testing

- **Test controls around:**
    - Policies and procedures to ensure system is operating effectively
    - Input and output controls
    - Process monitoring controls
    - Quality assurance controls

# SOC Controls Testing – Internal Audit Team



Service Organization

CPA Firm (i.e., Deloitte, PWC)

**Service Organization Controls (SOC)Audit**

**Service Organization Controls (SOC) Report**

ABC International Bank

# SOC Report

### Section 1: Independent Auditor's Report

- Audit Scope
  - Period
- Passed or Failed

### Section 2: Management Assertion

- Facts & Assertions by Management
- Product & Services Offered
- IT Systems & Controls

### Section 3: Description of Systems

- Detailed information on Systems & Infrastructures
- Risk Assessment
- Control Environment & Objectives
- Complementary Controls

### Section 4: Testing

- Tests of Controls
- Test Results
- Control Environment & Objectives
- Complementary Controls

# SOC Report Testing

## Section 1: Independent Auditor’s Report

- Audit Scope
  - Period
- Passed or Failed

## Section 2: Management Assertion

- Facts & Assertions by Management
- Product & Services Offered
- IT Systems & Controls

## Section 3: Description of Systems

- Detailed information on Systems & Infrastructures
- Risk Assessment
- Control Environment & Objectives
- Complementary Controls

## Section 4: Testing

- Tests of Controls
- Test Results
- Control Environment & Objectives
- Complementary Controls

# SOC Report

**Complementary Controls**

- End user controls
- 3rd party company (sub-service) controls

- **Complementary User Entity Controls** (**CUEC**) **:** End User Controls
- **Complementary Controls at Subservice Organizations:** 3rd party company

# SOC Report

### Section 1: Independent Auditor's Report

- Audit Scope
  - Period
- Passed or Failed

### Section 2: Management Assertion

- Facts & Assertions by Management
- Product & Services Offered
- IT Systems & Controls

### Section 3: Description of Systems

- Detailed information on Systems & Infrastructures
- Risk Assessment
- Control Environment & Objectives
- Complementary Controls

### Section 4: Testing

- Tests of Controls
- Test Results

# SOC Report Testing

**Section 1: Independent Auditor's Report**

- Audit Scope
  - Period
- **Auditors Opinion**
  - Controls are presented fairly
  - Controls are designed appropriately
  - Controls are operating effectively

- **Auditors Opinion** / Passed or Failed
  - Unqualified Opinion: Achieves all requirement (Passed)
  - Qualified Opinion: Achieves most requirements (Passed)
  - Adverse Opinion: Material weakness (Failed)

# SOC Report Testing

## Section 1: Independent Auditor's Report

- Audit Scope
  - Period
- Passed or Failed / **Auditors Opinion**
  - Unqualified Opinion
  - Qualified Opinion
  - Adverse Opinion

## Section 3: Description of Systems

- Complementary User Entity Controls (CUEC)

## Section 2: Management Assertion

- Facts & Assertions by Management
- Product & Services Offered
- IT Systems & Controls

## Section 4: Testing

- Test Results
  - Deficiencies identified

# SOC Report Testing

**Section 3: Description of Systems**

- Complementary User Entity Controls (CUEC)
    - IT auditor identifies all Complementary User Entity Controls
    - Meets with system/application owner to test the CUECs

**Section 4: Testing**

- Test Results
    - Identify deficiencies in the SOC report
    - Assess impact of deficiencies
- **Auditors Report**
    - CUEC test results
    - Assessment of deficiencies
    - SOC Report auditor's opinion

# Certifications

# Industry Certifications

- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
    - ISACA