MOHAMED BIN ZAYED
UNIVERSITY OF
ARTIFICIAL INTELLIGENCE

Internal Control Over Financial Reporting (ICFR) Framework

Prepared By: Date:21. 02.2023	Consultant agent GT
Reviewed By: Date: 22.02.2023	Finance Department & IEQA
Approved By: Date: 24. 04.2023	MBZUAI Board of Trustees (BoT)

Revision No. & Effective Date:	Approved: Date:
Revision No. & Effective Date:	Approved: Date:

A review of this framework must be performed every 2 years, and all related updates must be captured within this framework and reflected within the Amendment Sheet (on page 3).

DISTRIBUTION LIST

Distribution	Copy No.	Copyholder	Signature	Date

AMENDMENT SHEET

Document #: 1	Current Revision #: 1	Date Issued: 24.04.2023 New document

Rev. #	Date	Section	Sub-Section	Page#	Nature of Amendment	Done By

Table of Contents

1. Glossary

The following definition(s) apply to this policy document:

Terms / Abbreviations	Definitions
Application Controls in Information Technology (IT)	Manual or automated procedures that typically operate at a business process level. Application controls can be preventative or detective in nature and are designed to ensure the integrity of the accounting records. Accordingly, application controls relate to procedures used to initiate, record, process and report transactions or other financial data.
Assertions	Representations by Management, explicit or otherwise, that are embodied in the financial statements, as used by the auditor to consider the different types of potential misstatements that may occur.
Complexity	The scope and nature of a risk to the entity's success
Compliance and Risk officer / Manager	A position reporting to MBZUAI's senior management as part of the second line of defense responsible for review and monitoring of ICFR
Control Effectiveness	A rating of how well risk mitigations are expected to reduce an associated risk event's impact and/or likelihood. For example, a high control effectiveness indicates that the controls should significantly reduce the negative outcomes associated with a risk.
COSO	Committee of Sponsoring Organizations of the Treadway Commission. Five major U.S. professional associations initially organized it and includes included representatives from industry, public accounting, investment firms, and the New York Stock Exchange. COSO provides thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence.
Data	Raw facts that can be collected together to be analyzed, used or referenced.
Design Adequacy	Design adequacy is a measure of how well a system performs its functions. It is the most desired factor in the definition, design, and early stages of system development. A design adequacy quantification methodology is presented, and the relationship between design limitation and adequacy is discussed.
External Auditor	An external auditor performs an audit, in accordance with specific laws or rules, of the financial statements of a university, and is independent of the entity being audited. External Auditors inspect clients' accounting records and express an opinion as to whether financial statements are presented fairly in accordance with the applicable accounting standards of the

	entity, such as International Public Sector Accounting Standards (IPSAS).
External Environment	Anything outside of the entity that influences the ability to achieve strategy and business objectives
Fraud	An intentional act by one or more individuals among Management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage.
Financial Statements	Financial Statements are the reports that provide details of the entity's financial information including assets, liabilities, equities, incomes and expenses, shareholders' contribution, cash flow, and other related information during the period of time. Financial statements are formal records of the financial activities and position of a business, person, or other entity. Relevant financial information is presented in a structured manner.
Gap Assessment	Gap assessment involves the comparison of actual performance with potential or desired performance to determine whether business requirements are being met and, if not, what steps should be taken to ensure they are met successfully.
Governance	The systems and processes that ensure the overall effectiveness of an entity.
ICFR	Internal Control Over Financial Reporting.
Impact	The result or effect of a risk. There may be a range of possible impacts associated with a risk. The impact of a risk may be positive or negative relative to the entity’s strategy or business objectives.
Internal Audit	Internal auditing is an independent, objective assurance and consulting activity designed to add value to and improve an organization's operations. Internal auditors may belong to an internal audit department or equivalent function. Internal audits provide Management and Board of Trustees with a value-added service where flaws in a process may be caught and corrected prior to external audits.
Internal Control	A process, effected by an entity’s Board of Trustees, Management and other personnel, is designed to provide reasonable assurance regarding achieving objectives relating to operations, reporting, and compliance.
ITGC	Information Technology General Controls.
Likelihood	The possibility that a given event will occur.
Management/Senior Management	The person(s) with executive responsibility for the conduct of the entity’s operations.
Materiality/ Materiality Assessment	The process of identifying, refining, and assessing potential activities/accounts that could affect/impact the business and/or your stakeholders.
MBZUAI	Mohamed Bin Zayed University of Artificial Intelligence.
Mitigation	Mitigation refers to the processes put in place by Management/Senior Management that seek to reduce the

	likelihood of risk events occurring and/or their impact should risk events materialize.
Non-Compliance	Acts of omission or commission by the entity, either intentional or unintentional, which are contrary to the prevailing laws or regulations.
Objectives/Business Objectives	Those measurable steps the entity's/organizations take to achieve its strategy.
PLC	Process Level Controls.
Resources	Resources (e.g., human, social, natural) that businesses need in order to create and sustain value.
RCM	Risk & Control Matrix is a tool that assists the organization identify, rank, and implement control measures to mitigate risks. It is a repository of risks that pose a threat to an organization's operations, as well as the controls in place to mitigate those risks.
Sampling	The application of procedures to less than 100% of items within a population of testing relevance such that all sampling units have a chance of selection in order to provide the auditor/consultant with a reasonable basis on which to draw conclusions about the entire population.
Stakeholders	Parties that have a genuine or vested interest in the entity.
Standards of Conduct	Organization's expectations of ethical values communicated by Management to employees and other related parties through different formats, such as policies, operating principles, guidelines etc.
Tolerance	The boundaries of acceptable variation in performance related to achieving business objectives.
Tone at the Top	Management leads by example (through directives, attitudes, and behavior) to demonstrate a commitment to the organization's integrity and ethical values.

2. Background and Objective

2.1. Background

The Resolutions issued by the ADAA (Resolution #1 of 2017 and #88 of 2021), require external auditors of ADAA subject entities to express an opinion on the effectiveness of internal controls 'relevant to the audit'.

The Resolution requires external auditors to issue a separate opinion on the operational effectiveness of internal controls relevant to the audit. In order to issue such an opinion, external auditors will need to carry out extensive testing of the internal control framework in place at the ADAA subject entities across areas such as governance, process cycle controls and IT general controls i.e. test the control design adequacy and operating effectiveness.

In compliance with ADAA resolution ADAA subject entities shall adopt a formal Internal Control Framework., however, the framework should be a recognized framework established by a body/group that is globally accepted, or it may be internally developed; as long as it provides basis for the management's assessment of the ICFR (Internal Control Over Financial Reporting); and an independent opinion of the external auditors.

To ensure compliance with the ADAA Resolution, MBZUAI has adopted the COSO 2013 Framework (Committee of Sponsoring Organizations of the Treadway Commission) as the internal framework, to test, maintain and monitor adequate and effective internal controls over financial reporting.

2.2. Objectives

ICFR involves designing and implementing a system of controls, policies, and procedures to provide reasonable assurance that financial reporting is accurate, complete and in compliance with accounting standards.

The key objectives of ICFR are to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements in accordance with accounting standards. The main objectives of ICFR are:

1. Ensuring accurate and complete financial reporting.
2. Protecting the University's assets.
3. Compliance with laws and regulations.
4. Enhancing the effectiveness and efficiency of operations.
5. Improving the quality and credibility of financial reporting.

The objectives of ICFR Framework includes:

1. Define the adopted internal control framework.
2. Facilitate alignment of ICFR with the entity's overall risk management strategy and comply with any relevant laws and regulations.
3. Establish the responsibilities of Management towards ICFR and the implementation and maintenance of effective internal controls.
4. Detail the reporting obligations for employees and management.

3. Responsibilities

3.1. Overview

Management is responsible for ensuring the implementation and maintenance of effective internal controls. This includes regularly assessing the ICFR framework to ensure it remains relevant and effective, monitoring the performance of the controls, and taking corrective action when necessary. Management should also ensure that employees understand their roles and responsibilities in the ICFR framework and receive proper training on the controls and procedures.

3.2. Detailed ICFR responsibilities:

3.2.1. Responsibility of Senior Management

- Responsible for the design, implementation, and monitoring of ICFR, through development of an appropriate internal control framework and internal control procedures for MBZUAI.
- Design, implement and maintain procedures to monitor compliance to laws, regulations & internal policies.
- Select and apply appropriate accounting policies. Making accounting estimates that are approved and reasonable (ensuring existence of supporting documents).
- Annually assess the effectiveness of ICFR (Assess the entity's system of internal control in relation to the COSO Framework, focusing on how the entity applies the 17 principles in support of the components of internal control).
- Evaluate any change in the University's internal control over financial reporting that occurred during a fiscal quarter that has materially affected, or is reasonably likely to materially affect, the University's internal control over financial reporting.
- Maintain evidential matter, including documentation, to provide reasonable support for its assessment of ICFR.
- Provide quarterly and annual reporting of management's assessment of the university's ICFR.
- Provide regular reports to the board of trustees or audit committee on the effectiveness of the ICFR framework, including any identified deficiencies and any actions taken to address them.

3.2.2. Responsibility of Compliance and Risk officer / Manger

Senior Management would delegate the responsibility of monitoring ICFR to the Compliance and Risk officer / Manger, who would play a critical role in ensuring the reliability and integrity of an entity's financial information and promoting confidence in the financial reporting process. Key responsibilities would include:

- Perform ICFR assessment to assess the effectiveness of ICFR throughout the fiscal year and monitor the performance of the controls.
- Report to the Senior Management at least annually on potential control weaknesses or deficiencies, incidents of fraud or non-compliance, and any other information relevant to the ICFR framework.
- Perform quarterly follow-ups on the ICFR remediation plans implementation and escalate any delays.
- Liaison with external auditors and provide access to information (as required).
- Provide training and guidance to employees on the ICFR framework, including their roles and responsibilities.
- Stay current with changes to laws, regulations, and best practices relevant to ICFR and ensure that the ICFR framework remains compliant.

3.2.3. Responsibility of In-Scope Department/Process Owners

- Ensure the controls implemented are adequate in terms of design and operating effectiveness in the course of day-to-day/periodic activities.
- Ensure all activities within the department (with key importance to activities that have an impact on financial reporting) are safeguarded with active and effective controls.
- Perform periodic monitoring to ensure controls are operating as required, risks are monitored (pre-dominantly key risks/risks that may result in colossal business impact) and mitigated.
- Prepare internal reports (as required by the relevant department to discuss the status of remediation plans, etc.).
- Ensure approved remediation plans captured within ICFR Gap Assessment Report are implemented as per the planned implementation date. Delays in implementing the same must be communicated to authorized personnel.
- Any gaps identified during periodic monitoring must be communicated to the authorized personnel, further investigated, and remediation plans must be considered.
- Conduct periodic internal meetings with Senior Management to discuss ideas on how to strengthen internal controls feasibly and how existing controls affect the relevant COSO principles within the five (5) components of internal control.

3.2.4. Responsibility of the Audit Committee

The Board of Trustees has the general oversight responsibility for all the University's activities, including the preparation of financial statements and the design and operation of controls. The board's oversight of ICFR often is delegated to the Audit Committee, which has responsibility for:

- Overseeing management's assessment of ICFR: The Audit Committee should review management's assessment of the effectiveness of the ICFR and discuss any significant deficiencies or material weaknesses identified.
- Evaluating the external auditor's work: The Audit Committee should review the external auditor's findings and recommendations related to ICFR and discuss any significant issues with the auditor.
- Monitoring management's response to control deficiencies: The Audit Committee should monitor management's response to control deficiencies and ensure that appropriate corrective action is taken in a timely manner.
- Communicating with stakeholders: The Audit Committee should communicate with stakeholders, such as regulators, about the university's ICFR and the Audit Committee's role in overseeing it.

3.3. Role of External Auditor

- Obtain reasonable assurance if the university has maintained effective ICFR in all material aspects and express an opinion on the operating effectiveness of the ICFR.
- Obtain an understanding of internal controls over financial reporting, identify, and assess the risks, test and evaluate the design and operating effectiveness of internal control, based on the assessed risk and perform other procedures as considered necessary in the circumstances.

4. Implementation (Planning, Execution, Reporting and Monitoring)

4.1. COSO Framework

Regulations emphasizes on the requirement for all ADAA subject entities to maintain adequate and effective internal controls over financial reporting. In order to ensure compliance with the regulations, MBZUAI has adopted the COSO framework to enable the university to effectively and efficiently evaluate & monitor existing Internal Controls or develop (design/implement) new processes and systems of internal control over financial reporting, that adapt to changing business and operating environments, mitigate risk to acceptable levels, and support sound decision making and governance of the university, concerning financial reporting.

As per the COSO framework, internal control is a process effected by an entity's board of Trustees, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Adequacy, effectiveness, and efficiency of operations that impact financial reporting.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

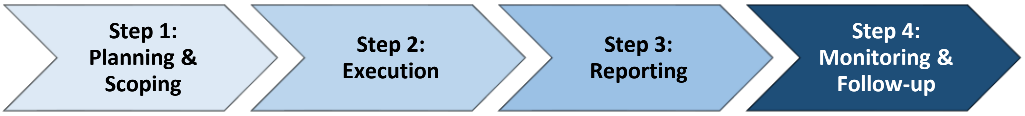
4.2. ICFR Key Phases

The ICFR journey consists of four (04) key phases:

1. Establish the COSO framework to address ICFR requirements, perform gap assessment and review the design adequacy and operating effectiveness of internal controls over financial reporting.
2. Provide the gap assessment report to the Senior Management and subsequently the Audit Committee including the results of the ICFR assessment annually.
3. Remediate control gaps identified during the gap assessment and test the operating effectiveness of implemented ICFR during the quarterly follow-up assignments.
4. Obtain a separate opinion from external auditors on the operating effectiveness of ICFR controls from the year end 2021 onwards.

4.3. ICFR Implementation Steps

MBZUAI has adapted a four (04) steps approach to perform the Gap Assessment of internal control over financial reporting, based on the COSO framework. This shall be carried out by the Compliance and Risk officer / Manger in liaison with the respective in-scoped department/process owner as per the defined timeline. A detailed description of the approach is illustrated below:



4.3.1. Step 1: Planning & Scoping

1

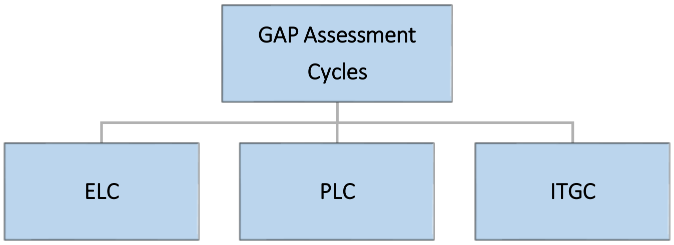
- Finalize scope and develop the gap assessment plan.
- Engage with process/control owners and key stakeholders, including external auditors (if required, via the Finance Department).
- Identify key controls and agree with the Finance Department and external auditors (if required) to drive more efficiency.

4.3.1.1. **Planning:** During this phase, the Compliance and Risk officer / Manager shall develop and finalize the gap assessment plan, including but not limited to;

- Identifying the in-scope cycles,
- Develop the timeline required to conduct the assessment,
- Identifying the in-scope significant accounts
- Communicating gap assessment commencement to the stakeholders via email.

4.3.1.2. **Scoping:** The ICFR gap assessment is divided into 3 areas/cycles:

- Entity Level Controls (ELC),
- Process Level Controls (PLC)/Business Processes,
- Information Technology General Controls (ITGC) - Application Controls.



- **Materiality:** Calculate the materiality benchmark and agree on the materiality threshold by communicating with the Finance Department. This materiality benchmark shall be used as the basis for scoping significant accounts that should be part of the PLC process. It will also form the basis for the external auditors to determine the nature and scope of their procedures. Materiality shall be calculated as identified below;

  - Identify the basis on which (e.g., net profit, revenue, expense, etc.) and the threshold (e.g., 5%) at which the external auditors benchmark materiality, by communicating with the Finance Department.
  - The Compliance and Risk officer / Manager may either utilize the same materiality threshold or chose to take a conservative approach by reducing the materiality threshold by 1 to 0.5 %, to increase the scope.
  - Calculate the materiality based on the agreed threshold and base account (e.g., 5% of net profit).
  - Upon calculating materiality, compare the yielded materiality value against the prior year's audited financial statements (Balance Sheet & Income Statement).
  - Identify the process/accounts that shall be scoped in the PLC testing phase (those accounts that are equal to and above the yielded materiality value).
  - Communicate the in-scope accounts with the Finance Department and agree on the materiality threshold and in-scope accounts.

- In addition to the materiality threshold, in-scope areas may be subject to change/addition based on the review of key business activities, considering historical misstatements (if any), any susceptibly to fraud, any control weakness noted in the prior years, and discussions with the management and external auditors (if applicable).
- Map the significant accounts to their relevant financial statement assertions (e.g., completeness, existence, valuation, etc.), identify the major classes of transactions (routine, estimates, or non-routine) and the related business processes and accounting activities that influence the significant accounts.

4.3.2. Step 2: Execution

During this phase the Compliance and Risk officer / Manger shall perform process understanding and gap assessment. Several steps shall be carried out to assess the adequacy and effectiveness of internal controls over financial reporting and further identify any existing gaps and suggest remediation plans.

Execution step 1: Documentation of ELC	**Execution step 2: Documentation of PLC & ITGC**
- Review existing policies and procedures, risk control matrices (RCM) and conduct walkthroughs to determine the level of existing internal financial control compliance. - Evaluate the ELC RCM against the COSO Framework requirements (for each of the 17 Principles across the five Components).	- Review existing policies and procedures and conduct walkthroughs to determine the level of existing internal financial control compliance. - Conduct process understanding meetings for in-scop processes and document process narratives to capture the existing control environment.

<table>
<tr>
<td>- Obtain MBZUAI’s Organization Chart to determine the degree of centralization of the ELC in place.
- Identify the members and conduct meetings with the Senior Management Team/process owners to gain an understanding of the ELC.
- Conduct walkthroughs to confirm control design and perform operative effectives testing.
- Document the ELC RCM with controls in the place to provide reasonable assurance that appropriate controls exist to mitigate material misstatement of the financial statements, fraud or misappropriation of assets.
- Validate the ELCs with the Senior Management Team/process owners.</td>
<td>- Identify broad categories and sources of risks for each business process, including IT risks.
- Develop RCMs to ensure coverage of all financial reporting assertions.</td>
</tr>
<tr>
<td colspan="2"><b><u>Execution step 3: Gap assessment, reporting and remediation planning</u></b>
- Review existing policies and procedures, risk control matrices (RCM) and conduct walkthroughs to determine the level of existing internal financial control compliance.
- Identify design and operating effectiveness control gaps.
- Evaluate the root cause for identified deficiencies.
- Recommend mitigation plan for remediation.
- Discuss exceptions identified with the process owners and management as required.
- Agree on a remediation plan and support management in remediating the gaps.</td>
</tr>
</table>

4.3.2.1. Documentation of ELC

- Internal control over financial reporting are the controls specifically designed to address the risks of intentional or unintentional misstatements in the financial statements. The COSO integrated framework for internal control has **five (5) components** which includes;
    1. **Control Environment/Tone at the Top:** this sets the tone for the organization, influencing the control consciousness of its people.
    2. **Risk Assessment:** identification and analysis of risks to achieve objectives.
    3. **Control Activities:** policies and procedures that help ensure management directives are carried out.
    4. **Information & Communication:** Systems or processes that support identifying, capturing, and exchanging information in a form and timeframe that enables people to carry out their responsibilities.
    5. **Monitoring:** processes used to assess the quality of internal control performance over time.

4.3.2.1.1. Relationship of Objectives and Components

- A direct relationship exists between objectives, which are what the University strives to achieve, and the components, which represent what is required to achieve the objectives, and the organizational structure of the University (the operating units, legal entities, and other). The relationship can be depicted in the form of a cube as captured in Exhibit 1.

- The three categories of **objectives** - operations, reporting, and compliance are represented by the columns.
- The five **components** are represented by the rows.
- The third dimension represents the University’s organizational structure.

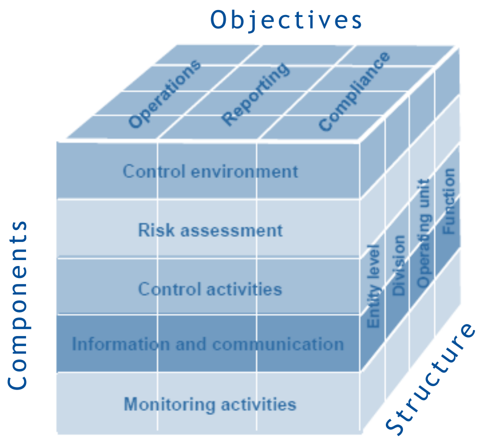


Exhibit 1: COSO Cube

- A detailed description of the 5 components is illustrated below:

#	Components	Principles	Points of Focus
1.	**Control Environment**	Demonstrates commitment to integrity and ethical values	Sets the tone at the top
			Establishes standards of conduct
			Evaluates adherence to standards of conduct
			Addresses deviations in a timely manner
		Exercises oversight responsibility	Establishes oversight responsibilities
			Applies relevant expertise
			Operates independently
			Provides oversight on Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities
		Establishes structure, authority, and responsibility	Considers all structures of the University
			Establishes reporting lines
			Defines, assigns, and limits authorities and responsibilities
		Demonstrates commitment to competence	Establishes policies and practices
			Evaluates competence and addresses shortcomings
			Attracts, develops, and retains individuals
			Plans and prepares for succession
		Enforces accountability	Enforces accountability through structures, authorities, and responsibilities
			Establishes performance measures, incentives, and rewards
			Evaluates performance measures, incentives, and rewards for ongoing relevance

#	Components	Principles	Points of Focus
			Considers excessive pressures
			Evaluates performance and rewards or disciplines individuals
2.	**Risk Assessment**	Specifies suitable objectives:	
		- Operations Objectives	Reflects management's choices
			Considers tolerances for risk
			Includes operations and financial performance goals
			Forms a basis for committing of resources
		- External Financial Reporting Objectives	Complies with applicable accounting standards
			Considers materiality
			Reflects University activities
		- External Non-Financial Reporting Objectives	Complies with externally established standards and frameworks
			Considers the required level of precision
			Reflects University activities
		- Internal Reporting Objectives	Reflects management's choices
			Considers the required level of precision
			Reflects University activities
		- Compliance Objectives	Reflects external laws and regulations
			Considers tolerances for risk
		Identifies and analyzes risk	Includes the University, subsidiary, division, operating unit, and functional levels
			Analyzes internal and external factors
			Involves appropriate levels of management
			Estimates significance of risks identified
			Determines how to respond to risks
		Assesses fraud risk	Considers various types of fraud
			Assesses incentives and pressures
			Assesses opportunities
			Assesses attitudes and rationalizations
		Identifies and analyzes significant change	Assesses changes in the external environment
			Assesses changes in the business model
			Assesses changes in leadership
3.	**Control Activities**	Selects and develops control activities	Integrates with risk assessment
			Considers University-specific factors
			Determines relevant business processes
			Evaluates a mix of control activity types
			Considers at what level activities are applied
			Addresses segregation of duties
		Selects and develops general controls over technology	Determines dependency between the use of technology in business process and technology general controls
			Establishes relevant technology infrastructure control activities
			Establishes relevant security management process control activities
			Establishes relevant technology acquisition, development, and maintenance process control activities
		Deploys through policies and procedures	Establishes policies and procedures to support deployment of management's directives
			Establishes responsibility and accountability for executing policies and procedures
			Performs in a timely manner
			Takes corrective action
			Performs using competent personnel

#	Components	Principles	Points of Focus
			Reassesses policies and procedures
4.	**Information & Communication**	Uses relevant information	Identifies information requirements
			Captures internal and external sources of data
			Processes relevant data into information
			Maintains quality throughout processing
			Considers costs and benefits
		Communicates internally	Communicates internal control information
			Communicates with the board of Trustees
			Provides separate communication lines
			Selects relevant method of communication
		Communicates externally	Communicates to external parties
			Enables inbound communications
			Communicates with the board of Trustees
			Provides separate communication lines
			Selects relevant method of communication
5.	**Monitoring Activities**	Conducts ongoing and/ or separate evaluations	Considers a mix of ongoing and separate evaluations
			Considers rate of change
			Establishes baseline understanding
			Uses knowledgeable personnel
			Integrates with business processes
			Adjusts scope and frequency
			Objectively evaluates
		Evaluates and communicates deficiencies	Assesses results
			Communicates deficiencies to parties responsible for corrective action and to senior management and the board of Trustees
			Monitors corrective actions

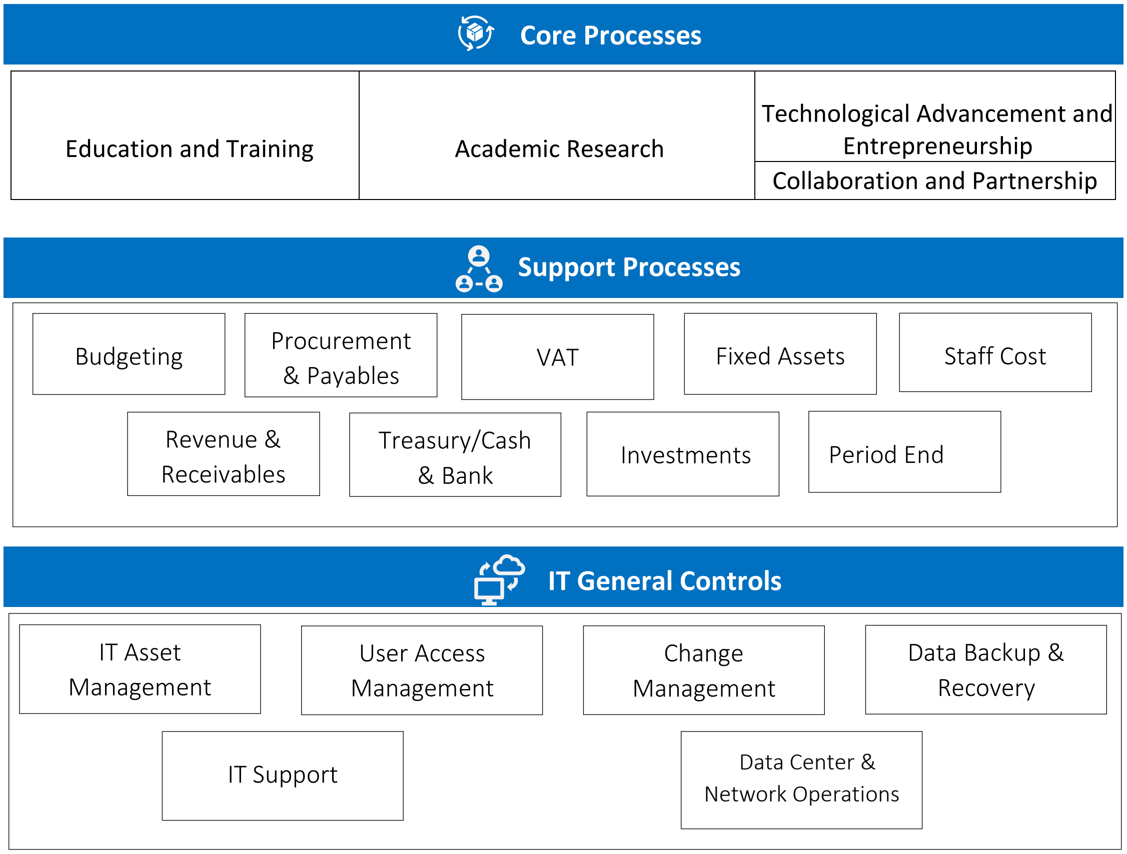
- *Identified below are the main scope areas for entities (non-exhaustive list), which should be covered as part of the ELC ICFR gap assessment. In-scope areas are subject to change based on the risks captured within the RCM and discussions with the management.*

Entity Level Control (ELC)

Organization structure	Enterprise risk management	Budgeting and management information systems	Delegation of authority	Policies and procedures
Code of conduct	Whistleblower mechanism	Internal audit	HR review and oversight	Financial review and oversight
	Board and Audit Committee operation	Third-party relationships	IT entity controls	

4.3.2.2. Documentation of PLC & ITGC

- Identified below are the main scope areas for entities, (non-exhaustive list), which will be covered as part of the PLC & ITGC ICFR gap assessment. In-scope areas are subject to change based on the review of key business activities, materiality and discussions with the management and external auditors, that will be conducted as part of the scoping exercise.



Core Processes

Education and Training

Academic Research

Technological Advancement and Entrepreneurship

Collaboration and Partnership

Support Processes

Budgeting

Procurement & Payables

VAT

Fixed Assets

Staff Cost

Revenue & Receivables

Treasury/Cash & Bank

Investments

Period End

IT General Controls

IT Asset Management

User Access Management

Change Management

Data Backup & Recovery

IT Support

Data Center & Network Operations

4.3.2.2.1. Documenting of current processes and controls

- Once the processes that are relevant and significant to the control activity component of the 2013 COSO Framework are identified, the next step is to carry out the GAP assessment, understand and document each process in order to identify those processes that may have a direct or in-direct impact over financial reporting, identify internal controls (or detect control gaps) within those processes.
- Identified below are the steps that shall assist in documenting the current processes and controls:
  - **Kick-off/introduction meeting:** Engage with process owners/management: prior/during each functional process understanding discussions, and communicating its purpose, benefits, and visibility to senior leadership and the importance of governance, to ensure the process owners'/management's full participation.
  - **Review existing documentation:**
    - Provided that documentation is available, initiate the initial document request with the process owner. This step shall give a good understanding of the current control structure and aid to plan for location visits (if required, to different branches) and conduct process understanding meetings with the relevant employees.

- If the documentation is formalized and complete, process understanding of business processes may be completed efficiently. This shall further assist in focusing on any process changes since the documentation was last updated (pre-dominantly during periodic annual gap assessments). E.g., policies and procedures, job responsibilities, etc.
- This information may be a good starting point and helps to gain a more detailed understanding of certain activities in the process. However, the documentation might be more tailored to explaining job responsibilities and specific job activities rather than explaining how a transaction flows through a system, where risks may exist for processing errors, and what internal controls are in place. Hence, the team performing the gap assessment must ensure the financial transaction flow is understood and captured from end to end, with the associated control within a process narrative document.

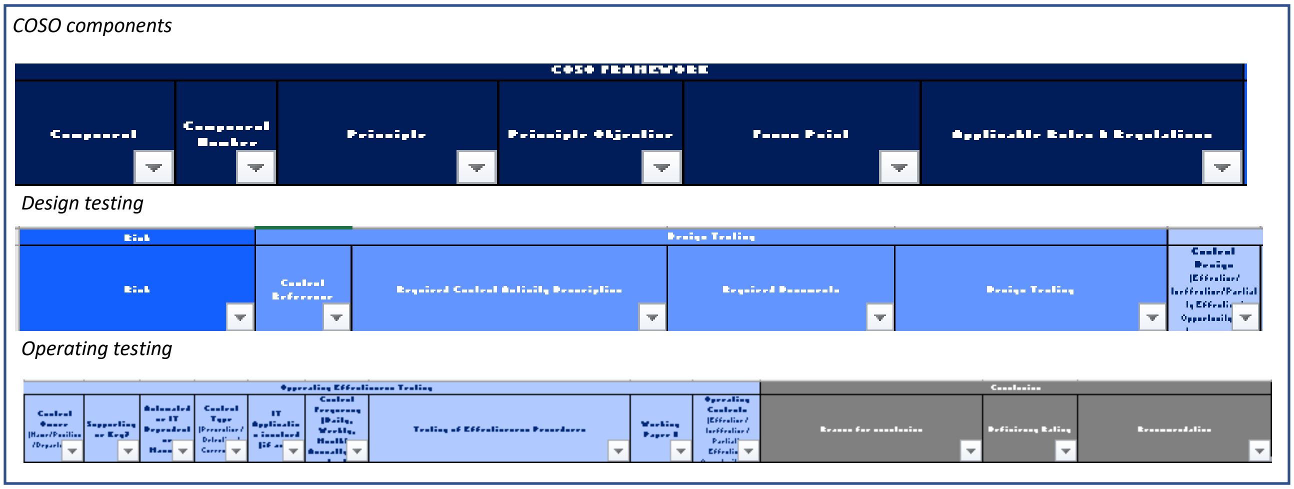
- **Conduct Process Understanding Meeting:**
  - With the information obtained during the review of the existing documentation, conduct process understanding meetings with relevant process owners.
  - The information gleaned during such meetings provides the evidence to make informed decisions about the department's compliance with the process.
  - If necessary, interviews may be conducted using technology to eliminate the need for face-to-face meetings. In addition, using well-tailored questionnaires in such situations can also be very effective. Given the complexity of certain cycles, it may take multiple interview sessions to fully understand the process.
  - Gain further understanding of the processes and related controls involved in generating financial statement information. The documentation approach for this step shall focus on the significant accounts/groups of accounts, Information Technology (IT) processes, and key spreadsheets used, that influence the significant account to determine the types of errors that can occur in initiating, authorizing, recording, processing, and reporting transactions, and Identifying controls, including IT controls that serve to prevent or detect errors could lead to financial misstatement on a timely basis, as well as to prevent and detect fraud.
  - Conduct meetings with the process owners to document/update process narratives and identify key subprocesses, risks (what can go wrong), and controls in place to mitigate such risks, type of control, frequency of controls, control owner, etc.
  - Perform a walkthrough of all the key controls identified at each PLC/ ITGC application.
- **Identify risks, controls, and gaps of existing processes:**
  - During the review of existing documentation and while performing process understanding meetings, begin to identify the risks, controls, and gaps related to the existing processes.
  - For control structures that are mature and complete, this process might include noting changes since the last time that the process and control documentation was updated. Building the foundation for control documentation and remediation plans for other control structures might require taking detailed notes about process risks, controls, and related gaps.
- **Prepare final process documentation with controls:**

    - Capture all documents reviewed and processes along with the controls related to ICFR with a process narrative document.
    - To demonstrate sufficient understanding of the process, the following points shall be considered (at minimum) for inclusion:
        - Basic flow of transactions from initiation to completion.
        - Personnel involved in the process flow.
        - Controls performed as part of the process flow, as well as the personnel responsible for performing controls versus those responsible for reviewing control performance.
        - Systems used in the process and reports generated by these systems.
        - Segregation of duties, whether manual or automated
  - **Validated the process narrative:** The last step is to validate the process narrative and controls with the process owners. It is important that the team obtains the control owners' confirmation of its documentation prior to presenting assessment results to the management/Audit Committee.

4.3.2.3. GAP Assessment, Reporting & Remediation Planning

- Develop the risk and control matrix (RCM) (see exhibits 2 & 3). The RCM may be developed prior/during, or post completion of process understanding.
- The RCM is a document (generally maintained in a spreadsheet format or a specialized database application) that identifies all internal controls in the process in addition to specific descriptions and category attributes related to each control. Information captured for each control shall include (at minimum) the following:
  - Focus points (ELC) and Sub-process being tested (PLC & ITGC).
  - Financial statement assertion (related to control).
  - Risk description associated with the sub-process.
  - Required Control activity, Documents, and Testing (for ELC).
  - Control number (assigned as a unique identifier).
  - Control description.
  - Control type (automated/manual) and Control type (preventative/detective).
  - Frequency of control (daily, monthly, quarterly, annually. Ad-hoc).
  - Supporting or key control (for ELC).
  - Process/Control owner name and designation (for ELC).
  - Design effectiveness test results (Effective, Partially Effective, Ineffective, Opportunity for Improvement).
  - Testing procedures for operating effectiveness.
  - Sample size and working paper reference (if appliable).
  - Operating Effectiveness Test Results (Effective, Partially Effective, Ineffective, Opportunity for Improvement).
  - Reason for the conclusion.
  - Recommendation.

Exhibit 2: ELC RCM



COSO components

COSO FRAMEWORK					
Component	Component Number	Principle	Principle Objective	Focus Point	Applicable Rules & Regulations

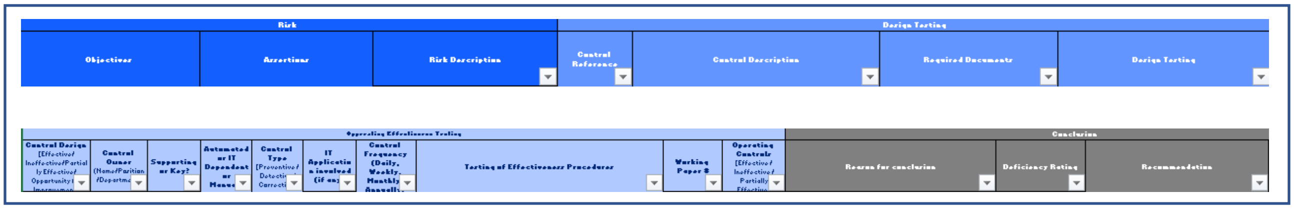
Design testing

Risk	Design Testing				
Risk	Control Reference	Required Control Activity Description	Required Documents	Design Testing	Control Design (Effective/ Ineffective/Partially Effecti Opportunity

Operating testing

Operating Effectiveness Testing									Conclusion		
Control Owner (Name/Position /Departm	Supporting or Key?	Automated or IT Dependent or Manu	Control Type (Preventive/ Detecti Corre	IT Application involved (if an	Control Frequency (Daily, Weekly, Monthl Annually	Testing of Effectiveness Procedures	Working Paper #	Operating Controls (Effective/ Ineffective/ Partial Effectiv	Reason for conclusion	Deficiency Rating	Recommendation

Exhibit 3: PLC & ITGC RCM



Risk			Design Testing			
Objectives	Assertions	Risk Description	Control Reference	Control Description	Required Documents	Design Testing

Operating Effectiveness Testing									Conclusion		
Control Design [Effective/ Ineffective/Partially Effective/ Opportunity f Improvemen	Control Owner (Name/Position /Departme	Supporting or Key?	Automated or IT Dependent or Manu	Control Type [Preventive/ Detecti Correcti	IT Application involved (if any	Control Frequency (Daily, Weekly, Monthly Annually	Testing of Effectiveness Procedures	Working Paper #	Operating Controls [Effective/ Ineffective/ Partially Effective	Reason for conclusion	Deficiency Rating	Recommendation

- Once the processes that are relevant and significant to the control activities component of the 2013 Framework and risks are identified, requested documents are received, and process understanding meetings are concluded, the next step is to carry out the GAP assessment and identify internal controls (or control gaps) against all the identified risks.
  - Evaluate the existing controls against the 2013 Framework's principles and points of focus (for ELC).
  - Identify areas where the current design of internal controls is lacking to achieve an effective internal control system.
    - In some cases, gaps identified will reveal design weaknesses in internal controls that could leave the organization vulnerable to serious financial reporting errors or misallocation of assets. In other cases, gaps identified may reveal merely areas of opportunities for improvement.
  - Identify the testing period (generally the most recent audited financial statements year i.e., January to December XX), MBZUAI's sampling methodology for testing considering the control type and frequency.
  - Based on the testing period, documents reviewed and process understating meeting conducted;
    - Test the ELC to assess if the management has created a control environment in which people are motivated to comply with controls rather than ignore or circumvent them and assess whether the necessary control mechanisms to monitor and correct non-compliance are functioning effectively.

  - Test business processes key controls (PLC) to the assess if the key controls identified are operating effectively as designed.
  - Test ITGCs to assess if the application's controls are operating effectively as designed, for the outsourced services, obtain the SOC report to review if the controls at the service provider are effective.
- Conduct testing at the ELC, PLC & ITGC levels by requesting supporting documents and documenting the same within the RCM and working papers (for sample testing).
- Test ELC and identified controls for the PLC and ITGCs to assess their operating effectiveness. The types of tests that the gap assessment team performs may vary from an inquiry, observation, reperformance, and vouching or combination of the aforementioned techniques for identified controls, dependent on the type of control (manual, IT dependent, and automated) and frequency of controls (daily, quarterly, annually, etc.).
- Update the RCM to list all control or control deficiencies, testing procedures, reasons for conclusion and recommendations.
- Communicate the results to the MBZUAI process owners, Senior Management, Director of Finance, and President as required.
- Controls must be tested based on design adequacy via walkthrough and operative effectiveness via sample testing and accordingly rate the control both design and operation independently as below;

Control Effectiveness Rating:

Rating Scale	Definition
Effective	Control is present and functioning; control design and operating effectiveness are effective.
Opportunity for improvement	Control is present and functioning, however, room for improvement is available.
Partially Effective	The control design is present however it requires improvement to address its objectives and/or control is always not operating effectively, and management must take necessary measures to ensure continuous application of the control.
Ineffective	Either control is not present or not functioning as designed to meet its objectives.

Deficiency Rating:

Rating Scale	Definition
Material weakness	A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the University's annual or interim financial statements will not be prevented or detected on a timely basis.
Significant deficiency	A significant deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the University's financial reporting.
Deficiency	A deficiency where 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

4.3.2.3.1. Design Testing & Reporting of Controls

- Key processes within the gap assessment include test design, execution, and reporting phase, which includes selecting the controls to be tested, designing the tests of controls, executing the tests as designed, and then reporting on the associated results.
    - **Selecting controls for testing:** Upon identifying the in-scope processes/accounts, the next step is to identify those processes/controls that have a direct or indirectly impact financial reporting. The team may assign a “key” or “non-key” classification to each control to aid in the selection of which controls should be part of the testing process. Key controls are the most critical controls for preventing the realization of risks and therefore are important in mitigating the risks of having a negative impact on financial reporting. Non-key controls generally are not as critical, as may be the case for duplicate controls or controls that have limited scope for select locations or specific transactions. The determination of key versus non-key is at the discretion of the GAP assessment team in liaison with the process owners.
    - **Design procedures for test of controls:** After selecting the processes/controls for testing, design the procedures for testing each control. In designing a test of controls, it is important to understand both the risk to be mitigated and the related control description, which details potential problems with the underlying activity or transaction that is intended to be mitigated.
- The control description must detail how the related control functions. Understanding both the risk to be mitigated and the control description shall help design controls tests that will apply to both the design adequacy and operating effectiveness of the controls.
- After understanding the risk to be mitigated, the related control description must be documented against the respective risk within the RCM and updated against the related process within the process narrative document.
- The next step shall be to consider the nature, timing, and extent (scope) of testing, along with the required supporting documentation to be gathered. Different methods are used to perform tests of controls and to create test plans. Each method should be evaluated based on the complexity and timing of the underlying control. It is possible that multiple methods of testing may be needed – one type of test may not address every control. These methods include;
    - **Inquiry:** Inquiry involves asking control owners about a specific control and having them explain the control process. However, an inquiry is not considered conclusive evidence on its own to determine the effectiveness of the control, and it should be combined with other testing procedures and evidence to garner a conclusion.
    - **Observation:**
        - During observation, watch the actual performance of the control. Observations work well when the team wants to observe a live, real-time application control, such as a system generating a “not authorized” type of error message when an employee tries to access a part of an application in which the system is designed to restrict such access.
        - In this case, the team performing the gap assessment would ask an employee/control owner to demonstrate an attempt to gain unauthorized access and observe the application denying the unauthorized access.

- Obtain screenshots throughout the observation steps to have evidence of the test for the control testing work papers. Observation is also useful to validate the control design regarding manual procedures to understand whether the written process documentation is what is being performed.

- **Documentation Examination:** Documentation examination requires understanding the entire population of transactions or activities that would necessitate the performance of a control. An examination may be performed to test for the control's design adequacy and operating effectiveness. Testing shall include examining the supporting documentation generated by the performance of the control and the procedures necessary to verify that the IT system reports or other manually generated data used during the performance of the control were complete and accurate.
- **Re-performance:** Re-performance often is used for controls that may be manual and are performed on an infrequent basis. Re-perform the control steps in order to obtain the same testing results. Evidence obtained might include the original process documentation with notations on the results of procedures re-performed or a separate set of re-performance documentation/working papers with a comparison to the original control documentation.
- **Timing of testing:** The timing of control testing often is determined by the risk of control failure and the severity of the possible control deficiency. Earlier testing, when appropriate, may decrease the duration of negative consequences (such as an increased likelihood of theft or fraud) resulting from the control deficiency.
- **Extent of testing:** The extent of testing depends on many factors, including the importance of the process to the organization, the volume of transactions per period, the complexity of the control procedures, and the consequences of a control failure in Dirhams at risk or another relevant measurement such as reputational harm. Testing can be either statistically, not statistically, or judgmentally determined depending on the purpose of the testing and who may be relying on the results (e.g., external auditors, ADAA).

4.3.2.3.2. Perform test of controls, Remediation Planning and Reporting

- As the tests are being performed, it is important to keep management/process owners updated concerning the progress of the testing and any issues or complications encountered. Management/process owners may be able to assist in finding solutions to issues and complications, which may help in meeting testing deadlines.
- For any controls that fail testing, the gap assessment team should work with the process and control owners to determine a remediation plan, including timing, to address the failure.

4.3.2.3.3. Remediation Planning

- Upon concluding with the gap assessment and the deficiencies have been identified and rated, the concerned departments can begin designing remediation plans and associated actions to implement the plans.
- Remediation plans should consider the severity of each identified deficiencies by prioritizing the remediation of more severe deficiencies ahead of those less severe ones.

- Remediation plans generally include the following characteristics depending on the severity of the deficiency being remediated and the complexity of the remediation action:
  - Indication of the related cycle, control number, and control description of the deficiency to be remediated (with the caveat that the control number and wording may not be available if no control currently exists)
  - Description of the deficiency including affected IT system.
  - Notation of the responsible control owner or process owner.
  - Description of the remediation plan, including, at a minimum, the remediation action to be performed, the person(s) responsible for the remediation action, and the estimated completion date for the remediation action.
  - Significant milestones or follow-up dates to monitor the remediation plan and its progress.
  - Highly complex remediation plans may require elevated management attention to ensure successful implementation. Complex remediation plans may involve multiple processes and personnel, affect multiple IT systems, or require action by third-party service providers.

4.3.2.3.4. Remediation Implementation

- Remediation plans may require significant time commitments from process owners or changes to current business processes. So, before beginning the remediation implementation process, it is important to confirm plans with and establish buy-in from those who will be involved.
- Successful and sustainable remediation efforts depend on input and commitment from process owners. Additionally, process owners will be able to assist in evaluating the effectiveness of the proposed remediation actions and provide valuable insights into the remediation process, including the reasonableness of objectives, proposed milestones, and the timing of project completion. Once process owners provide input and confirm support, the remediation plans should be updated and verified.
- It is important to ensure the updated remediation plans remain focused on addressing the control deficiencies noted in the gap assessment phase and that the focus has not shifted to processes not identified as deficient or to processes with lower-rated deficiencies.
- Ongoing attention is needed to address control deficiencies as planned.

4.3.3. Step 3: Reporting

3 **Management Reporting**

- Document the gap assessments with control rating (for design & operations – ELC. PLC & ITGC) for all the identified risks with the RCM, within a gap assessment report.
- This report must capture the agreed remediation plan, implementation date and implementation ownership/responsibility.
- The reports must be distributed to the Finance Department, President, and the Audit Committee.

- The results of control testing shall be communicated to management in a written format within the gap assessment report. The format and content of the report shall include:

- Methodology used for conducting the gap assessment.
- Project overview and scope (including materiality threshold and significant accounts).
- Summary of findings.
- Description of the process and controls to tested, including a description of the risks to be mitigated by the identified controls.
- Description of risks, controls, and reason for conclusion.
- Rating of control deficiencies to assist in prioritizing remediation actions and plans.
- Summary of management remediation plans, personnel responsible for remediation, and deadlines.
- Appendices.

4.3.4. Step 4: Monitoring & Follow-up

4 **Monitoring & Follow-up**

- Continuously monitor and update the RCMs.
- Improve the effectiveness of internal control.
- Keep a tab on continuous improvements needed in the framework, processes, leading practices and changes in laws and regulations.
- Conduct quarterly follow-ups and annual gap assessments

4.3.4.1. Continuous monitoring

- To assess the adequacy and effectiveness of internal controls, a continuous monitoring process may provide stronger support than scheduled monitoring that may occur on a periodic basis. Continuous monitoring usually involves the automated testing of all transactions and system activities within a given business process area versus testing based on sampling criteria so that continuous monitoring can offer a more comprehensive view of portions of the status of the control environment. Continuous monitoring includes the following;
    - Purpose: consider the business objective and critical success factors.
    - Risk: determine likely obstacles that would inhibit the organization's success.
    - Response: align diverse sources of data to discover and corroborate emerging risks such as configurable conditions, changes, event logging, financial transactions, and unstructured data.
    - Timing: detect control issues in real time.
    - Action: track deficiencies for corrective action.
- Results of continuous monitoring should be made available to management as soon as practicable. Appropriate results also should be shared with the management.

4.3.4.2. Follow-up

- It is preferable to wait on initiating Phase 4 until after the remediation plans in Phase 3 are tracked to completion so that the new controls created during the remediation work can be included in the initial testing of all selected controls.

- However, if the remediation plans are delayed or will take a long time to implement (e.g., more than three months), management should consider initiating testing of all other selected controls without waiting for the completion of the remediation work.
- While controls related to remediation eventually will need to be tested after those plans are completed, these controls generally would not be expected to be a large percentage of the total controls tested.
- Furthermore, any controls that were already existing (in other words, not related to remediation plans) will need to go through separate, additional remediation plans if they fail during testing, which is the strongest argument for not delaying their testing in order to wait for the completion of lengthy remediation plans from Phase 3.
- The Internal Control Team shall conduct quarterly follow-ups to check if the suggested and agreed remediation plans have been implemented and, if not investigate and validate the reason for the delay.
- Annually, GAP assessment must be conducted to ensure continuous design adequacy and operating effectiveness of ongoing processes/controls or new processes. The prior year’s RCMs must be reviewed annually to re-test the processes as well as test new processes/controls.

End of the Document