

World Union of Arab Bankers COSO Internal Control Workshop

February 2023

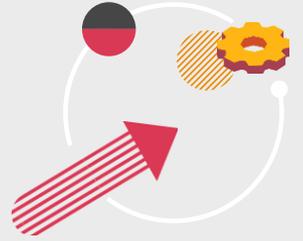
Day One



Reporting to the Board



Presented by: Mohamed Elmoataz, *Financial Services Advisor*



CBE's Internal Control Requirements

According to CBE instructions dated 4 August 2022 and provisions of Article (125) of the Law of the Central Bank and the Banking System promulgated by Law No. 194 of 2020, banks must abide by the following:

- Preparation of Annual Report on Internal Controls:
 - The report should be guided by the COSO Integrated Internal Control Framework of 2013. The report may be guided by other principles or guidelines provided that they are complementary to COSO.
 - The report must include the bank's assessment of the control environment, risks, control activities, information and communication systems, and periodic control processes as well as any deficiencies in internal control procedures and corrective actions.
- Submit the report to the Audit Committee/ Bank's Board of Directors for approval and follow-up on the implementation of corrective plans.
- Submit approved report to the bank's auditors for for them to send a final report on internal controls to CBE, together with their audit reports on the financial statements, in accordance with Article 125 of the law.

Control Environment

Risk Assessment

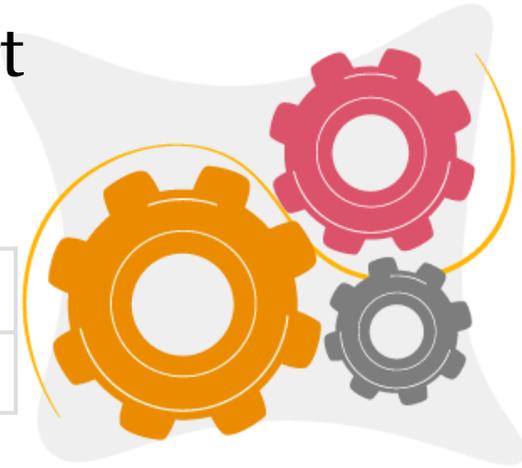
Control Activities

Information and
Communication

Monitoring Activities

Sample Table of Contents for an IC Report

1. Introduction	
2. Roles & Responsibilities	4. Management Conclusion
3. Management Assessment	5. Board of Directors' Approval
3.1 Internal Control Framework	
3.2 Assessment Approach and Scope	
3.3 Walkthrough and Design Testing	
3.4 Sampling Approach	
3.5 Testing Approach	
3.6 Internal Control Deficiencies and Remediation Plan	



Opportunities and Challenges - ICFR implementation



Opportunities

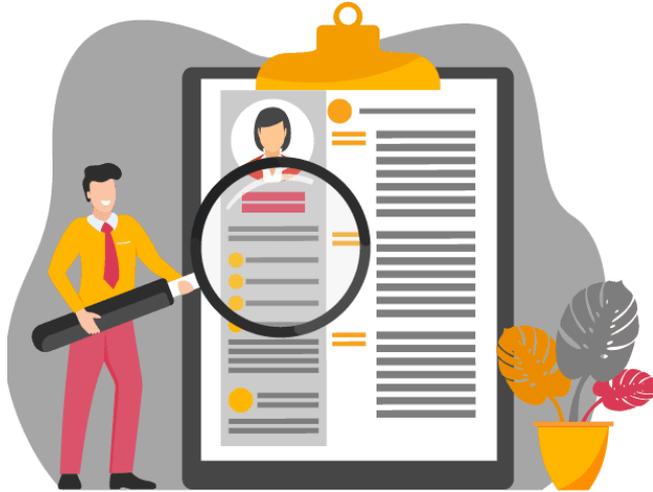
- Improve **governance** and transparency
- Increasing accountability and improving **control ownership**
- Optimize process flows by eliminating **duplicate controls**
- Assess **digitalization** of controls where possible
- Ensure systematic **compliance** with laws and regulations
- Objective selection of **accounting policies**
- Develop infrastructure for effective **ESG reporting**



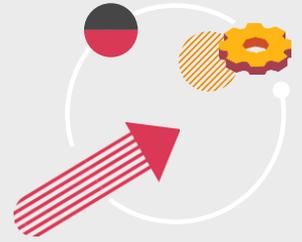
Challenges

- Consider ICFR as a **tick box** exercise
- Failure to identify **critical control** gaps
- Less focus on **governance and culture** related controls
- **Cost of compliance** higher than the underlying benefit
- Engaging individuals without proper understanding or **expertise** in IFRS and COSO
- Unrepresentative **sample** or incomprehensive **population** analysis
- Less reliance by **external auditor** on management ICFR practices

External Auditors' Expectations



Presented by: Tamer Tawab, *Core Assurance Partner*



Reporting Requirements

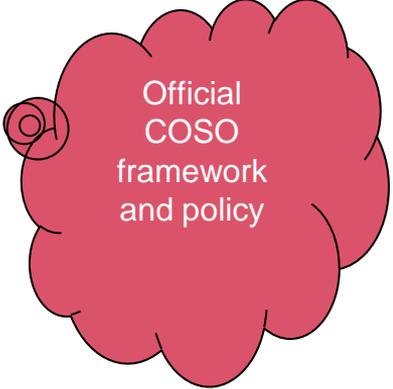
Provide the bank's auditors with the report after its approval by the Board of Directors for study and discussion, in preparation for the auditors to send a final report to the Central Bank of Egypt.

The report should include an assessment of the adequacy of the internal control system in the bank at all levels in accordance with Article 125 of the law.

The external auditor is required to conduct an independent assessment on the Bank's internal control system over financial reporting, based on the criteria established in Internal Control Integrated Framework (2013) issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and subsequently issue an assessment report on the adequacy of the Internal Control System at all bank levels, in accordance with the "CBE Article No. 125.



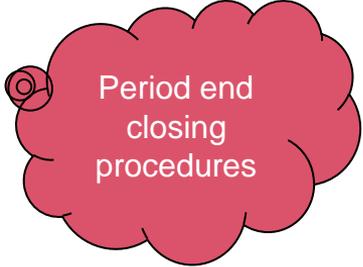
Points for consideration



Official
COSO
framework
and policy



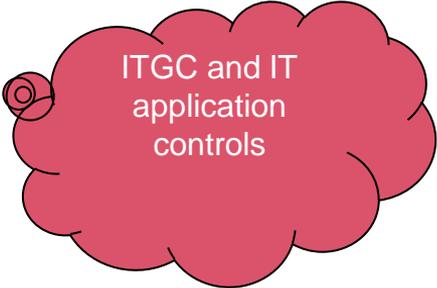
Severity of the
control
deficiency and
impact of the
overall
assessment



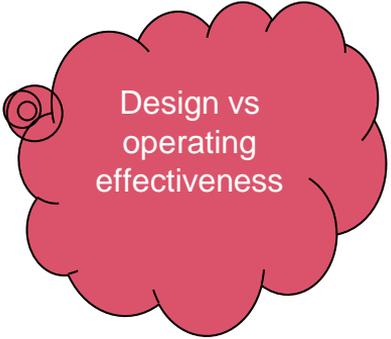
Period end
closing
procedures



RCM reflecting
risk related to
financial
reporting



ITGC and IT
application
controls



Design vs
operating
effectiveness

COSO - Reflecting on What Banks Have Done So Far



Table Group Discussion

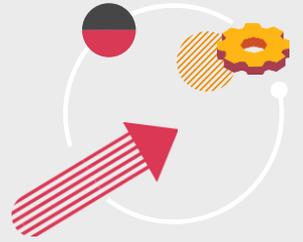


Table Group Discussion

- **What worked well and what didn't?**

Points to consider:

- Expertise to implement the COSO framework/ use of external consultants
- Tone-at-the-top - support from board members and senior management to strengthen the current internal control environment
- Quick wins!

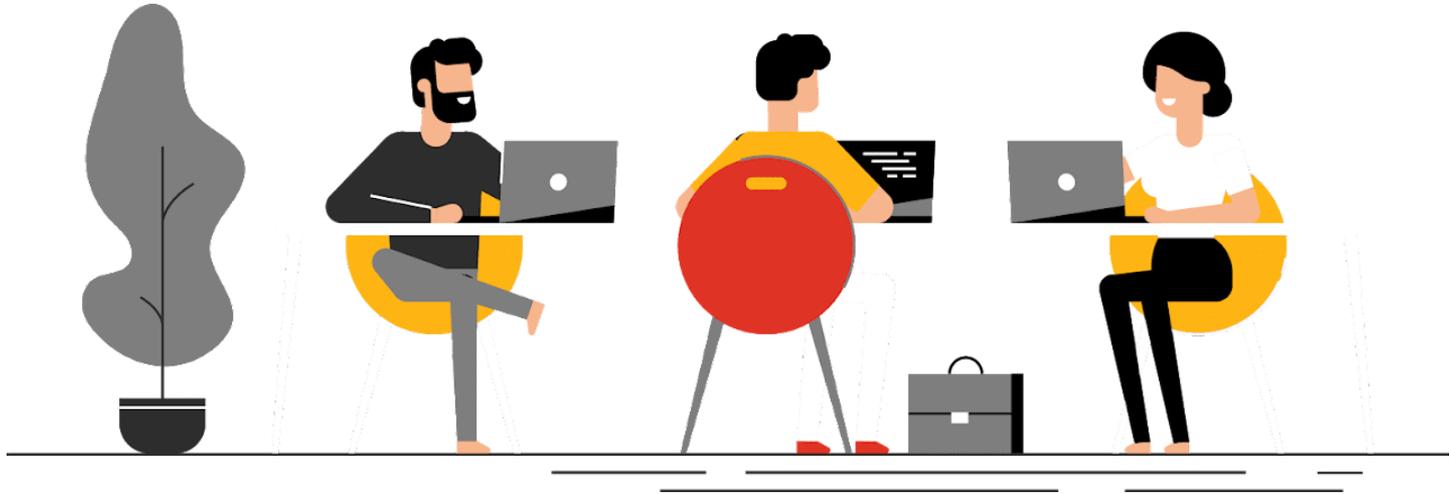


Table Group Discussion

- **What have banks done to comply with CBE instructions?**

Points to consider:

- The critical goals and objectives of internal control reporting and the risks associated with that
- Addressing all COSO components as functioning and working in integrated manner
- Identification of processes in-scope/out-of-scope

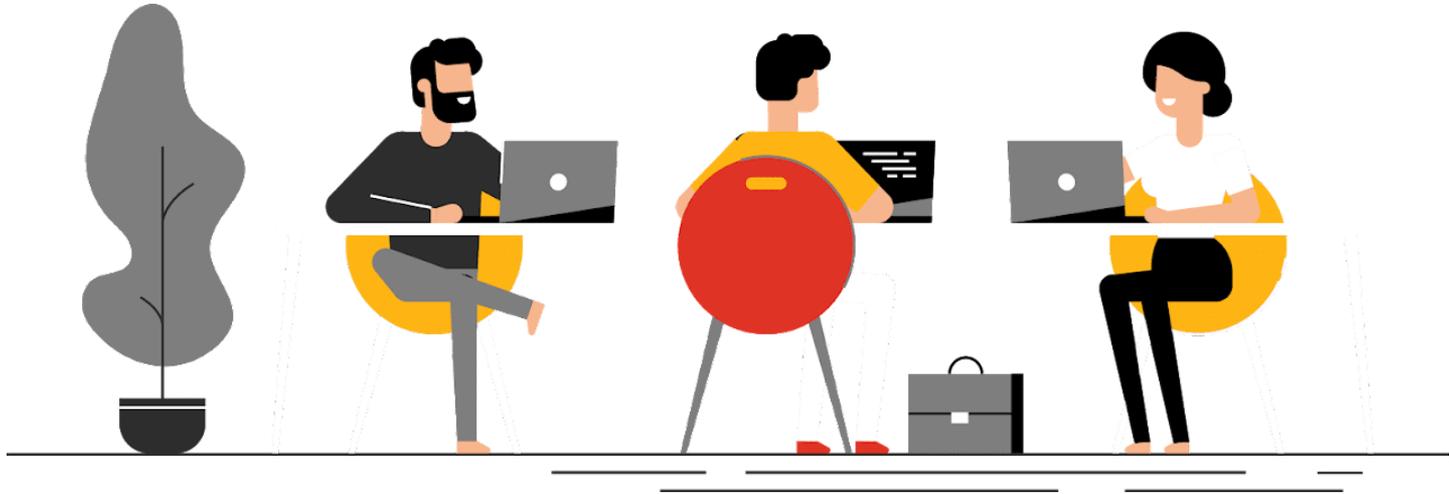


Table Group Discussion

- What are the key management expectations of their auditors / consultants?

Points to consider:

- Role of consultants vs management
- Role of auditors vs consultants



World Union of Arab Bankers COSO Internal Control Workshop

February 2023

Day Two



Automation



Presented by: Hassan Ahmed, *PwC Manager*



TeamMate

TeamMate was originally developed in 1994 by Price Waterhouse and from 1998 continued to be developed and marketed by PricewaterhouseCoopers and from 2007 TeamMate was acquired by Wolters Kluwer. Over the last 25+ years TeamMate has grown to be the market leading audit automation system with more auditors using TeamMate than all other competitors combined.

PricewaterhouseCoopers (PwC) and Wolters Kluwer (WK) partner together to provide TeamMate Audit Management software related services in the Middle East. PwC is the authorized provider of all TeamMate licensing, implementation and training services the region using within the region to both new and existing clients. This partnership has resulted in > 200 clients across TeamMate.

PwC in the Middle East

PwC has operated in the Middle East region for more than 40 years.

Collectively, our Middle East network employs in the region of over 10,000 people including over 374 partners and 585 directors working from 24 offices (in 23 locations) across 12 countries: Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Oman, the Palestinian territories, Qatar, Saudi Arabia and the United Arab Emirates and 40% of our Middle East workforce is female.

Wolters Kluwer

Wolters Kluwer (WK) is a multinational business headquartered in the Netherlands with a listing on Euronext which specializes in providing information for professionals in the Healthcare, Tax & Accounting, Corporate and Financial Service industries.

Wolters Kluwer is committed to helping professionals improve the way they do business and solve complex problems with confidence in an ever-changing world.

Wolters Kluwer has total revenues in excess of €4.6 billion (2021) and over 19,500 employees globally.

TeamMate

TeamMate is a leading provider of audit management solutions, delivered with premium professional services, to auditors around the globe.

Our expert audit management solutions combine deep domain knowledge with technology to deliver both content and workflow automation to drive improved outcomes and productivity for our customers.

We take a customer-focused approach to product development, aim to solve customers' problems and add value to their organization with our range of digital solutions and services, which we continuously evolve to meet the changing needs of the profession.

Our expert solutions and professional services deliver on six core capabilities to solve your current challenges, as well as address your future needs.



Purpose built for audit



Stakeholder engagement



Open ecosystem



Data-driven insights

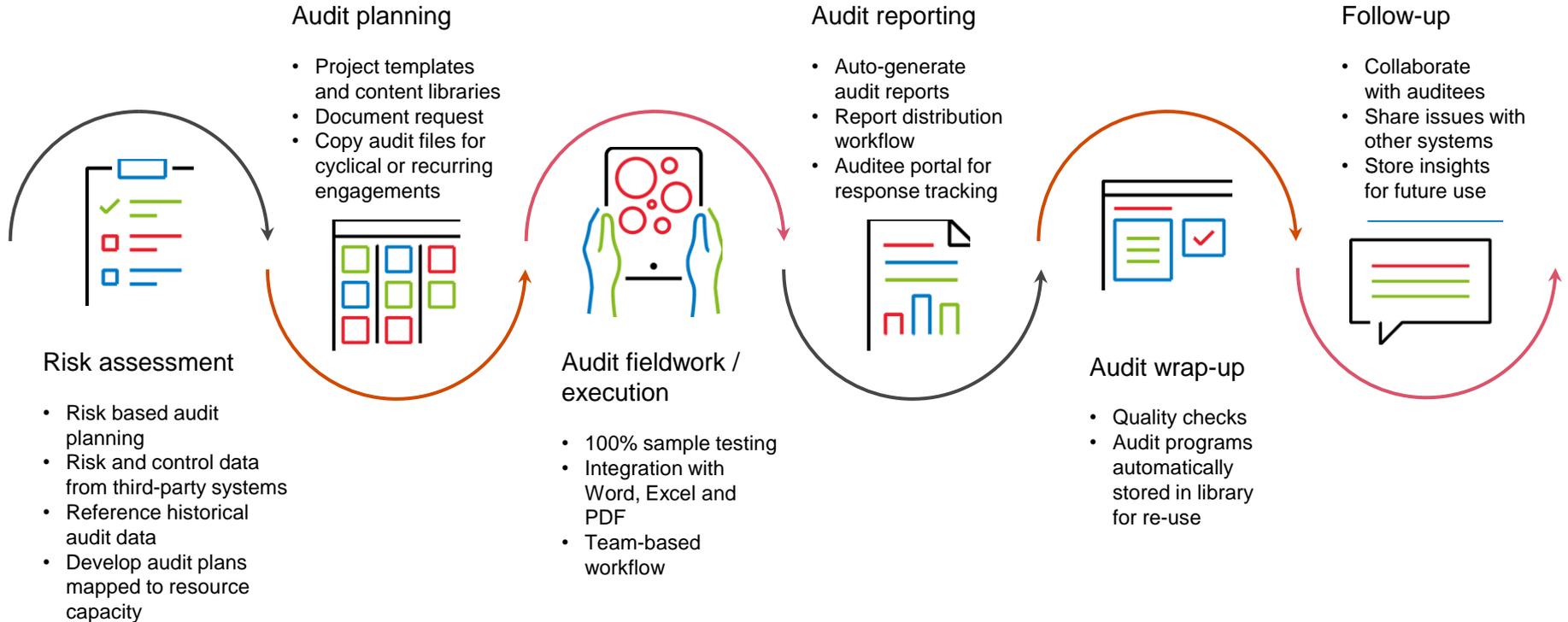


Infrastructure compatibility

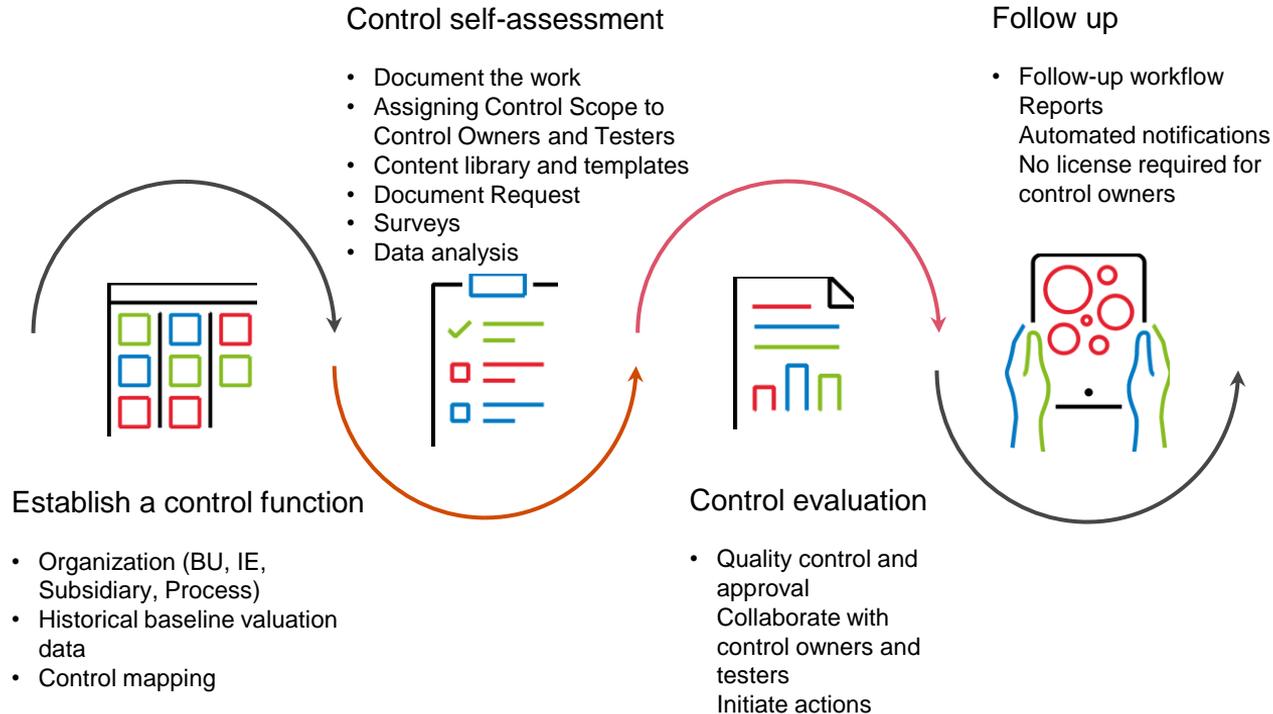


Risk-focused planning
& execution

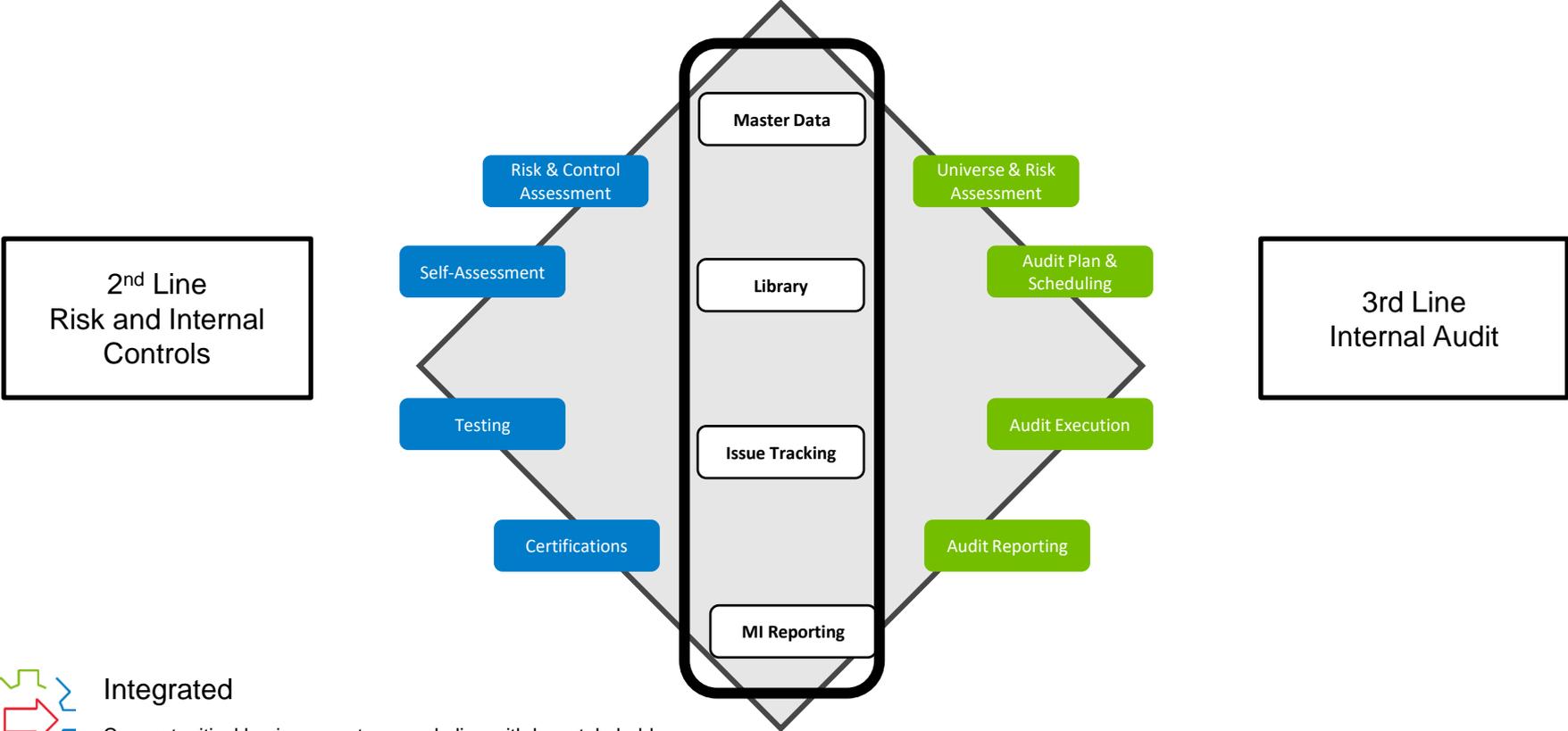
Our Solution: TeamMate + Audit



Our Solution: TeamMate + Control



Combined Assurance



Integrated

Connect critical business systems and align with key stakeholders

Our Solution: TeamMate + Control

What makes TeamMate+ Controls different?

TeamMate + Controls is a member of the TeamMate suite of applications, focused on the management and testing of any other set of controls an organization may choose to follow or be required to implement.

TeamMate + Controls provides built-in workflows around the assessment, process owner review, testing, documentation, retesting, and certification processes. It gives you the ability to view and interact with controls through a truly unique User-defined structure based on Dimensions and Perspectives of data. This innovative design leads to much greater efficiency when completing controls work as well as better insight into the potential impact the given control environment and the failure of any given control could have on an organization.

What is TeamMate + Controls?

Flexible relationship between entities, processes, financial statement accounts, and other reporting structures

- You are not forced to use a fixed, rigid hierarchy of entity/account, process, risk, control. As such, the TeamMate+ Controls hierarchy can be set up to use for other types of control or compliance testing.
- Our approach allows you to create a relationship between dimensions such as entities and processes to each instance of a risk or control.

Our Solution: TeamMate+ Control

Self-Assessment Change Management

A powerful feature of TeamMate + Controls is the ability to allow business contacts to manage their own narratives, self-identify issues, and edit their controls during the self assessment process. A track changes option gives you the option to view and approve all changes before committing the updates to the live assessment.

Reporting

A robust reporting database contains a library of available reports including:

- Control Usage
- Control Testing Results
- Risk Control Matrix
- Comprehensive Issue Grid with Controls Issues

Ease of Use

- Simple, consistent and intuitive user interface
- Reduce onboarding costs
- Improve auditor satisfaction

The screenshot displays the TeamMate+ user interface. On the left is a navigation menu with options: Home, Audit Clients, Audit, Notifications, Audit Report, and Reports. Below the menu is a laurel wreath award for 'TeamMate+ Audit WINNER Best User Experience in Audit Management GRC 20/20'. The main content area features a table with columns for Area, State, Due Date, and Review Due Date. Below the table are two charts: 'My Test Status' and 'My Test Status'.

Area	State	Due Date	Review Due Date
Financial Audit Demo (WK 010)	Not Started		
Financial Audit Demo (WK 010)	In Progress		
Financial Audit Demo (WK 010)	Prepared	3/31/2017	4/7/2017

My Test Status (Total: 4)

Milestone	Count
1	1
2	3
3	0

My Test Status (Total: 56)

State	Count
Not Started	47
In Progress	3
Prepared	6



Digital

Harness the latest technologies and methodologies

No Code Solution

- Reduce risk during implementation
- Settings stored in the database so you can always upgrade seamlessly
- Make changes to configuration including reports without vendor assistance reducing lifetime cost of ownership



Digital

Harness the latest technologies and methodologies

Open Ecosystem

Assurance Systems

Business Intelligence

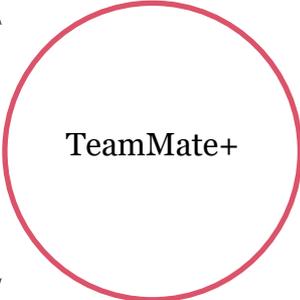


Risks and controls
audit findings

Audit, schedule
and resource



Reporting data



TeamMate+



KPI and KRI
data

User accounts



SSO



Integrated
Connect critical business systems
and align with key stakeholders

ERP Systems

User Management

We Work Wherever You Are

350 full time employees



TeamMate is Proud to be Recognized in Industry Awards

Global Leader in Cloud Computing

Stratus Awards

2020 | TeamMate

Internal Audit Management Solutions

Chartis Risktech Quadrant

2021 | TeamMate | Category Leader

Honorable Mention Top New Product in Audit

Accounting Today

TeamMate+ Audit | Gold Winner

Top 10 in Audit Software

Software World

2020 | TeamMate

Internal Audit Management Solutions

Chartis Risktech Quadrant

TeamMate+ Audit | Category Leader

Best User Experience in Audit Management

GRC 20/20

TeamMate+ Audit | Gold Winner

Best Product in Auditing Innovations

Golden Bridge Awards

2021 | TeamMate Agile Audit

Winner in Audit Technology

K2 Quality Awards

TeamMate Analytics

Best Product in Auditing Innovations

Golden Bridge Awards

2020 | TeamMate | Gold Winner

New Product of the Year

American Business Awards

2021 | TeamMate Agile Audit

New Product of the Year in Governance, Risk & Compliance Solutions

American Business Awards

TeamMate Analytics | Bronze Stevie

Product of the Year

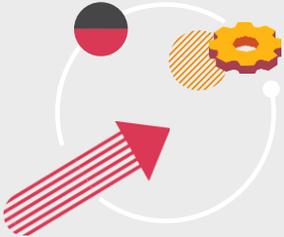
Big Awards for Business

2020 | TeamMate

The Documentation Challenge



Presented by: Salma Elshabrawy, *Risk Senior Manager*



COSO Framework - Documentation

The COSO Framework requires management to maintain adequate documentation for the following reasons:

- To provide clarity around roles and responsibilities, which promotes consistency in adhering to the entity's practices, policies and procedures;
- To assist in capturing the design of internal control and setting expectations of performance and conduct;
- To assist in training new personnel and to offer a reference for other employees;
- To provide a means to retain organization knowledge; and
- To provide evidence of the conduct of internal control, enable proper monitoring, and support reporting.



COSO Framework - Documentation Requirements

The COSO Framework states that management assumes a higher degree of responsibility for maintaining the requisite supporting documentation.

Management should pay particular attention to documenting the following:



Purpose
The purpose of this practice aid is to provide a template to identify key risks, perform a risk coverage assessment, and compile a comprehensive listing of controls and risks they are designed to address.

Instructions
Complete each column for identified Business Process and Sub-processes. Refer to Guidance and Example provided for additional instructions.

Location	Process	Sub-process	Risk number	Risk Statement	Financial Statement Assertions							Control number	Key control activity
					Accuracy	Completeness	Cutoff	Existence, Occurrence & Rights	Measurement & Disclosure	Valuation			
<i>Guidance</i> Define the primary location where the control operates	Document the process in which the control operates	Document the sub-process in which the control operates	Enter the corresponding risk number(s) from the top Key Risks Listing	Enter the description of the corresponding risk(s) from the top Key Risks Listing	Select the Financial Assertions relevant to the control							Enter the control number	Document the control activity / control description
<i>Example</i> Corporate Accounting	BUS	Business Combinations accounting			-	-	-	-	-	X	-	[CONTROL NUMBER]	[CONTROL DESCRIPTION]
					-	-	-	-	-	-	-		
					-	-	-	-	-	-	-		
					-	-	-	-	-	-	-		
					-	-	-	-	-	-	-		

Control Description
Kindly note that below is an example of a control description.

Design Assessment

Who? _____

What? _____

Where? _____

When? _____

Why? _____

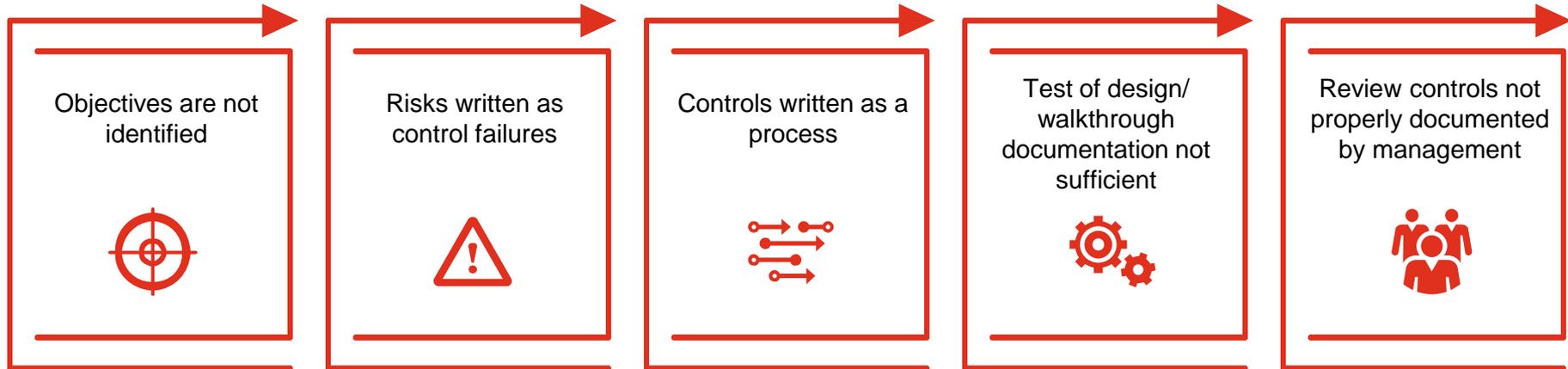
How? (Evidence) _____

1. Introduction
 - 1.1 Assessment approach and scope
2. Executive Summary
 - 2.1 Internal Control Framework Adopted
 - 2.2 Activities Performed
3. Roles & Responsibilities
 - 3.1 Board of Directors
 - 3.2 Senior Management
 - 3.3 External Auditor
4. Internal Control Deficiencies and Remediation Plan

Documentation Challenges

Documentation should be sufficient to demonstrate effectiveness for all components and principles, including those outside of control activities.

Examples of documentation challenges that have been encountered include:



Activity

8 Quiz Questions:

Q1: Is this an objective?

- *'Ensure that bank reconciliation is performed on timely basis.'*

No

Q2: Is this an objective?

- *'Ensure that loan applications are properly reviewed and approved'*

No

Q3: Is this an objective?

- *'Ensure that fixed assets are accurately, completely and timely recorded in the accounting books'*

Yes

Activity

8 Quiz Questions: Objective - *'Ensure that fixed assets are accurately, completely and timely recorded in the accounting books'*

Q4: Is this a relevant risk?

- *'Fixed assets physical count is not performed'*

No

Q5: Is this a relevant risk?

- *'Fixed assets are not accurately recorded.'*

No

Q6: Is this a relevant risk?

- *'Fixed assets may be lost or stolen without being detected, resulting in an overstatement in FA.'*

Yes

Activity

8 Quiz Questions: Objective - *'Ensure that fixed assets are accurately, completely and timely recorded in the accounting books'*

Q7: Is this a relevant control?

- *'Fixed assets are insured by a third party'*

No

Q8: Is this a relevant control?

- *'Fixed assets are counted on annual basis by an independent Committee who sign the physical count report.'*

No

Q9: Is this a relevant control?

'Annual Fixed assets physical count report is reconciled on monthly basis with the risk register balances. The Reconciliation is reviewed and approved by the Financial Control. Any unreconciled items are investigated and settled on timely basis.'

Yes

Processes vs controls: Polling activity

- Is a “Policy” a process or control?

Process

- Is “Reperformance / recalculation by a second person” a process or control?

Control

- Is “Reconciliation” a process or control?

Process



RCM Example - Illustrative Purposes Only

Key controls are typically documented in a risk and control matrix.

Key controls are typically documented in a risk and control matrix:

Location	FSLI	Process	Sub-process	objective	Risk number	Risk Statement	Financial Statement Assertions						Control number	Control title	Key control activities	
							Accuracy	Completeness	Cutoff	Existence & Occurrence	Presentation and disclosure	Right & Obligation				Valuation
Financial Shared Service	Accounts Payable	PTP	Vendor Maintenance	Ensure payments are accurately paid towards valid/authorized vendors	R.PTP.1	Unauthorized changes are made to the master file data	X						X	PTP-1	Vendor Master File Change Requests	As needed, the FSS Specialist verifies new vendor requests are properly approved prior to entry into the system. All requests for new vendors require a secondary approval from the requestor's manager. Evidence maintained consists of the approved vendor request.

COSO 2013 Mapping

COSO 2013 Mapping		Control Attributes							Information processing				Key Control		Control Risk Rating		
COSO Component	COSO Principle	Control owner	Control Frequency	Control category	Control Classification	Preventative or detective	Fraud consideration	Accounting system/Source that generated the data or report used in the control	Critical reports and/or spreadsheets	Effective date of control	Completeness	Accuracy	Validity	Restricted Access	Key control	Non-key rationale	Risk
3.Control Activities	10.Selects and Develops Control Activities	Relevant Manager	As Needed	Transactional Control	IT Dependent Manual	Preventative	Yes	[Client EPR System]	N/A	1/1/2016			X	X	Yes	N/A	Medium

Walkthrough, not Talkthrough

1) The client should explain how transactions flow through the process **from beginning to end.**

2) Walkthroughs should be performed for **each relevant business process** that is included in the scope of the Controls Report.

3) Should contain details of who, what, where, when and how.

4) Identify any exceptions to the standard process.



Walkthrough, not Talkthrough

In practice, we often do **‘talkthrough’** rather than **‘walkthrough’** – this is not adequate and can result in, but not limited to, the following issues:

- The control mentioned does not exist; and
- The control does not operate as described by the control owner (e.g. frequency, evidence, manual/automated).

We need to **trace a transaction through**, and ask the client to **‘show me’** so that we see evidence of the process happening as described.

Process details		
Process name	<i>(E.g. Client onboarding, Trade Execution, client reporting etc)</i>	
Scope of products covered		
Process input	<i>(Include details or insert Aura link to ESG where the preceding process is documented) / (not applicable)</i>	
Process output	<i>(Include details or insert client link to ESG where the follow-on process is documented) / (not applicable)</i>	
Client provided process documentation / material		
Evidence obtained		
Systems and Applications applicable to process	Control Ref	Summary of Evidence Obtained / examined
Are Systems / Applications applicable to process in scope for IT testing? <i>Provide rationale if not applicable</i>		Attachments - examples reviewed
Key reports or EUCs applicable	<p><input checked="" type="checkbox"/> Confirmed details above are reflected in the DSM (controls matrix), the applicable Aura EGAs and the narrative 'Description' within the controls report</p> <p><i>Engagement teams also review the client's narrative process descriptions in the draft controls report to ensure consistent with the above walkthrough details.</i></p>	

Checklist for a well documented walkthrough:

- Perform walkthrough for each relevant business process.
- The client should explain how transactions flow through the process from beginning to end.
- Cover all types of transaction.
- Where possible, perform in ‘real time’.
- Include screenshots of what you have seen to help understanding
- Identify key reports which are critical to the effective operation of that control
- Identify the IT applications supporting key controls.
- If observing a “test environment”, test that this matches the “live environment”.
- Involve sufficiently senior engagement team members.
- Be clearly documented on the engagement file.
- Use the Walkthrough template available [here](#)

Test of Design Template

Test of design are typically documented within the risk and control matrix in a separate tab.

Control #	Cx
Control Description	<i>Description of the control</i>
Design Assessment	Response
Who?	<i>Who is the document owner? Who will be held accountable for this document?</i>
What?	<i>What is the document name and details?</i>
Where?	<i>Where is the department located? Head office, branch etc..</i>
When?	<i>What is the frequency of the document or report?</i>
Why?	<i>What is the purpose of the document or report?</i>
How? (Evidence)	<p><i>"How did you do your walkthrough? What was your walkthrough testing procedures performed on the samples taken? (For example ensured that xxx signed the document as the approval. ensured that the preparer signed. ensured that all unreconciling items were identified..etc.)</i></p> <p><i>Is it performed manually or automatically and name of the system?</i></p> <p><i>Please explain the step by step performed to make sure the control is applicable on ground and the adequacy of the controll. For example if the department walked you through the whole process on the system until we got the final report or performed actual on-ground reconciliation between two documents X and Y and the results of the reconciliation you performed."</i></p>
Walkthrough Document Ref. #	<i>Reference & Name of Documents</i>
Exceptions Noted?	<i>Yes/No</i>
Conclusion	<i>Control is deemed to be effectively/not effectively designed</i>

Test of Design Example 1

Control #	C1
Control Description	<i>Financial Statements are reviewed and approved by the Financial Controller and CFO before being submitted to the Audit Committee.</i>
Design Assessment	Response
How? (Evidence)	<i>Received the financial statements and reviewed the evidence of review of the CEO and Executive Committee before being submitted to the audit committee.</i>
Walkthrough Document Ref. #	<i>Financial Statements</i>
Exceptions Noted?	<i>No</i>
Conclusion	<i>Control is deemed to be effectively designed.</i>

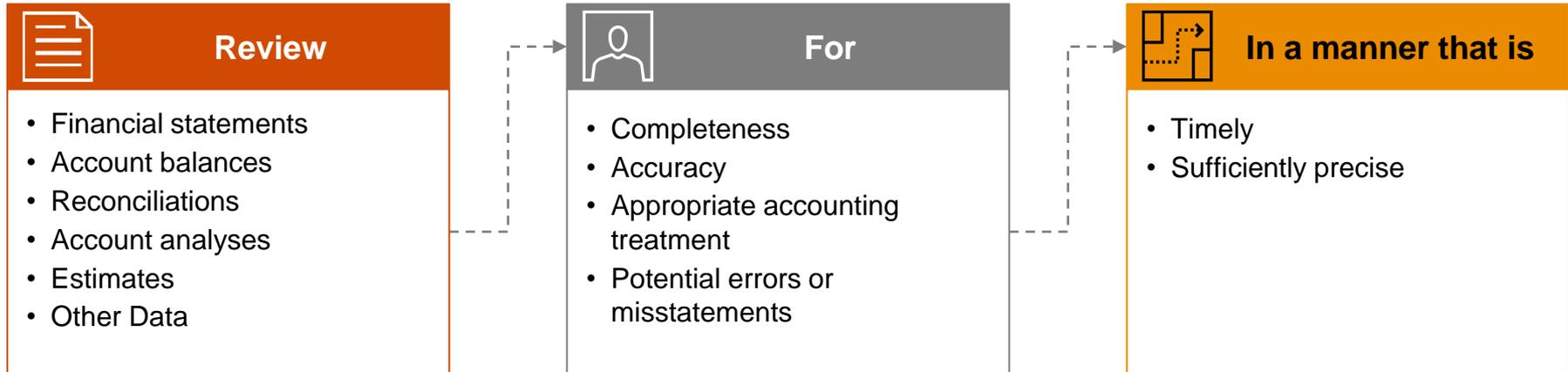
Test of Design Example 2

Control #	C4
Control Description	<i>Fixed asset GL & FA register reconciliation is performed on monthly basis by the GL senior accounted, reviewed and approved by the Financial controller. Any unreconciled balances are investigated, justified, and aged.</i>
Design Assessment	Response
Who?	<i>The finance team</i>
How? (Evidence)	<i>The process owner has showed us the GL FA ending balance at the end of the month, and the fixed asset register, and there were no variance.</i>
Walkthrough Document Ref. #	<i>Print out from the system GL, FA Register</i>
Exceptions Noted?	<i>No</i>
Conclusion	<i>Control is deemed to be effectively designed.</i>

What exactly is a "review" control?

A management review control is a control in which a designated individual reviews documentation prepared by another individual and applies judgment to determine the acceptability of the results and any required actions to be taken as a result of the performance of the review.

A well-designed management review control is designed to:



Review Control Documentation



Review controls – example – fluctuation analysis

Control: On a quarterly basis the Accounting Manager performs a quarterly Balance Sheet and P&L variance analysis that identifies and explains all variances above the threshold of \$100k and 10%. This analysis is reviewed and approved by the Head of Finance prior to the submission of the financials to Corporate.



Review steps

Validates the data used in the variance analysis agrees to BPC (General Ledger) for accuracy and tying out the revenue and expense totals to the BPC (through review of the BPC screenshots maintained in the support package)

Validates clerical and mathematical accuracy of schedule (by recalculating, footing, cross-footing key data)

Validates or investigates explanations for variances above the defined threshold of \$100k and 10% by reviewing supporting documents or discussing with the preparer or relevant individuals

Sign-off and date variance analysis schedule, attesting to timely completion of review steps



Evidence of review step

Checkmarks/comments next to the data tied to supporting screenshot or regenerated report

Checkmarks/comments next to data recalculated, footed, or cross-footed

Handwritten comments on schedule evidencing validation/investigation steps performed and resolution, or email trail showing investigation steps performed and resolution

Physical sign-off and date on schedule and attestation



Support required

Variance analysis excel schedule and

- Screenshot of parameters used to generate the report to verify it included the correct period and ad hoc analysis selections
- Screenshot of the revenue and expense amounts from BPC (support provided by preparer)

Variance analysis excel schedule and supporting calculations

Variance analysis excel schedule and support evidencing resolution of investigation (varies based on nature of items- examples include handwritten notes on schedule, email follow-up)

Variance analysis excel schedule and attestation with physical sign-off and date

Management review control challenges

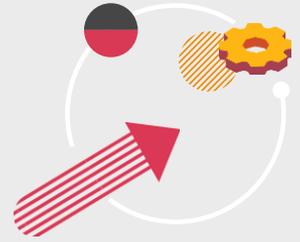
- Limited transparency and evidence provided to support the control activities as they are executed and waiting until the process is complete and all control activities have operated
- Understanding and evidencing the design of the control including exactly what the control operator does in performing each control activity
- Identifying information used in the control and understanding and evidencing management's controls over the completeness and accuracy of the information (IPE)
- Understanding and evidencing the level of precision of the control
- Evidencing that the control operated as designed including the steps involved in developing expectations and identifying, investigating and resolving differences from expectations
- Evaluating potential contrary evidence over the effectiveness of the control, including the identification of errors
- Evaluating control deficiencies based on potential misstatements that may not be detected in light of the control deficiency (the "could factor") rather than actual errors



COSO Scoping



Presented by: Mohamed Elmoataz, Financial Services Advisor



Internal Controls Reporting Lifecycle

Program management and auditor collaboration

Risk assessment
and scoping

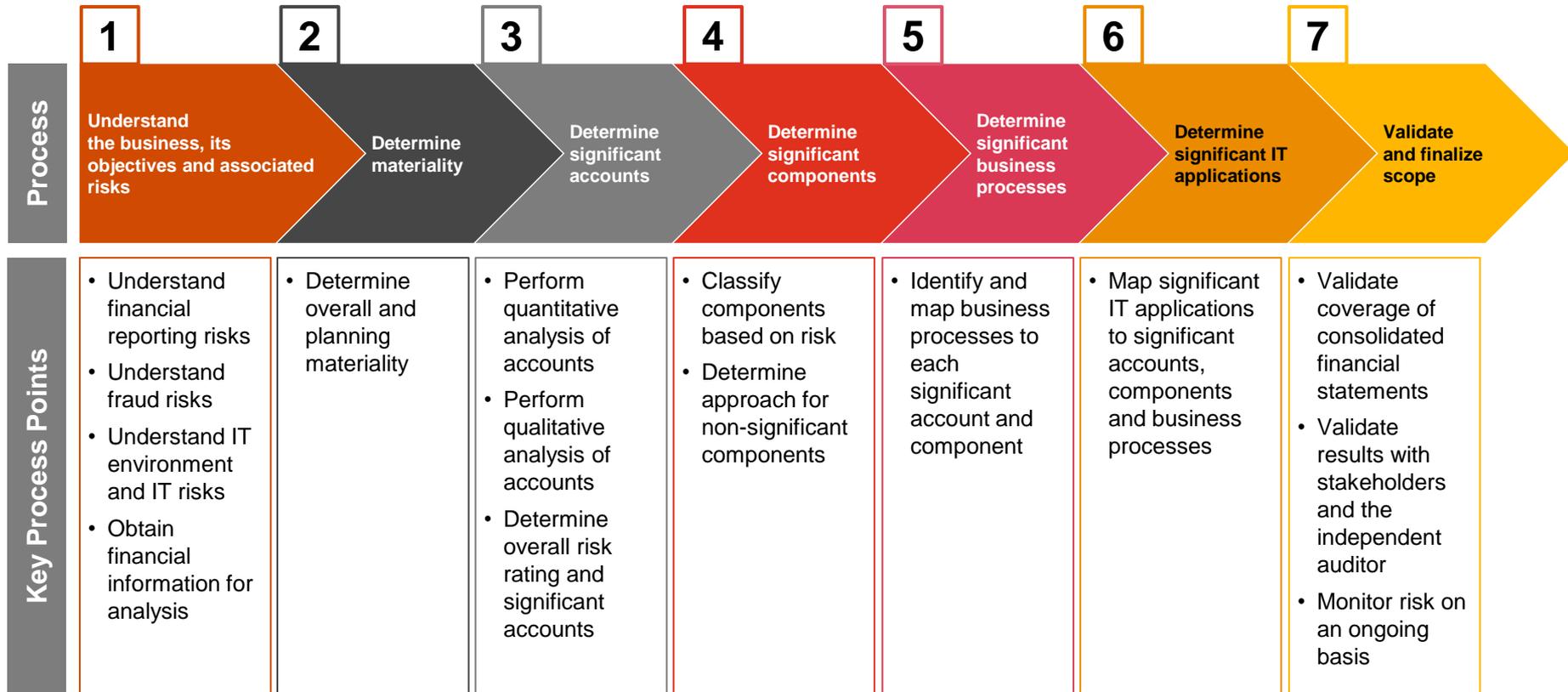
Control documentation
and design

Control testing

Remediation and
reporting

Internal control over financial reporting

Risk Assessment & Scoping



Step 2

Determine materiality

“Misstatements, including omissions, are considered to be material if they, individually or in the aggregate, could reasonably be expected to influence the economic decisions of users made on the basis of the financial statements;”



Overall Materiality

Materiality level for the financial statements as a whole.



Performance Materiality

Materiality in relation to financial statement assertions for classes of transactions, account balances and disclosures.

- Lower than the materiality level for the financial statements as a whole;
- Allows us to reduce to an appropriately low level the probability that the total of uncorrected and undetected misstatements would result in a material misstatement of the financial statements;
- Affected by the expected level of misstatement, and the nature, cause, and amount of misstatements from prior periods.

Step 3

Determine significant accounts

COVID-19 considerations, such as:

Changes to projected revenue

Changes in liquidity

Goodwill and intangible impairment



Management's quantitative and qualitative analyses can be used to establish an overall risk rating for each account and sub-account. The overall risk ranking can be used as a basis for determining significant accounts at the consolidated level.



Quantitative Analysis of Accounts

- Primarily a materiality test, which helps Management make an initial determination of the significant accounts
- Management can perform a quantitative analysis by applying the planning materiality threshold to the accounts that make up each FSLI as filed.

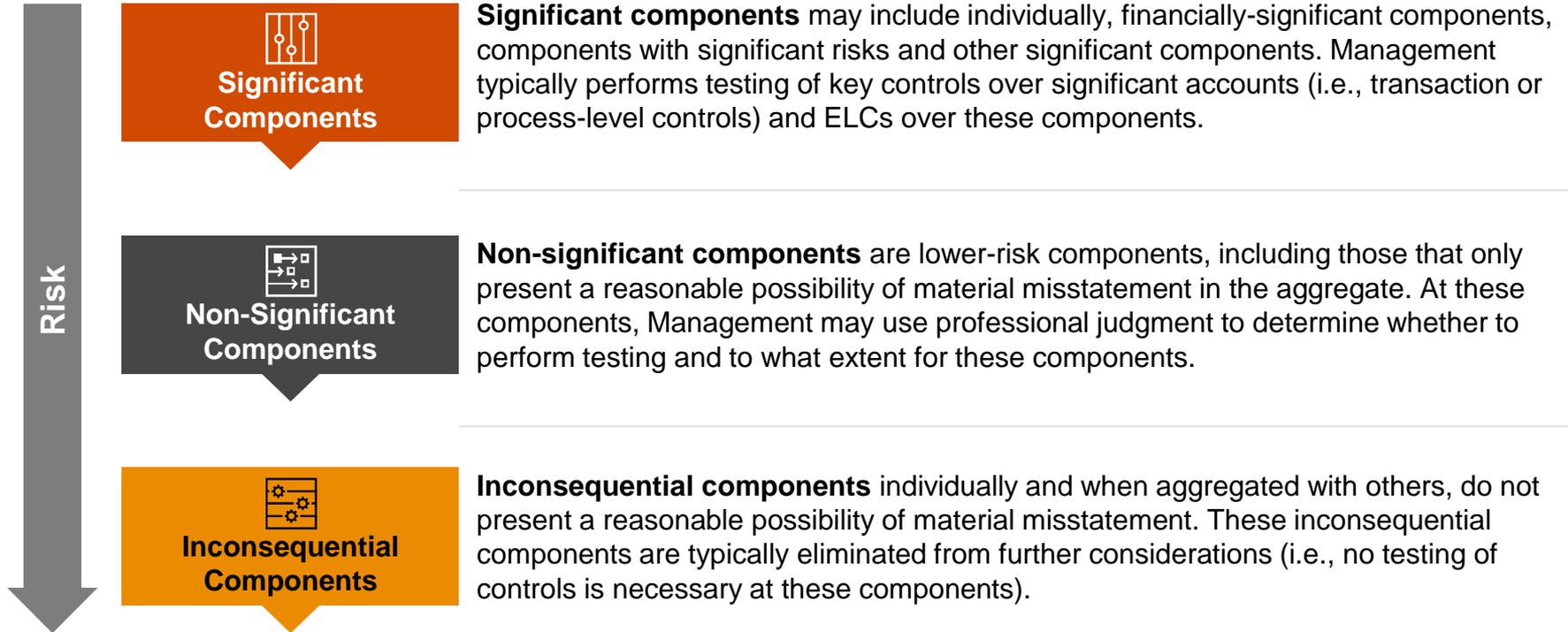


Qualitative Analysis of Accounts

- Misstatement risks may be higher when underlying transactions, accounts and other information:
 - Involve judgment in determining the recorded amounts.
 - Are susceptible to misstatement due to error or fraud.
 - Include complex accounting requirements.
 - Experience change in the nature or volume.
 - Are sensitive to changes in environmental factors, such as technological and/or economic developments.

Step 4

Determine significant components



Step 5 & 6

Determine significant business processes and IT applications



What is a business process?

A business process is any sequence of activities (transactions) that takes place to get work accomplished and achieve the business' objectives.



What is a significant IT application?

A significant IT application is an IT application considered in scope for purposes of ICFR based on the identification of relevant IT dependencies within a significant business process.



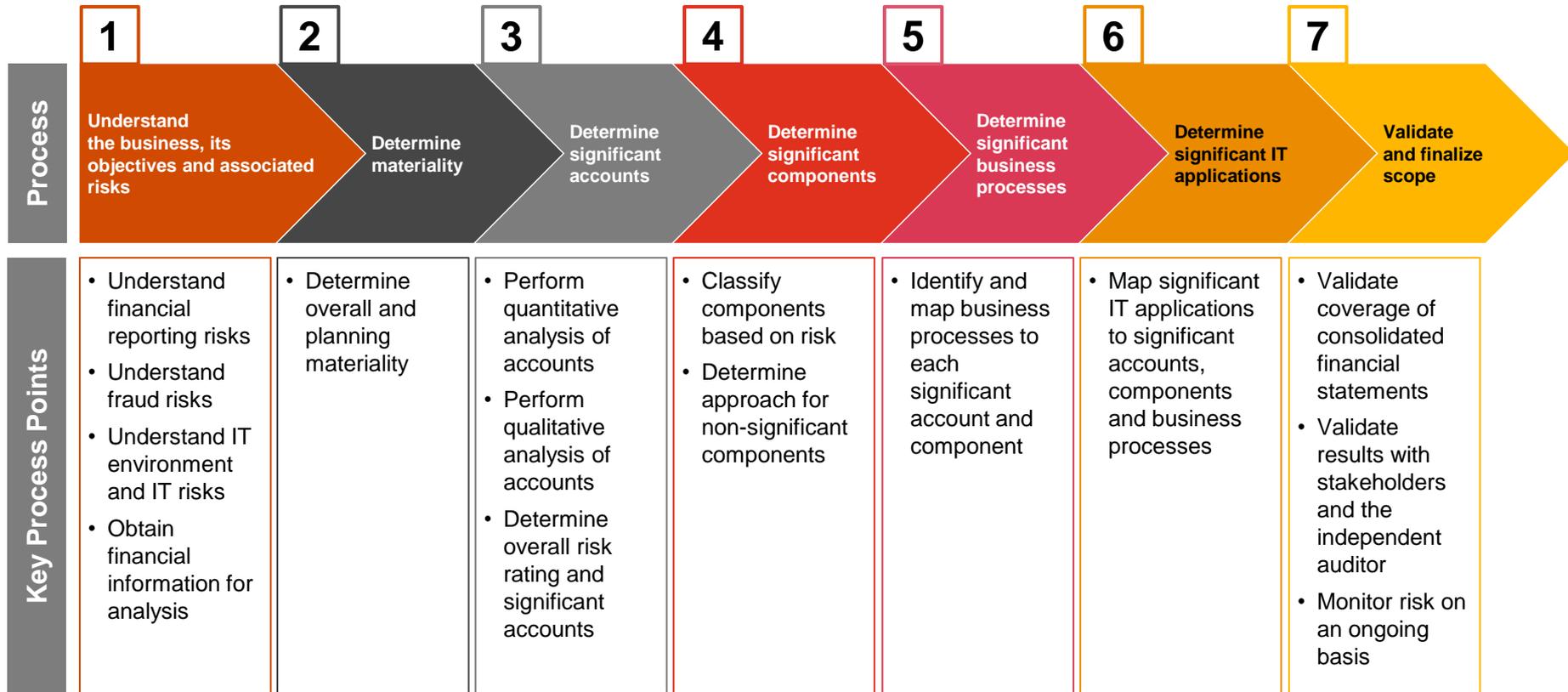
This process is most effective when Management has a solid understanding of the relationship between accounts, components and the associated business process activities.



How do you identify them?

- Map significant accounts and components to their respective business processes
- Make any necessary adjustments for additional qualitative factors that may arise
- Use information gathered during business process walkthroughs to identify significant IT applications

Step 7



Step 1 - Cont'd

To determine the extent of testing/ sample size selection, we refer to the PCAOB sampling methodology, as follows:

Frequency of Control	Assumed population of control occurrence	Number of items to test
Annual	1	1
Quarterly	4	2
Monthly	12	2 to 5
Weekly	52	5, 10, 15
Daily	250	20, 30, 40
Multiple times per day	Over 250	25, 45 , 60

Deficiency Evaluation



Deficiency Evaluation Process - Definitions

Reporting requirement

Control deficiency



A deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

Management classification

SUMMARY

FSLI COVERAGE

COSO PRINCIPLES

CONTROL MATRIX

RECOMMENDATIONS

Process	COSO Component	COSO Principles	Control #	Assertions
All	All	All	All	All

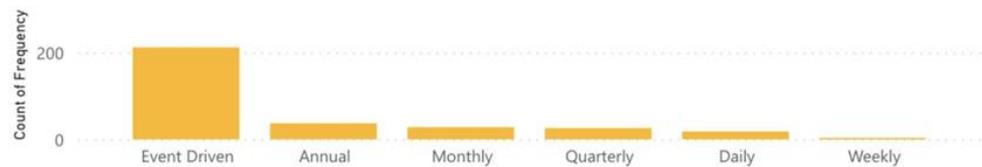
Financial statements line items

Name	No of Controls
Cash and bank balances	33
Customers' current accounts	23
Depreciation and amortisation	12
Due from banks	16
Due to banks	16
Equity of investment account holders	11
Fee and commission net income	12
Finance expenses	12

Business processes



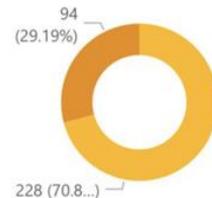
Frequency of control occurrence



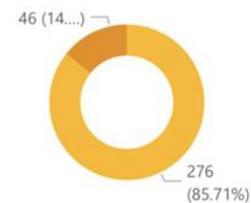
COSO components

Name	Count of Control #
Control Activities	223
Control Environment	199
Information & Communication	6
Monitoring Activities	33
Risk Assessment	3

Key/Non-Key



Preventive/ Detective

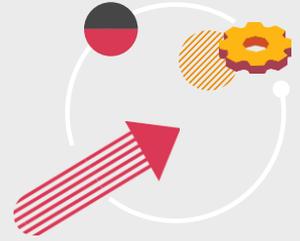


COSO Scoping - Special Considerations



Case Study

Presented by: Eslam Hassan, *Risk Senior Manager*



Case Study

Bank XYZ has 4000+ employees, with 110 branches operating across the Middle East in Egypt, UAE, Jordan, Lebanon, and Saudi Arabia. The headquarter is located in Cairo, Egypt. Bank XYZ uses ABC banking system. During the last financial year, the bank has acquired a new subsidiary in Egypt, a leasing company. The bank has recently contract with Fawry to provide e-payment solutions to clients and implement digital finance solutions. What is the impact on financial reporting internal controls scoping if the following factors are considered:

- The bank has multiple locations
- The bank has recently acquired a subsidiary
- The bank has outsourced e-payment solutions



Scoping Considerations

As you right-size the scope of your project, you will need to make sure you considered factors that contribute to the overall breadth and depth of the project. Those matters may be affected by one or more of these issues:

- Operations in multiple locations
- Internal controls that reside with third parties, such as service organizations (SOs)

Multiple Locations

- **Risks subject to centralized controls:** Some companies may manage multiple locations or business units by using standard control procedures, the same software, and centralized controls.
- **Specific risks at individual locations or business units:** In some cases, a risk may be related only to an individual location or business and therefore may not be adequately addressed by the common controls.
- **Low-risk locations or business units:** Some of the controls that operate at an individual location or business unit may be related to risks that are relatively low, based on experience and prior testing.

Service Organisations - The Basics



What is a service organization?

A service organization is an entity (or segment of an entity) that provides services to a user entity that are part of the user entity's information system.



Why is it important to understand how service organizations support significant business processes?

Many companies use outside service organizations to process financial data. The use of a service organization neither **reduces or eliminates Management's responsibility** to maintain effective ICFR for its processes.



What is a SOC 1 report?

The service organization may engage an auditor to issue a report on the organization's controls for use by user entities and their auditors. The primary purpose of the report is to provide information to auditors who audit the user entity's financial statements (i.e., it's an auditor-to-auditor communication).

Service Organisations - The Basics Cont'd



Are there different types of SOC reports?

There are two types of SOC 1 reports, a **Type 1 report** and a **Type 2 report**:

- **Type 1 Report** – reports on controls placed in operation. This report expresses an opinion on the description of the controls at the service organization as of a specified date. However, it doesn't give Management the necessary level of evidence that controls have operated effectively over a period of time and, thus, typically needs to be supplemented by tests of controls by Management.
- **Type 2 Report** – reports on controls placed in operation and tests of operating effectiveness. This report provides a description of the results of tests of operating effectiveness performed by the service auditor, as well as the service auditor's opinion on whether the controls that were tested were operating effectively during the specified period

A **SOC 2 report** is **not** designed to be used for ICFR, but instead for outside institutions (customers, regulators, etc.).

What if I can't get a SOC 1?

In certain circumstances, management may encounter difficulty in assessing certain aspects of its ICFR. The Commission's disclosure requirements state that management's annual report on ICFR must include a statement as to whether or not ICFR is effective and **do not permit management to issue a report on ICFR with a scope limitation.**

Therefore, management must determine whether the inability to assess controls over a particular process is significant enough to conclude in its report that ICFR is not effective.

In such cases, Management can decide to perform one or more of the following procedures in addition to testing user controls to uncover evidence the service organization controls are operating effectively:

- Evaluating procedures performed by management and the results of those procedures.
- Performing tests of controls at the service organization.
- Engaging another auditor to perform the procedures that will provide the needed information, such as performing attestation examination or agreed-upon procedures that describe relevant controls tests.

I got the SOC 1 – now what?



There is a lot to look at in SOC1 reports, including:

- The **time period** covered by the tests of controls and its relation to ICFR assessment period.
- Whether **controls** the service organization identified are relevant and, if so, whether Management has designed and implemented such controls.
- The **scope** of the examination and applications covered, the controls tested, and the way in which tested controls relate to the company's controls.
- The report identifies controls over the service organization's activities that support relevant financial statement assertions at the user entity.
- The report includes both an evaluation of the design of controls and tests of operating effectiveness (i.e., a **Type 2 report**).
- The **results** of those controls tests, as well as the service auditor's opinion on the controls' operating effectiveness and whether each control objective was achieved.
- Whether **significant changes** that have occurred at the service organization between the SOC 1 report date and the user entity's financial year-end date have been identified and addressed.
- Whether the report excludes the services provided by a **subservice organization** that are relevant to the audit of the user entity's financial statements.
- The **impact** the results of control tests have on the assessment of ICFR.



Fraud Considerations

If the entity uses a service organization that has either reported to Management or Management is otherwise aware of fraud, non-compliance with laws and regulations, or uncorrected misstatements affecting the financial statements of the entity, Management may consider how such matters affect the NTE of further procedures, which may require additional information from the service organization.



Identified Deficiencies

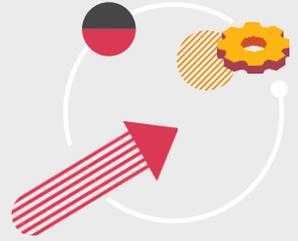
Management should evaluate control deficiencies identified at the service organization in line with its standard deficiency evaluation and aggregation process.

Roles & Responsibilities



Group Discussion

Moderator: Mohamed Elmoataz, Financial Services Advisor



Knowledge Check Up

Which line of defense is responsible for the activities below?

Activity	Responsibility of 1st Line of Defense	Responsibility of 2nd Line of Defense	Responsibility of 3rd Line of Defense
Evaluate and communicate internal control deficiencies in a timely manner to those parties responsible for taking corrective action.			
Express an opinion over the effectiveness of internal control measures.			
Evaluate the adequacy and effectiveness of controls in responding to risks within the organization's oversight, operations, and information systems.			
Select and develop control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
Specify objectives with sufficient clarity to enable the identification and assessment of risks relating to compliance objectives, operational objectives, and internal reporting objectives			
Identify risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
Define expectations about integrity and ethical values, transparency, and accountability for the performance of internal control responsibilities.			

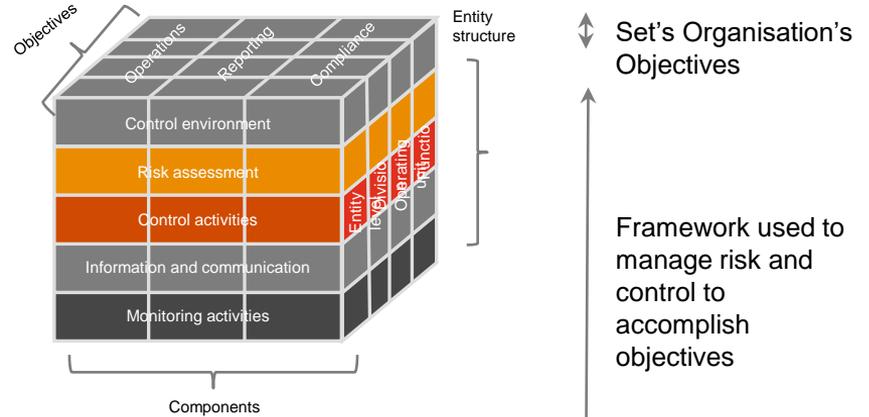
Knowledge Check Up Cont'd

Which line of defense is responsible for the activities below?

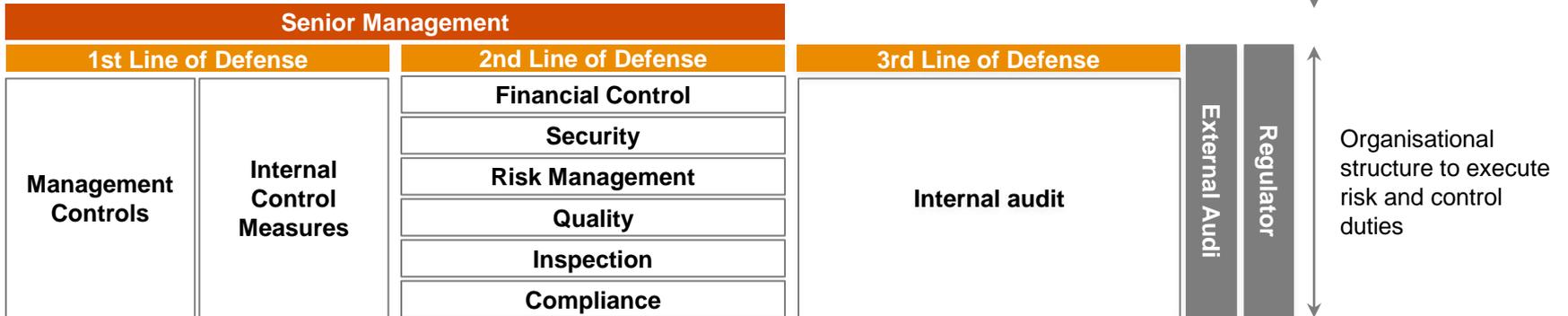
Activity	Responsibility of 1st Line of Defense	Responsibility of 2nd Line of Defense	Responsibility of 3rd Line of Defense
Guide the development and implementation of internal control policies and procedures that address the objectives .			
Provide assurance and advisory support to management on internal control.			
Identify and assess changes that could significantly impact the system of internal control.			
Establish structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
Considers the potential for fraud in assessing risks to the achievement of objectives.			
Obtain and use relevant, quality information and communicate information internally/externally to support the functioning of internal control.			
Specify objectives with sufficient clarity to enable the identification and assessment of risks relating to external financial reporting objectives.			
Holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			

Recap: The Three Lines Model

The Three Lines Model (the Model) addresses how specific duties related to risk and control could be assigned and coordinated within an organization. The model clarifies the difference and relationship between the organizations' assurance and other monitoring activities.



The Organisation's Board



Thank you



pwc.com.me

© 2023 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.