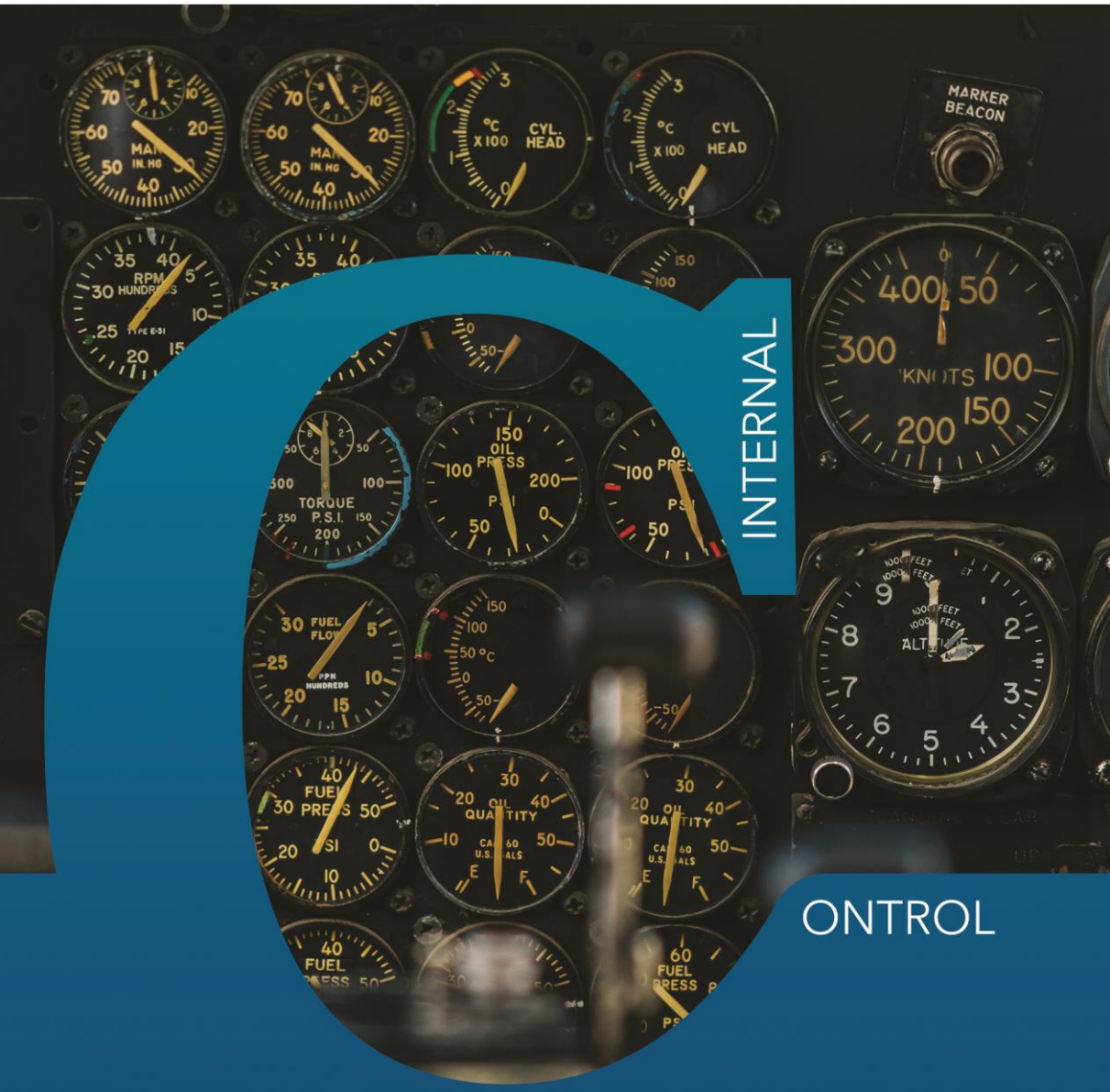
PEMPAL

IACOP Internal Audit Community of Practice



INTERNAL CONTROL

Assessing the Effectiveness of Internal Control: PEMPAL Guidance for Public Sector Internal Auditors

October 2020

Internal Audit Community of Practice (IACOP)
T: +7 495 745 70 00 ext. 2002
E: IACOP@pempal.org
W: www.pempal.org

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

This guidance was developed by the Internal Control Working Group of the Public Expenditure Management Peer Assisted Learning (PEMPAL) Internal Audit Community of Practice (IACOP). The IACOP would like to thank all those who contributed including all members of the IACOP Internal Control Working Group, and recognize, in particular, the following key contributors: Richard Maggs, World Bank consultant; Edit Nemeth (Hungary), former IACOP Executive Committee (ExCom) Chair and former Lead of Internal Control Working Group; and Arman Vatyan, World Bank, PEMPAL Program Leader.

WHAT ARE PEMPAL AND IACOP?

PEMPAL is a network to facilitate exchange of professional experience and knowledge transfer among public financial management practitioners in countries across the Europe and Central Asia Region. The network, launched in 2006, aims to contribute to strengthening public financial management practices in member countries through developing and disseminating information on good practices and their application.

PEMPAL organizes around three thematic communities of practice:

- Budget Community of Practice,
- Treasury Community of Practice, and
- Internal Audit Community of Practice (IACOP).

The main overall objective of the IACOP is to support its member countries in establishing modern and effective internal audit systems that meet international standards and good practices; important for good governance and accountability in the public sector.

The key donors and development partners to the program are the Swiss State Secretariat for Economic Affairs, the Ministry of Finance of the Russian Federation, and the World Bank. The Dutch National Academy for Finance and Economics provides non-financial support.

PREFACE

“Assessing the Effectiveness of Internal Control: PEMPAL Guidance for Public Sector Internal Auditors” is a knowledge product developed by the IACOP for internal auditors, to assist with understanding and assessing the effectiveness of internal control.

Other IACOP good practice knowledge products include: Good Practice Internal Audit Manual Template; Good Practice Continuing Professional Development Manual Template; Internal Audit Body of Knowledge; Risk Assessment in Audit Planning; Quality Assessment Guide; PEMPAL Guidance on Internal Audit: Demonstrating and Measuring Added Value; PEMPAL Glossary of Terms: Internal Control; The Impact of COVID-19 on the Role and Activities of Internal Audit; and Key Performance Indicators For Internal Audit Functions. All are available from **www.pempal.org.**

ACRONYMS

COBIT	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
IACOP	Internal Audit Community of Practice
IIA	Institute of Internal Auditors
IT	Information Technology
KPI	Key Performance Indicator
PFM	Public Financial Management
PEMPAL	Public Expenditure Management Peer Assisted Learning network
PIC	Public Sector Internal Control
SAI	Supreme Audit Institution

PART 1. INTRODUCTION

This guidance has been developed to help internal auditors better understand the main features of effective internal control and how to assess and evaluate the functionality of internal control systems. It includes a series of criteria for assessing the maturity of internal controls. These may be useful for internal auditors working in organizations that are in the process of developing/refining public financial management (PFM) systems. The guidance:

- Outlines the main features of internal control as promoted by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[1] (Part 2 and Annex A).
- Explains the five components of internal control and the 17 underlying principles of internal control that need to be met for internal control to be effective, tailored to the public sector context (Part 3 and Annexes B1-B5).
- Identifies criteria for assessing the extent to which each of the principles has been met (Annexes B1-B5).
- Promotes a model for a four-level assessment of the maturity of internal control (Part 4).
- Presents a detailed framework for assessing the maturity of internal controls at the four levels, drawing on PEMPAL assessment criteria (Annex C).

This guidance will be used by the IACOP and may be further updated to reflect views expressed and knowledge developed at future meetings of the Internal Control Working Group.

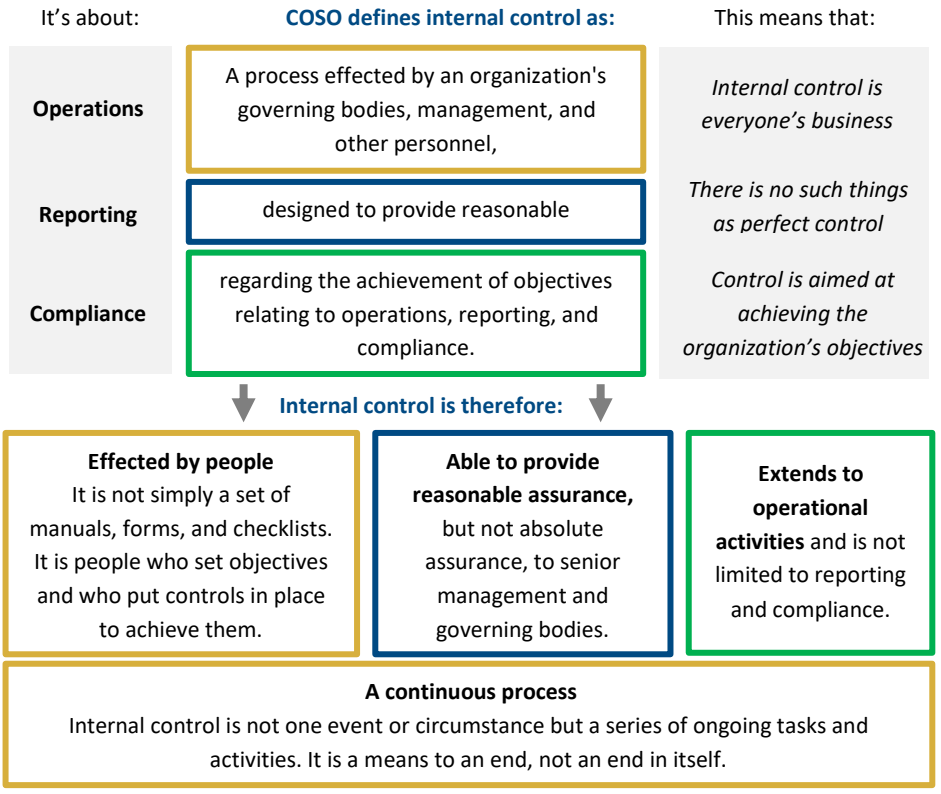
[1] COSO is a global initiative to develop frameworks and guidance on enterprise risk management, internal control, and fraud deterrence. https://www.coso.org/Pages/default.aspx

PART 2. WHAT IS INTERNAL CONTROL?

The definition of internal control

COSO defines internal control as "*A process, effected by an organization's governing bodies,*[2] *management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.*"[3] Figure 1 illustrates how this definition can be interpreted for use in PEMPAL countries.

Figure 1. The definition of internal control explored

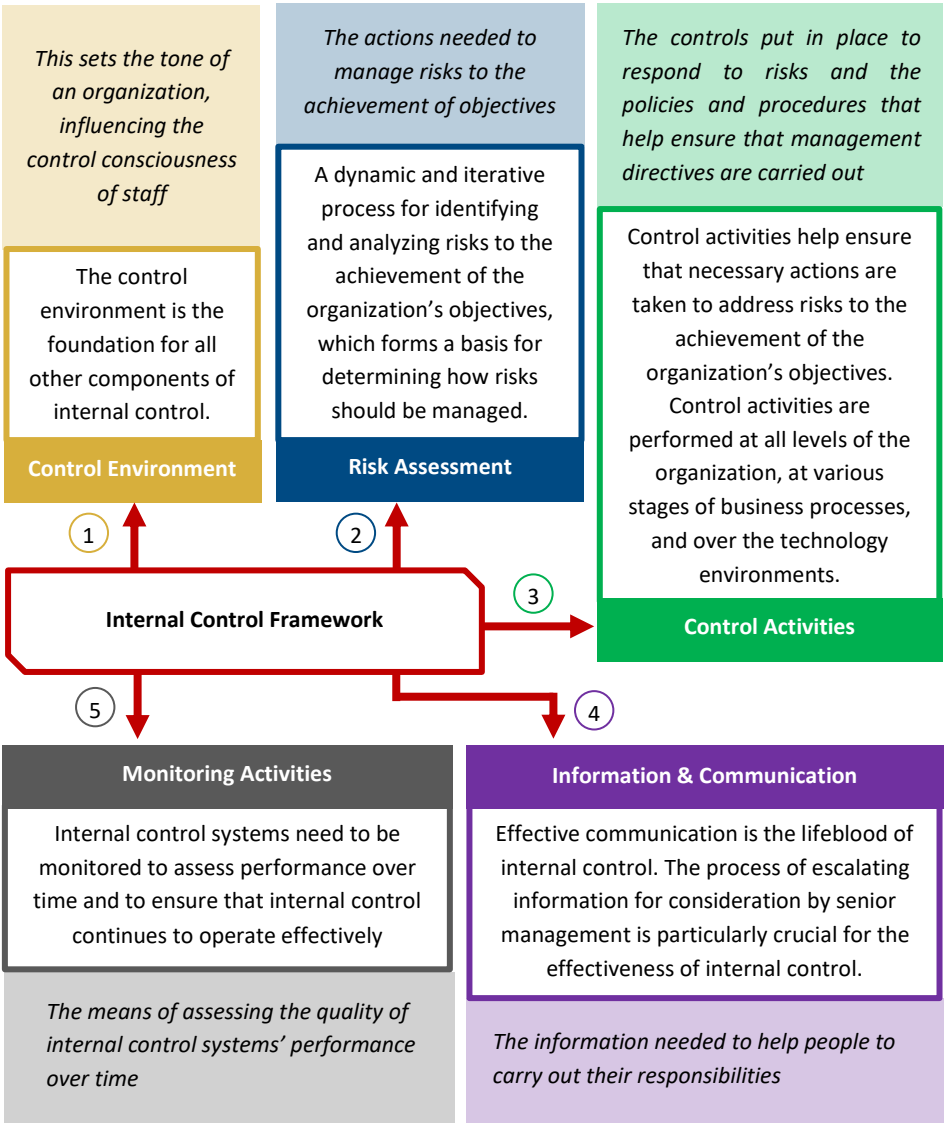


[2] The word "board" as used in COSO can be translated in the public sector as the entity or entities that are responsible for providing governance and oversight of the public sector organization concerned or governing bodies. In some countries (for example, the United Kingdom) this governance role is filled by a board of independent directors.
[3] COSO. "Internal Control - Integrated Framework", 2013

The main components of internal control

COSO recognizes five inter-related components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring activities. These five components, shown in Figure 2 below, all need to be in place and integrated to be effective across operational, reporting, and compliance objectives.

Figure 2. The five components of internal control



Internal control is not a process in which one component affects only the next component. It is a multidirectional process in which almost any component can and will influence another.

COSO has developed 17 principles (listed and described in Annex A) that must be present and functioning to meet the five components of internal control. The components and related principles are discussed further in part 3 and explained in detail in Annexes B1-B5.

Limitations of internal control: The concept of reasonable assurance

Internal control is a process of providing reasonable assurance on the achievement of objectives.

Internal control helps an organization achieve its strategic objectives, produce reliable financial and performance information, and comply with relevant regulations. However, internal control cannot change a poor manager into a good one, nor can it influence external factors or severe operational constraints that may significantly impact the organization's operations, for example, the COVID-19 pandemic.

Inherent limitations of internal control may include faulty human judgment in decision-making; simple human error and mistakes; and the need to balance the cost of controls against the risks and benefits involved. Internal controls may also provide limited protection in certain situations relating to fraudulent actions, such as collusion between two or more individuals.

The aim of internal control is to provide reasonable assurance that the organization will achieve its objectives. It would neither be desirable nor possible for internal control systems to provide absolute assurance that an organization will achieve all of its objectives.

Internal controls need to be "present and functioning" and "operating together"

COSO clarify the requirements for effective internal control: that each of the 5 components and 17 relevant principles must be **present and functioning** and the 5 components **must operate togethe**r.

The phrase "present and functioning" applies to both components and principles.

- "Present" refers to the determination that components and relevant principles exist in the design and implementation of the system of internal control to achieve specified objectives.
- "Functioning" refers to the determination that components and relevant principles continue to exist in the conduct of the system of internal control to achieve specified objectives.

"Operating together" refers to the determination that all five components collectively reduce, to an acceptable level, the risk of not achieving an objective.

Providing assurance on the effectiveness of internal control using the three lines model

There is no single or straightforward way to assess the effectiveness of an organization's system of internal control. Internal control needs to be present and functioning at every level of the organization and across all business processes. Everyone working in the organization implements internal controls in some way or another. Moreover, internal control must be continuously reviewed.

Many organizations use the three lines model[4] (Figure 3), which identifies the

[4] Based on the Institute of Internal Auditors (IIA) paper THE THREE LINES MODEL – An update of the Three Lines of Defense, July 2020

various roles of the governing body, senior and operational management, risk and compliance functions, and internal auditing to ensure that internal controls are present and functioning.

Figure 3. The three lines model

Under this model:

- Operational management provides the first line of defense through implementation of internal controls in their everyday work;
- The management functions that oversee risk, control, and compliance provide the second line of defense; and
- Independent functions, specifically internal audit, provide the third line of defense.

PART 3. APPLYING INTERNAL CONTROL IN PEMPAL COUNTRIES

This guidance aims to support public sector internal auditors in PEMPAL countries to implement effective systems of internal control using the framework developed by COSO. This section outlines how to use the detailed material contained in the annexes to achieve this. Each country will need to ensure the system they develop is consistent with its legal framework.

Understanding internal control: The points of focus

To better explain the principles within the five components, COSO has identified explanatory details on each known as "points of focus" in COSO guidance.

Annex A sets out each of the 17 principles and the related points of focus.

Understanding internal control: Interpreting the principles

To help internal auditors interpret and apply the five components and 17 principles of internal control, **Annexes B1 to B5** provide for each component:

a. A diagram for each principle illustrating how the points of focus might be interpreted.

b. A short commentary on the purpose and main features of each principle.

c. A set of criteria for assessing internal control effectiveness developed by the IACOP Internal Control Working Group.

Applying COSO principles in the public sector in PEMPAL countries

One important issue to be considered when applying COSO principles to the public sector in PEMPAL countries is the need to match the legal framework in operation.

In anglophone countries, the legal system allows for the simple adoption of a set of COSO principles through enabling legislation that permits managers to follow the guidance issued by COSO. However, in many PEMPAL countries the legal system requires that public sector staff are given very specific legal mandates.

Consequently, it may be necessary to frame COSO principles and advice as some form of standard or internal regulation so that they are consistent with the legal framework in each country. For example:

- **In Moldova** these have been framed as a set of internal control standards which have legal force through their issuance in the public Gazette.
- **In Georgia**, all five COSO components are identified in the "Law on State Internal Financial Control", which obliges the heads of state organizations to ensure the development, formation, and operation of financial management and control components. There is additionally an instruction on the implementation of the requirements of this law, which also refers to COSO 2013.

PART 4. INTERNAL CONTROL MATURITY MODEL

The public administrations in PEMPAL member countries are at different levels of maturity. For this reason, IACOP decided to develop a generic model for assessing the maturity (or capability) of internal control. After researching a range of maturity models developed for different elements of organizational growth, IACOP decided on a four-level model to avoid a bias towards selecting the mid-point of the scale. The characteristics of the four levels are shown in Table 1 below.

Table 1. A four-level model for assessing the maturity of internal control[5]

Level	Characteristics
Level 1: Informal *Ad-hoc /Chaotic*	The characteristics of internal controls at this level are that they are (typically) undocumented and in a state of dynamic change. They are driven in an *ad hoc*, uncontrolled, and reactive manner by users to events. This provides a chaotic or unstable environment for internal control.
Level 2: Defined *Standard / Repeatable*	The characteristics at this level of maturity are that some internal controls are in place and are repeatable, possibly with consistent results. Internal control discipline is unlikely to be rigorous, but where it exists it may help to ensure that internal controls are maintained during times of stress. Over time, sets of defined and documented standard control processes will be established and subject to improvement. **This could be a lengthy *developmental stage* and is the level where most organizations will probably sit.**

[5] Based on a thought leadership article by Weaver & Tidwell LLP on Determining Maturity Levels for Internal Control, September 16, 2015.

Level	Characteristics
Level 3: Managed & Monitored *Predictable*	At this level of maturity, the majority of internal controls are repeatable and generate consistent results. Internal control discipline is rigorous and ensures that internal controls are maintained in times of stress. Designed and documented standard processes exist and the focus is on continually improving internal control performance through both incremental and innovative changes and improvements.
Level 4: Optimized *Efficient / Effective*	The characteristics of internal control at this level are that the effectiveness of internal control is measured and benchmarked against best practice to ensure strong performance across different situations.

Annex C presents a detailed framework for assessing the maturity of internal controls at the four maturity levels identified above. It does this by drawing on the criteria developed by PEMPAL for each principle and point of focus as presented in Annexes B1-B5.

While in theory it would be possible to assign a numerical score (1-4) to each point of focus to obtain an overall maturity level score, this would only be relevant if each point of focus was equally important. This is not the case. Assessments of maturity therefore depend on judgments of the relative importance of each point of focus.

ANNEX A. INTERNAL CONTROL PRINCIPLES AND POINTS OF FOCUS

COSO has provided guidance for each of the 17 principles including supporting details which it calls "points of focus". This annex outlines the 17 principles together with the points of focus that may be relevant in understanding the application of each principle in the public sector.

Control Environment

1. **The organization demonstrates a commitment to integrity and ethical values.**

   1.1. **Sets the tone at the top.** Governing bodies and management at all levels demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control. There is consistency of messaging on ethics and integrity between the political and operational levels within the public sector.

   1.2. **Establishes standards of conduct.** The expectation of the governing bodies and senior management concerning integrity and ethical values are defined in the organization's standards of conduct and understood at all levels of the organization and by outsourced service providers and business partners.

   1.3. **Checks adherence to standards of conduct.** Processes are in place to evaluate the performance of individuals and teams against the organization's expected standards of conduct.

   1.4. **Addresses deviations promptly.** Deviations from the organization's expected standards of conduct are identified and remedied in a timely and consistent manner

2. **The board demonstrates independence from management and exercises oversight of the development and performance of internal control.**

   2.1. Establishes oversight responsibilities. The governing bodies identify and accept their oversight responsibilities in relation to established requirements and expectations.

   2.2. Has access to relevant skills. The governing bodies define, maintain, and periodically evaluate the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate actions.

   2.3. Operates independently. The governing bodies have sufficient members who are independent from management and objective in evaluations and decision-making.

   2.4. Provides oversight of the system of internal control. The governing bodies retain oversight responsibility for management's design, implementation, and conduct of internal control.

   For example: **Control environment**: establishing integrity and ethical values, oversight structures, authority, and responsibilities, expectations of competence, and accountability to the board. **Risk assessment**: overseeing management's assessment of risks to the achievement of objectives, including the potential impact of significant changes, fraud, and management override of internal control. **Control activities**: providing oversight to senior management in the development and performance of control activities. **Information and communication**: analyzing and discussing information relating to the achievement of the organization's objectives. **Monitoring activities**: assessing and overseeing the nature and scope of monitoring activities and management evaluation and remediation of deficiencies.

3. **Management, with board oversight, establishes structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**

   3.1. Considers all structures of the organization. Management and the governing bodies consider the multiple structures used (including

operating units, geographic distribution, and outsourced service providers) to support the achievement of objectives.

3.2. Establishes reporting lines. Management designs and evaluates lines of reporting for each organizational structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the organization.

3.3. Defines, assigns, and limits authorities and responsibilities. Management and the governing bodies delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization:

- **Governing bodies** – retain authority over significant decisions and review management assignments and limitations of authorities and responsibilities;
- **Senior management** – establishes directives, guidance, and control to enable management and other personnel to understand and carry out their internal control responsibilities;
- **Management** – guides and facilitates the execution of senior management directives within the organization and its subunits;
- **Personnel** - understand the organization's standards of conduct, assessed risks to objectives, and the related control activities at their respective levels of the organization, the expected information and communication flow, and monitoring activities relevant to their achievement of objectives;
- **Outsourced service providers** – Adhere to management's definition of the scope of authority and responsibility for all non-employees engaged by the organization

4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

4.1. Establishes policies and procedures. Policies and procedures reflect expectations of competence necessary to support the achievement of objectives.

4.2. **Evaluates competence and addresses shortcomings.** The governing bodies and management evaluate competences across the organization and in outsourced services providers in relation to established policies and practices, and act as necessary to address shortcomings.

4.3. **Attracts, develops, and retains individuals.** The organization provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced services providers to support the achievement of objectives.

4.4. **Plans and prepares for succession.** Senior management and the governing bodies develop contingency plans for assignment of responsibilities important for internal control.

5. **The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**

5.1. **Enforces accountability through structures, authorities, and responsibilities.** Management and the governing bodies establish mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the organization and implement corrective actions as necessary.

5.2. **Establishes performance measures, incentives, and rewards.** Management and the governing bodies establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the organization, reflecting appropriate dimensions of performance and expected standards of conduct and considering the achievement of both short-term and long-term objectives.

5.3. **Evaluates performance measures, incentives, and rewards for ongoing relevance.** Management and the governing bodies align incentives and rewards with the fulfilment of internal control responsibilities, develop performance measures, and evaluate performance.

5.4. **Considers excessive pressures.** Management and the governing bodies evaluate and adjust pressures associated with the

achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.

5.5. Evaluates performance and rewards or disciplines individuals. Managers and the governing bodies evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence and provide rewards or exercise disciplinary action as appropriate.

Risk Assessment

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

6.1. Operations objectives

- **Reflects management's choices:** operations objectives reflect management's choices about structure and performance of the organization.
- **Considers tolerances for risk:** management considers the acceptable levels of variation relative to the achievement of operations objectives.
- **Includes operations and financial performance goals:** the organization reflects the desired level of operations and financial performance for the organization within operations objectives.
- **Forms a basis for committing resources:** management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.

6.2. External reporting objectives

- **Complies with applicable accounting standards:** financial reporting objectives are consistent with accounting principles suitable and available for the organization. The accounting principles selected are appropriate in the circumstances.
- **Considers materiality:** management considers materiality in financial statement presentation.

- **Reflects the organization's activities:** external reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.

6.3. Internal reporting objectives

- **Reflect management's choices:** internal reporting provides management with accurate and complete information regarding management choices and information needed in managing the organization.
- **Consider the required level of precision:** management reflects the required level of precision and accuracy suitable for user needs in non-financial reporting objectives and materiality within financial reporting objectives.
- **Reflect the organization's activities:** internal reporting reflects the underlying transactions and events within a range of acceptable limits.

6.4. Compliance objectives

- **Reflect external laws and regulations:** laws and regulations establish minimum standards of conduct which the organization integrates into compliance objectives.
- **Consider tolerance for risk:** management considers the acceptable levels of variation relative to the achievement of compliance objectives.

7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

7.1. Includes organization and main structures. The organization identifies and assesses risks at the organization, region, and division levels relevant to the achievement of objectives.

7.2. Analyzes internal and external factors. Risk identification considers both internal and external factors and their impact on the achievement of objectives.

7.3. Involves appropriate levels of management. The organization puts into place effective risk assessment mechanisms that involve appropriate levels of management.

7.4. Estimates significance of risks identified. Identified risks are analyzed through a process that includes estimating the potential significance of the risk.

7.5. Determines how to respond to risks. Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.

8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.

8.1. Considers various types of fraud. The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.

8.2. Assesses incentive and pressures. The assessment of fraud risk considers incentives and pressures.

8.3. Assesses opportunities. The assessment of fraud risk considers opportunities for unauthorized acquisition, use or disposal of assets, altering of the organization's reporting records, or committing other inappropriate acts.

8.4. Assesses attitudes and rationalizations. The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.

9. The organization identifies and assesses changes that could significantly impact the system of internal control.

9.1. Assesses changes in the external environment. The risk identification process considers changes to the regulatory, economic, and physical environment in which the organization operates.

9.2. Assesses changes in the business model. The organization considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, and acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.

9.3. Assesses changes in leadership. The organization considers changes in management and respective attitudes in philosophies on the system of internal control.

Control Activities

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

10.1. Integrates with risk assessment. Control activities help ensure that risk responses that address and mitigate risks are carried out.

10.2. Considers organization-specific factors. Management considers how the environment, complexity, nature, and scope of its operations, as well as specific characteristics of the organization, affect selection and development of control activities.

10.3. Determines relevant business processes. Management determines which relevant business processes require control activities.

10.4. Evaluates a mix of control activity types. Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls and preventive and detective controls.

10.5. Considers at what level activities are applied. Management considers control activities at various levels in the organization.

10.6. Addresses segregation of duties. Management segregates incompatible duties, and where such segregation is not practical management selects and develops alternative control activities

11. The organization selects and develops general control activities over technology to support the achievement of objectives.

11.1. Determines dependency between the use of technology in business processes and technology general controls. Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.

11.2. **Establishes relevant technology infrastructure control activities.** Management selects and develops control activities over technology infrastructure, which are designed and implemented to ensure completeness, accuracy, and availability of technology processing.

11.3. **Establishes relevant security management process control activities.** Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the organization's assets from external threats.

11.4. **Establishes relevant technology acquisition, development, and maintenance process control activities.** Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.

12. **The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.**

12.1. **Establishes policies and procedures to support deployment of management's directives.** Management establishes control activities that are built into business procedures and employees' day-to-day activities through policies.

12.2. **Establishes responsibility and accountability for executing policies and procedures.** Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.

12.3. **Performs in a timely manner.** Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.

12.4. **Takes corrective action.** Responsible personnel investigate and act on matters identified as result of executing control activities.

12.5. **Performs using competent personnel.** Competent personnel with sufficient authority perform control activities with diligence and continuing focus.

12.6. **Reassesses policies and procedures.** Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.

Information and Communication

13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

13.1. **Identifies information requirements.** A process is in place to identify the information required and expected to support the functioning of other components of internal control and the achievement of the organization's objectives.

13.2. **Captures internal and external sources of data.** Information systems capture internal and external sources of data.

13.3. **Processes relevant data into information.** Information systems process and transform relevant data into information.

13.4. **Maintains quality throughout processing.** Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components.

13.5. **Considers costs and benefits.** The nature, quantity, and precision of information communicated is commensurate with and supports the achievement of objectives.

14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

14.1. **Communicates internal control information.** A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.

14.2. **Communicates with the governing bodies.** Communication exists between management and governing bodies so that both have the

information needed to fulfil their roles with respect to the organization's objectives.

14.3. Provides separate communication lines. Separate communication channels, such as whistleblower hotlines, are in place and serve as a fail-safe mechanism to enable anonymous and confidential communication when normal channels are inoperative or ineffective.

14.4. Selects relevant methods of communication. The method of communication considers the timing, audience, and nature of information.

15. The organization communicates with external parties regarding matters affecting the functioning of internal control.

15.1. Communicates to external parties. Processes are in place to communicate relevant and timely information to external parties, including parliament, partners, regulators, and other external parties.

15.2. Enables inbound communications. Open communication channels allow input from beneficiaries or clients, suppliers, external auditors, regulators, and others, providing management and governing bodies with relevant information.

15.3. Communicates with governing bodies. Relevant information resulting from assessments conducted by external parties is communicated to governing bodies.

15.4. Provides separate communication lines. Separate communication channels, such as whistleblower hot lines, are in place and serve as failsafe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.

15.5. Selects relevant methods of communication. The method of communication considers timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.

Monitoring Activities

16. **The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.**

    16.1. **Considers a mix of ongoing and separate evaluations.** Management includes a balance of ongoing and separate evaluations.

    16.2. **Considers rate of change.** Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.

    16.3. **Establishes baseline understandings.** The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.

    16.4. **Uses knowledgeable personnel.** Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.

    16.5. **Integrates with business processes.** Ongoing evaluations are built into the business process and adjust to changing conditions.

    16.6. **Adjusts scope and frequency.** Management varies the scope and frequency of separate evaluations depending on risk.

    16.7. **Evaluates objectively.** Separate evaluations are performed periodically to provide objective feedback.

17. **The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the governing bodies, as appropriate.**

    17.1. **Assesses results.** Management and the board, as appropriate, assess results of ongoing and separate evaluations.

    17.2. **Communicates deficiencies.** Deficiencies are communicated to parties responsible for taking corrective actions and to senior management and the board as appropriate.

    17.3. **Monitors corrective actions.** Management tracks whether deficiencies are remediated on a timely basis.

ANNEX B1. THE CONTROL ENVIRONMENT

The following annexes should help internal auditors interpret and apply the five components and 17 principles of internal control. Each annex focuses on one of the components, illustrating how the points of focus might be interpreted, outlining the purpose and main features of each principle, and providing a set of criteria for assessing internal control effectiveness.

This annex focuses on Component 1 - **The Control Environment,** which is the foundation of all other components of internal control. The control environment reflects the tone at the top of an organization. It depends in part on the structures established by management but also on the way that people act within the organization in fulfilling their responsibilities. For example, there is a need for policies to explain how people should act in certain situations, but there is also a need for management to demonstrate through their actions that they are following this guidance.

COSO identifies **five principles within this component**, which are listed in the table below.

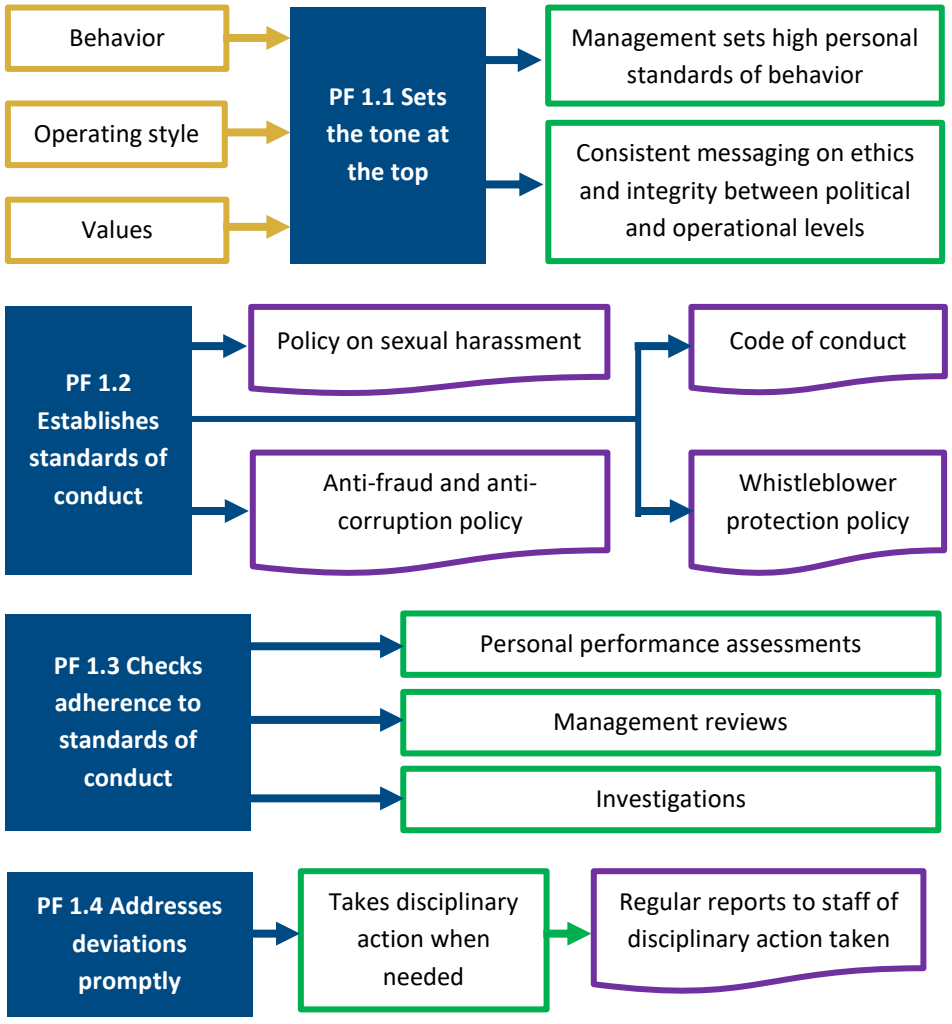
Table 2. The Principles and Points of Focus for Component 1 – The Control Environment

Principle		Points of Focus (PF)
1	The organization demonstrates a commitment to integrity and ethical values.	1.1. Sets the tone at the top.
		1.2. Establishes standards of conduct.
		1.3. Checks adherence to standards of conduct.
		1.4. Addresses deviations promptly.

	Principle	Points of Focus (PF)
2	The board demonstrates independence from management and exercises oversight of the development and performance of internal control.	2.1. Establishes oversight responsibilities.
		2.2. Has access to relevant skills.
		2.3. Operates independently.
		2.4. Provides oversight of the system of internal control.
3	Management, with board oversight, establishes structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	3.1. Considers all structures of the organization.
		3.2. Establishes reporting lines.
		3.3. Defines, assigns, and limits authorities and responsibilities.
4	The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	4.1. Establishes policies and procedures.
		4.2. Evaluates competence and addresses shortcomings.
		4.3. Attracts, develops, and retains individuals.
		4.4. Plans and prepares for succession.
5	The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	5.1. Enforces accountability through structures, authorities, and responsibilities.
		5.2. Establishes performance measures, incentives, and rewards.
		5.3. Evaluates performance measures, incentives, and rewards for ongoing relevance.
		5.4. Considers excessive pressures.
		5.5. Evaluates performance and rewards or disciplines individuals.

Principle 1. The organization demonstrates a commitment to integrity and ethical values

Figure 4. Interpretation of Principle 1



Commentary

It is not possible for people to act with integrity if they are not aware of the ethical standards that they are expected to follow. It is crucial therefore that each organization provides its staff with guidance that explains the standards

expected. This should include provisions to protect individuals that report wrongdoing (known as whistleblowers). Having established clear standards of behavior, it is essential that actual behavior is reviewed and that any deviations are fully investigated with disciplinary action when needed. In the public sector there is also a need for consistent messaging on the importance of ethics and integrity between the political and operational levels. Both politicians and public servants must demonstrate ethics and integrity.

Criteria for assessing internal control effectiveness

Do senior managers "walk the talk", where what they say in terms of the behavior they expect from staff is consistent with the way they act?

Does the organization have one or more policies that define expected standards of behavior for managers and staff, including statements about ethics and values? Do these include:

- Code of Ethics.
- Anti-fraud and corruption policy.
- Policy on sexual harassment and abuse.
- Arrangements for protecting whistleblowers.
- Training in the standards of behavior expected.
- Regular reminders to staff of the need to carry out their duties with integrity in ways that meet the ethical standards established.

Are there processes in place to evaluate the performance of individuals and teams in meeting the ethical standards expected? For example:

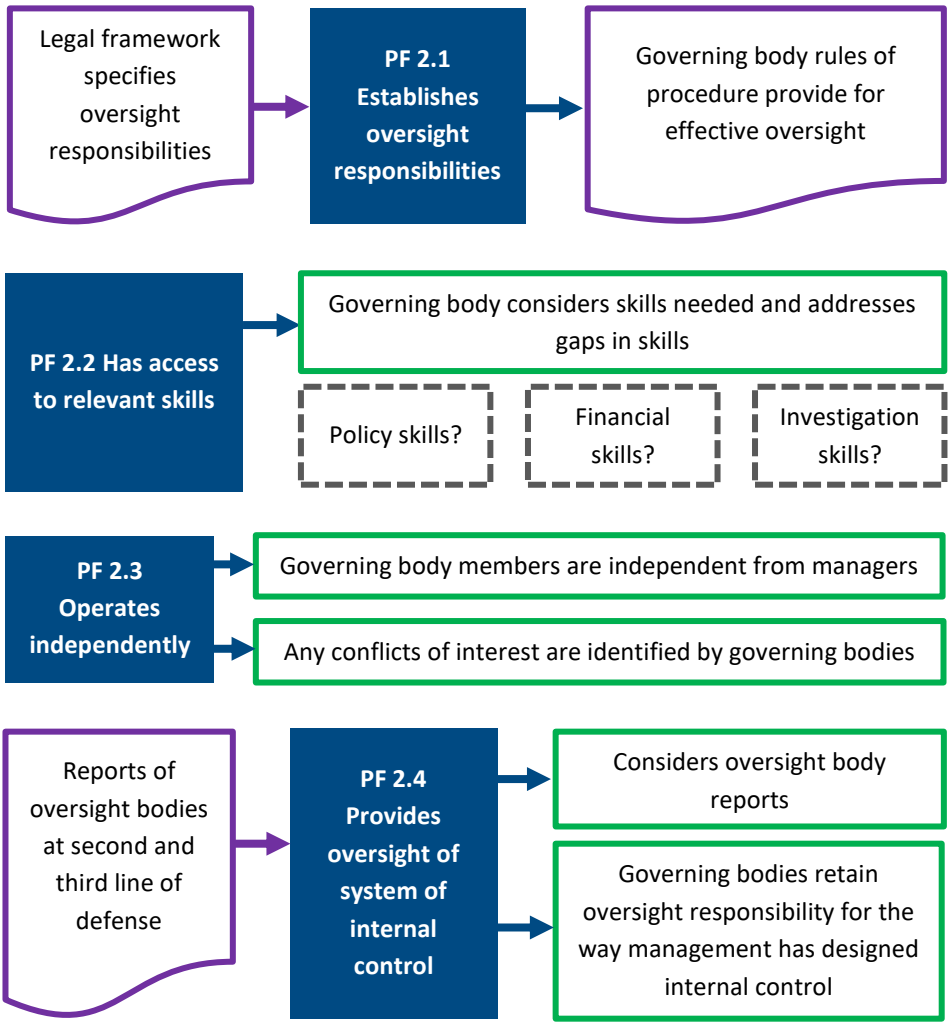
- All staff are required to self-assess and declare on a regular basis whether they have met the standards of behavior expected.
- Conflicts of interest in the public sector are clearly defined, declared, regularly recorded/signed, and monitored.
- Declarations of assets and expenses are made regularly.

Is there a clear process for managing deviations from the standards expected?
For example:

- Data are kept on all deviations from the standards expected.
- Deviations from the standards expected are investigated and action taken to address shortcomings.

Principle 2. Governing bodies demonstrate independence from management and exercise oversight of the development and performance of internal control

Figure 5. Interpretation of Principle 2



Commentary

This principle has been modified from the COSO guidance which refers to a board of directors. The principle applies to public sector organizations even when there is not a board of directors with oversight responsibilities. This is because all public sector organizations should be subject to some degree of oversight from supervisory bodies external to the entity. There are a range of options for oversight in the public sector as noted in Table 3 below.

Table 3. Possible governing bodies in the public sector

Arrangements in the public sector to fulfill the role of governing body as identified during PEMPAL discussions
1. Head of the organization (minister, etc.) - a single person
2. External oversight committee which could take different forms (e.g. parliamentary committee, government committee, committee represented by different ministries)
3. Oversight by line ministry or a superior organization
4. Dual leadership: minister (political leader) plus secretary general (administrative leader)
5. Board of the agency/department represented by the executive only (with those appointed within organization)
6. Audit committees at the agency/department level with non-executive directors/independent members
7. Audit committee centralized for the government
8. Thematic boards: e.g. internal control board led by a secretary general (or deputy)
9. Dedicated unit or person in the Presidential administration (where relevant) with specific oversight responsibilities

In the public sector, oversight arrangements will often be identified in legislation and may be supplemented by rules of procedure for certain governing bodies. Key features of COSO are that governing bodies must operate independently and have the skills to work effectively. It is also essential that governing bodies actually review the operation of internal controls. This can often be done by reviewing the reports generated at the second and third lines.

Criteria for assessing internal control effectiveness

Is there an independent governing body responsible for oversight of management?

If not, what level of independent oversight exists of the actions of management? See Table 3 above for examples of the type of oversight arrangements that may exist in PEMPAL countries.

Are oversight arrangements clearly defined, for example:

- A legal framework which defines the oversight responsibility over internal control.

Does the governing body have the expertise to oversee the work of the organization? For example:

- Necessary skills and relevant experiences are defined and match the objectives of the organization.
- Governing body consists of members with various skills and competencies that are appropriate (education and qualification).
- There is a clear process for appointing or recruiting members of the governing body.
- Governing body has access to independent expertise as necessary.
- Governing body demonstrably supports the independence of internal audit as the third line of defense.

Does the governing body operate independently of management? For example:

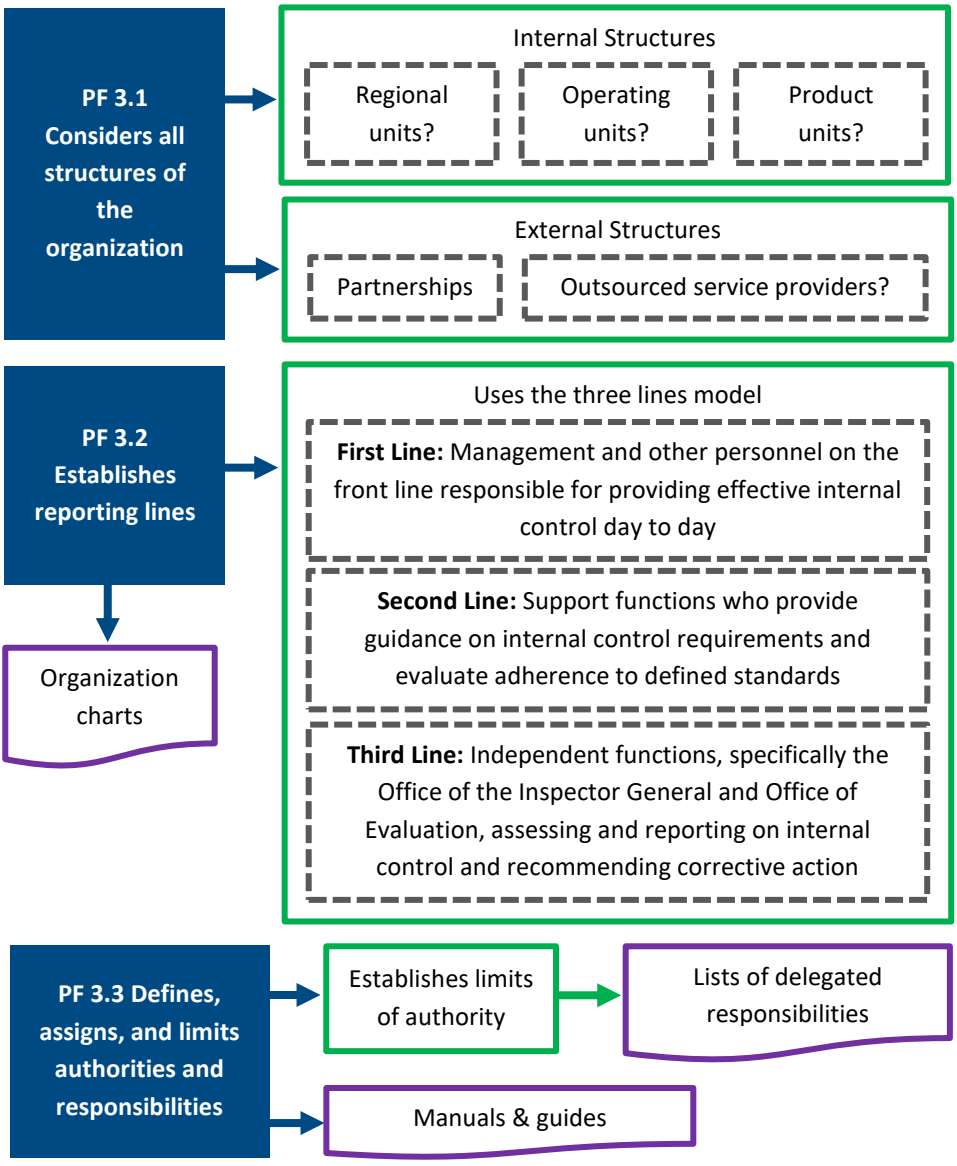
- There is clear separation of the management decision making role from the oversight/advisory role.
- There is a clear mandate for oversight of internal control.
- The information required to exercise oversight is collected on time and reported in an accurate and reliable manner.
- Oversight arrangements have been evaluated for efficiency and effectiveness by the supreme audit institution (SAI).

Does the governing body provide oversight of management's implementation of the system of internal control? For example:

- There is an established system of internal control oversight.
- There are independent criteria for reporting internal control issues to the governing body.
- There is a system established for providing a declaration concerning internal control system status within the organization.
- There is an annual internal audit opinion on the effectiveness of internal control in the organization.
- The audit committee provides a public report on the effectiveness of internal control.

Principle 3. Management, with governing body oversight, establishes structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives

Figure 6. Interpretation of Principle 3



Commentary

The way an organization is structured has a direct impact on the way internal control operates. For example, organizations with separate regional offices will operate differently from those with one central office. The desired structures need to be supplemented with clear reporting lines and these should be reflected in official organization charts. There should be a clear definition of the authority and responsibility of all the individuals in the organization. These should be clearly laid out in manuals and guides. Many organizations also have separate lists of all delegated authorities.

Current best practice is to use the "three lines model" as an internal organizational model. These differentiate between (a) the first line responsibility of managers and personnel for providing effective internal control day to day; (b) the second line support functions who provide guidance on risk, control, and compliance activities and review adherence to such guidance; and (c) independent functions such as internal audit who provide a third line of defense by assessing and reporting on the effectiveness of internal control.

Criteria for assessing internal control effectiveness

Has management established clear internal structures, including as necessary for subsidiary units such as regional offices? For example:

- There is an approved organization structure.
- The established structure is clear and easy to understand.
- Relationships with external partners are clearly defined by management.
- There are contracts in place for outsourced service providers that clearly specify the responsibilities of these providers in relation to internal control.
- Governing bodies regularly review the effectiveness of the organizational structure.

Are the limits of authority clearly defined and communicated to staff? For example:

- There is a clear written statement of the delegated authorities of all staff.

- Staff are provided with manuals or other guidance where the limits of authority are defined.
- Internal audit provide assurance on the clarity of authorities and responsibilities.

Do internal structures result in clear reporting lines? For example:

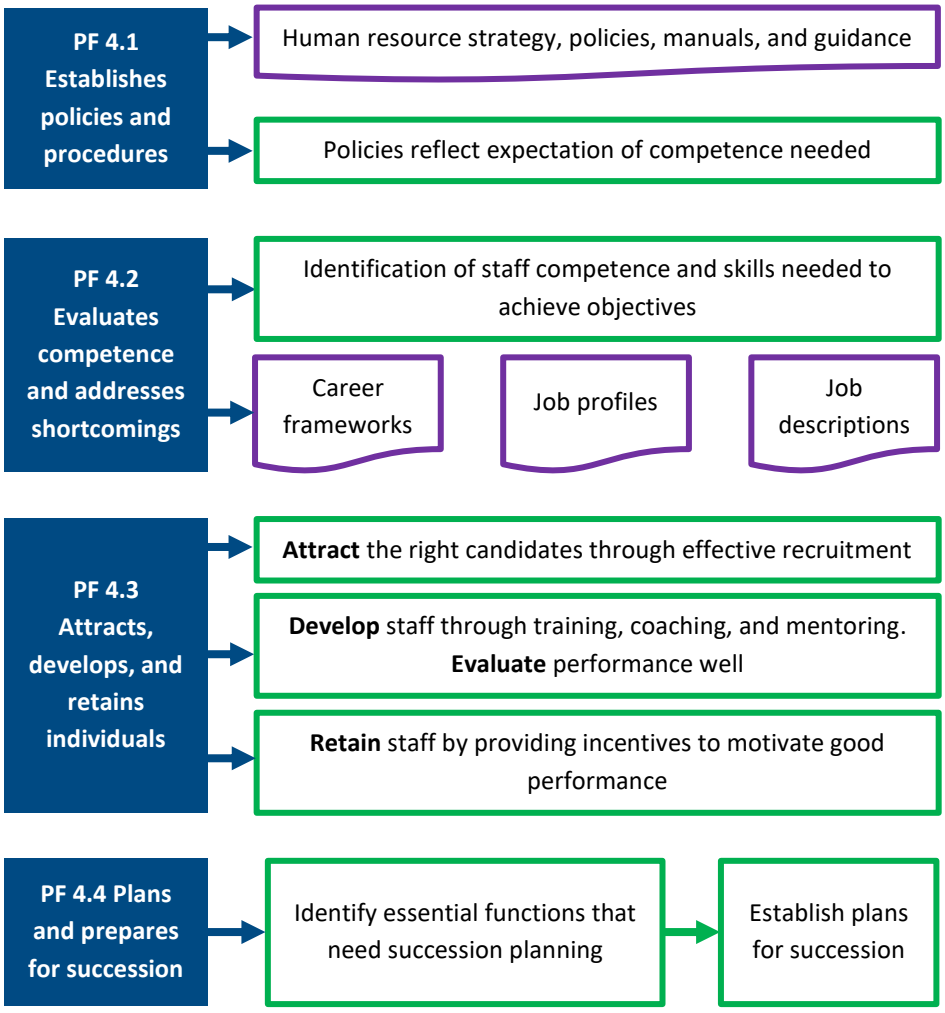
- There are formal organization charts that specify reporting lines.
- Few individuals have dual reporting responsibilities.

Does the organization understand and use the concept of three lines o in maintaining effective internal control? For example:

- There is awareness by all staff of the roles of the first, second, and third lines.
- The results of the third line of defense are usable and actioned.

Principle 4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives

Figure 7. Interpretation of Principle 4



Commentary

You need good people to implement internal controls effectively. This principle examines whether there are the human resource policies that reflect the need

for competent staff, including systems for assessing whether staff perform their duties effectively.

Organizations with a high turnover of staff or who cannot attract and retain staff of the right caliber will have difficulty running effective internal control systems. The principle therefore looks at the ability of the organization to attract, develop, and retain people. It is also important to prepare for the succession of people in important posts.

Criteria for assessing internal control effectiveness

Is there a clear statement of the human resource policies and practices of the organization? For example:

- A human resource strategy document outlines the goals of the human resource policies of the organization.
- Circulars, manuals, and guides clearly identify the competences and skills needed for staff, using as necessary career frameworks, competency statements, job descriptions etc.
- Human resource strategy and policies are periodically reviewed by governing bodies.

Does the organization evaluate the competence of staff and address shortcomings? For example:

- There is a formal performance appraisal system which is applied to all staff.
- The performance of staff is regularly assessed against the standards of competence expected.
- There are formal tests required of the skills of staff in critical functions such as internal audit.

Can the organization attract, develop, and retain staff of sufficient quality to perform its functions? For example:

- There is a mechanism for recruitment with pre-defined and clear rules.
- There are clear qualifications required for all staff at the time of recruitment.

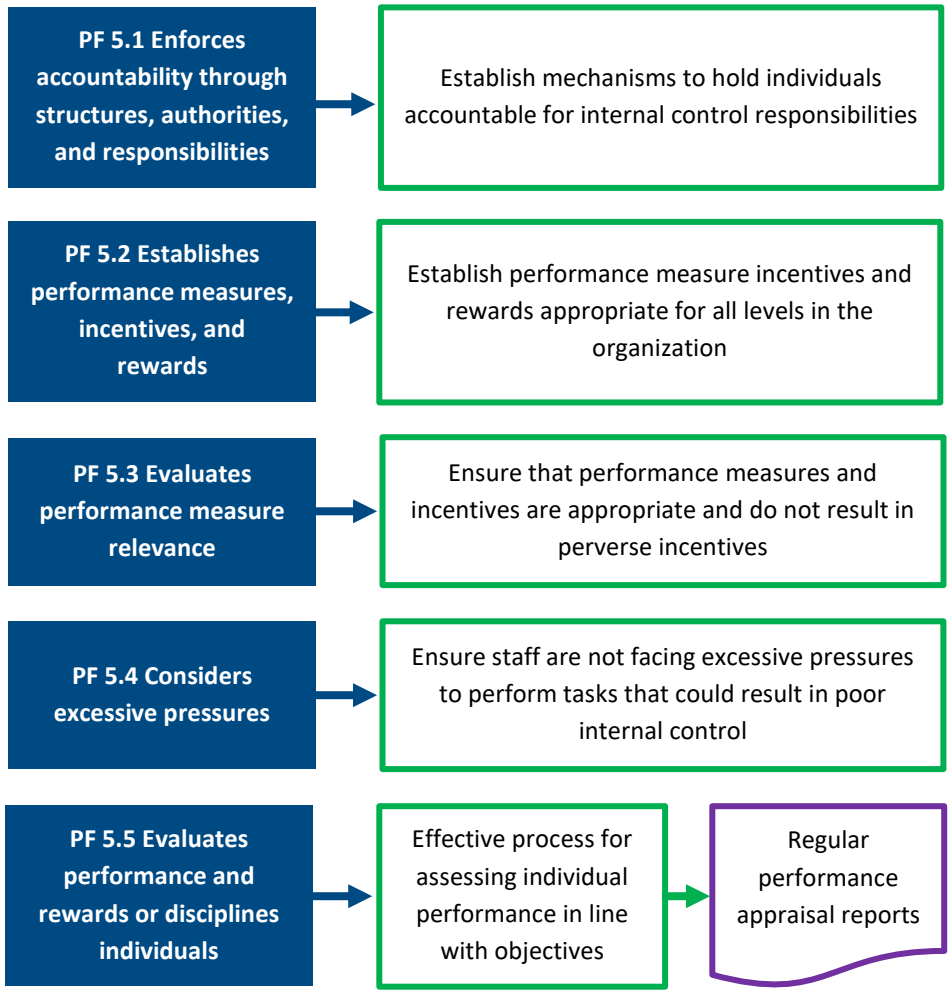
- There is a training plan for the organization as a whole and personal development plans for individuals.
- The organization provides mentoring support to develop staff.
- There is a mechanism to send staff to international seminars, conferences, and workshops such as PEMPAL.
- Promotion requirements within the organization are related to additional skills needed at higher levels of the organization.
- There are mechanisms to reward high levels of staff performance with both financial and non-financial rewards.

Does the organization plan and prepare for succession? For example:

- The organization has identified key posts that should not be left unfilled.
- The organization has identified positions where employee turnover is expected.
- There is a "succession plan" for filling key posts in the organization.
- There is a policy of regular staff rotation to broaden the skills mix available.
- There is a mentoring program to help identify future leaders.

Principle 5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives

Figure 8. Interpretation of Principle 5



Commentary

Internal control will not be effective if there are no processes in place for holding individuals accountable for the implementation of internal control. Accountability is reinforced by an effective performance management system

for individuals which rewards or disciplines individuals. Performance management systems should consider any excessive pressures that may influence the way that people implement their duties.

Criteria for assessing internal control effectiveness

Does the organization enforce accountability through structures, authorities, and responsibilities? For example:

- Responsibilities are identified and allocated to individuals.
- There is a performance evaluation system that operates at different levels of the organization and focuses on how managers manage their region / offices / divisions / units.
- Employees are aware of their responsibilities through job descriptions or other mechanisms.
- Responsibilities meet the internal control and business objectives of the organization.
- Well-understood chains of accountability exist and most staff are held to account for their internal control responsibilities.
- Individual objectives are linked to higher-level objectives in the strategy or management plan.
- All staff are regularly held to account for their internal control responsibilities

Has the organization established performance measures incentives and rewards at all levels of organization? For example:

- There is a policy for setting objectives and key performance indicators (KPIs). At different levels of maturity this may exist at the “entity”, “business unit” and “individual” levels.
- All staff are actively involved in setting their performance objectives and related KPIs.

Does the organization evaluate the relevance of its performance measures?

- The second line of defense is responsible for reviewing the relevance of performance measures.
- The quality and relevance of performance measures is regularly assessed by internal audit.
- Management attest to the relevance of their performance measures.

Does management consider excessive pressures that may impact the way people undertake their duties? For example:

- There is a formalized procedure/mechanism for measuring the workload of staff which identifies situations of overload or underload and mechanisms to address these disparities.
- Management identify staff who are not taking enough time off from their duties.
- Staff suffering from stress-related illnesses are identified and changes made to workloads to reduce such stress.
- There are staff counselling arrangements to identify staff facing undue pressures.

Is there a staff performance management policy that provides for staff to be regularly assessed in terms of achieving their objectives? For example:

- There is a formal performance appraisal system which is applied to all staff.
- The appraisal system results in formal performance reports.
- There is consistency between the level of duties undertaken and the rewards.
- The performance appraisal results in rewarding staff positively and negatively (both financially and non-financial).

ANNEX B2. RISK ASSESSMENT

This annex focuses on Component 2 – Risk Assessment, which allows an organization to consider the extent to which potential events have an impact on the achievement of objectives. Risk assessment seeks to address key questions facing an organization:

- Are managers fully aware of the risks being taken by their staff?
- Are there areas where staff have to take risks that should be considered and supported by senior management?
- What is the limit of risk that the organization and its staff should be subjected to?
- Is the organization accepting risks that could and should be shared with others?
- Is the organization putting in place controls that have little impact on the risks it faces?
- Can some risks simply be accepted rather than controlled?
- Are risks recorded in risk registers and are they kept up to date?

COSO identifies **four principles within this component**, which are listed in the table below.

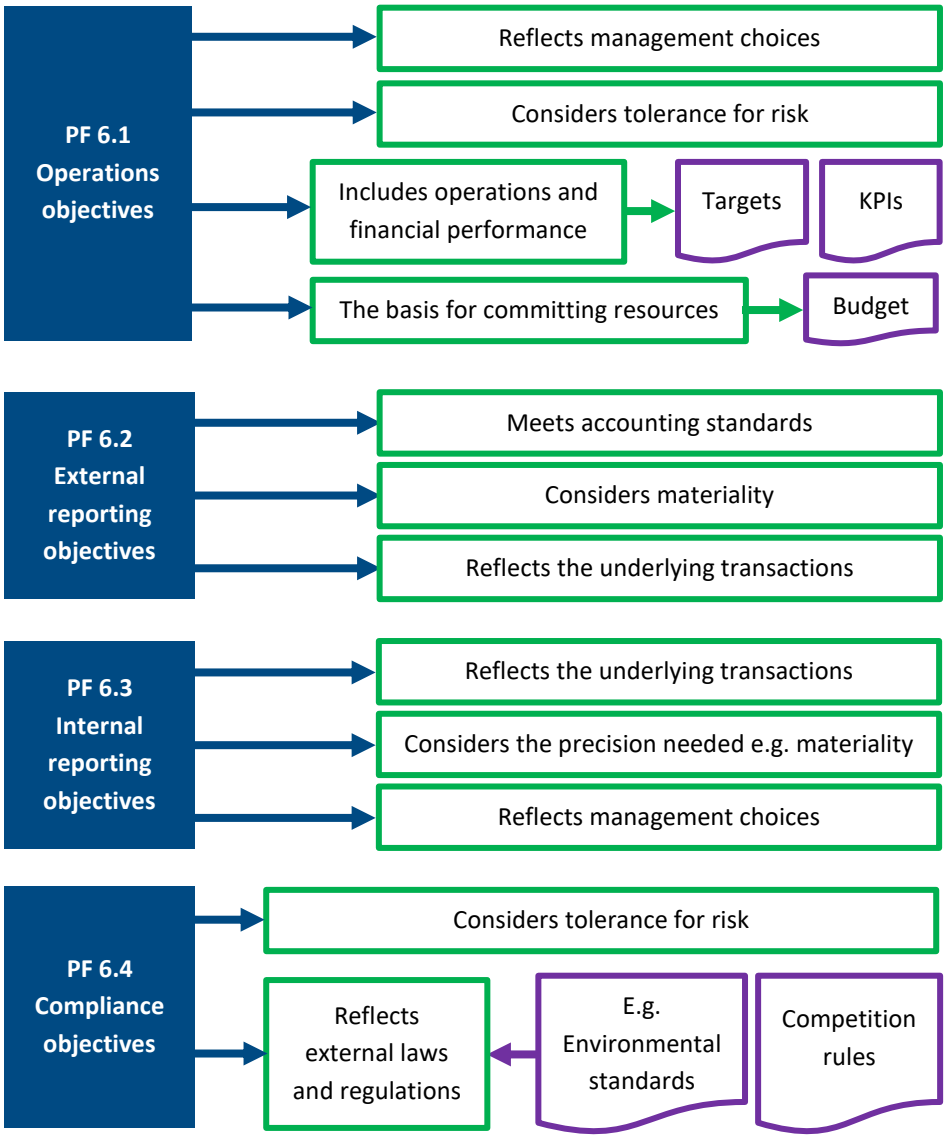
Table 4. The Principles and Points of Focus for Component 2 – Risk Management

Principle		Points of Focus
6	The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	6.1. Operations objectives
		6.2. External reporting objectives
		6.3. Internal reporting objectives
		6.4. Compliance objectives

Principle		Points of Focus
7	The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	7.1. Includes organization and main structures.
		7.2. Analyzes internal and external factors.
		7.3. Involves appropriate levels of management.
		7.4. Estimates significance of risks identified.
		7.5. Determines how to respond to risks.
8	The organization considers the potential for fraud in assessing risks to the achievement of objectives.	8.1. Considers various types of fraud.
		8.2. Assesses incentive and pressures.
		8.3. Assesses opportunities.
		8.4. Assesses attitudes and rationalizations.
9	The organization identifies and assesses changes that could significantly impact the system of internal control.	9.1. Assesses changes in the external environment.
		9.2. Assesses changes in the business model.
		9.3. Assesses changes in leadership.

Principle 6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives

Figure 9. Interpretation of Principle 6



Commentary

Objective setting is a precondition for both accountability and performing effective risk assessment. Objectives must be set before managers can identify and assess the risks to their achievement and take necessary actions to manage these risks. And no accountability system can function without the existence of clear objectives. All objectives set should be "SMART":

- **S**pecific
- **M**easurable
- **A**chievable/Attainable
- **R**ecorded and
- **T**imetabled

This principle encourages managers to focus on the four types of objectives that may exist in the public sector.

Operations objectives relate to the purpose of a public sector activity or program and form the basis for modern systems of program-based budgeting. The objectives should reflect choices (by managers) on how best to implement policies as there are always options relating to public sector policy implementation. Ideally, objectives should include targets and KPIs to promote accountability for implementation. The objectives should also reflect the tolerance for risk. One way of illustrating risk tolerance is that it represents a level below 100% achievement of objectives that would still be considered successful performance. For example, the risk tolerance relating to the safety of members of the public may be small whereas the risk tolerance for losses of grain stored in government stockpiles may be high because there are many factors that can lead to losses of food.

External reporting objectives relate to the requirement placed on all public sector organizations to report on their performance to their governing bodies (often this will be parliament) and their stakeholders (which include the general public). External reporting should reflect the concept of materiality, where only the most important issues are reported. They should also reflect the reality as shown in the underlying transactions. Any financial reports should be produced in accordance with defined accounting standards.

Internal reporting objectives relate to the wide range of internal reporting within an organization that is critical to the effectiveness of internal control. As with external reporting, objectives should reflect materiality and the underlying transactions. Managers should also consider how precise internal reports need to be. Preparing internal reports to a high level of precision may be costly and not worth the effort. For example, a report on the accuracy of transaction processing could be based on a 100% check of a small statistical sample of transactions and still provide management with reliable information on the accuracy of transaction processing

Compliance objectives relate to those external laws and requirements that public sector organizations must comply with. Compliance objectives may, for example, include laws on competition for public sector contracts, the treatment of staff, and environmental standards.

Criteria for assessing internal control effectiveness

Does the organization specify objectives relating to its operations? For example:

- There is a high-level strategy for the organization which contains the objectives of the department as a whole.
- Organizational objectives reflect management and political level choices on how best to respond to policy challenges.
- The high-level strategy is supported by targets and KPIs.
- Each business unit in the organization sets annual objectives with targets and related KPIs.
- Operations objectives form the basis for setting the budget of the organization.
- There is a clear statement of the overall risk appetite of the organization.
- Risk tolerance levels are identified for all main objectives and measured through relevant KPIs.

Does the organization specify objectives relating to external reporting? For example:

- The organization maintains records of income and expenditure against the budget allocated and reports on budget outturn to the ministry of finance.
- The organization is required to prepare annual financial statements in line with the accounting standards adopted for the organization as a whole.
- There is an automated accounting system that supports the accurate preparation of accounts to reflect underlying transactions to an acceptable level of materiality.
- Reports on performance are provided when requested by governing bodies.
- There is a system for the preparation of annual reports on the performance of the organization against its stated objectives.

Does the organization specify objectives relating to internal reporting? For example:

- Internal reports are prepared by units within the organization when they consider it appropriate to do so.
- Internal reports are prepared to an appropriate level of precision and reflect underlying transactions.
- Senior management decides what level of internal reporting is appropriate for different aspects of budgeting and financial management.

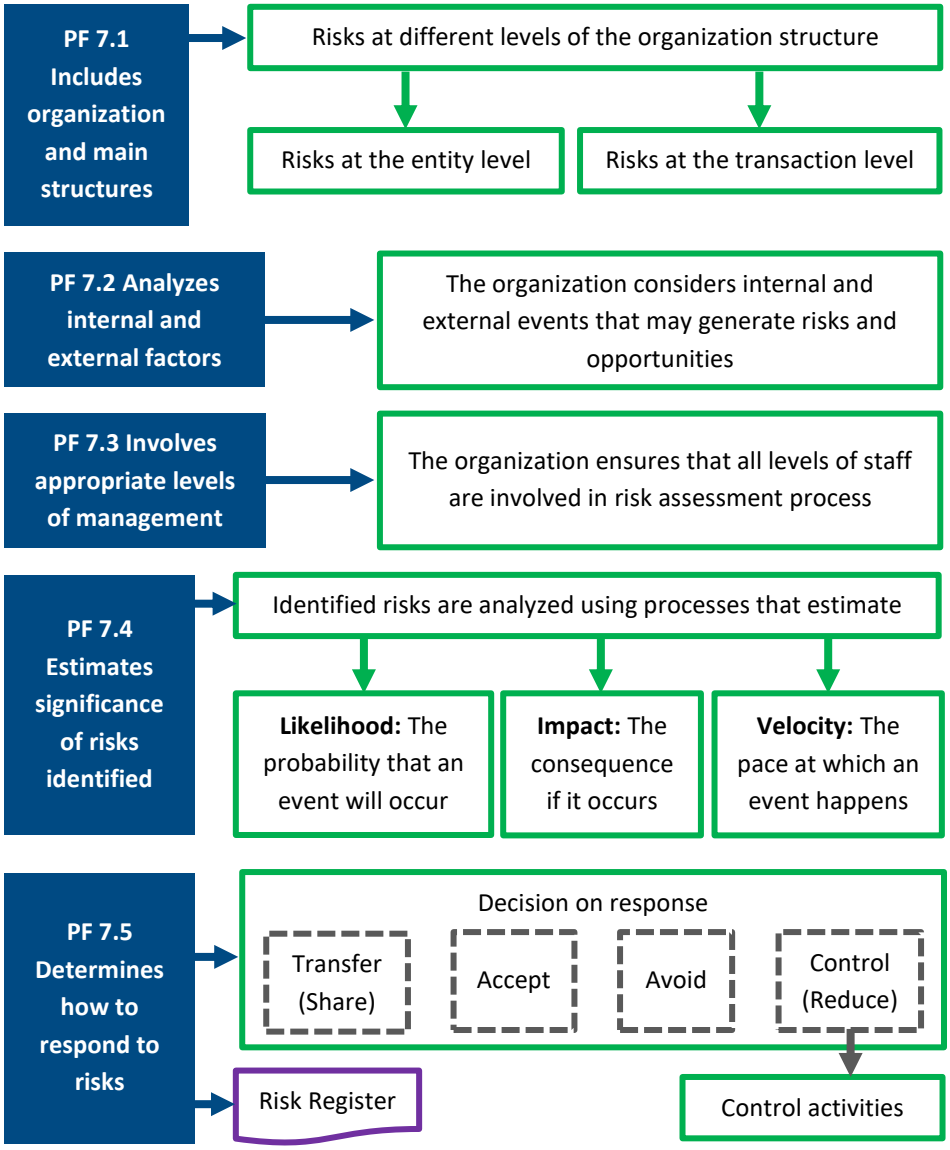
Does the organization specify objectives relating to compliance with external laws and regulations? For example:

- There is a policy explaining how managers should set objectives to comply with government-wide standards.
- Compliance objectives can be wide ranging and include environmental issues, the need for competition, safety and security regulations, and fundamental staffing policies such as minimum rates of pay and harassment.
- Compliance objectives are included in the high-level strategy for the organization.

- The organization meets all main compliance objectives.
- There is a high level of awareness in the organization of the importance of compliance objectives.

Principle 7. The organization identifies risks to the achievement of its objectives across the organization and analyzes risks as a basis for determining how the risks should be managed

Figure 10. Interpretation of Principle 7



Commentary

Once objectives have been set as provided for under Principle 6, management must identify risks to the achievement of these objectives and analyze these to determine how risks should be managed. COSO promotes the use of event-driven risk assessment where events are things that may happen that have a positive or negative impact on an organization: positive impacts are opportunities to achieve objectives and negative impacts are risks to achieving objectives.

Risks should be addressed at all levels of the organization from assessing the impact on transactions (transaction risks) to assessing the impact on the organization as a whole (corporate risks). The process should assess both external events (weather events, social disruption, theft of assets, electrical supply problems) and internal events (staffing losses, machinery breakdowns, errors made by staff, etc.). Managers should be able to distinguish events/risks that are within their control from those that are outside their control.

It is important that staff at all levels are involved in the process of identifying and assessing risks. Those staff responsible for processing transactions may have vital information on risk that is not known by their supervisors.

Having identified events that may represent risks, the organization must assess the significance of each risk to ensure that it is addressing the most important risks it faces. Common practice is to assess risk in three ways:

- **Likelihood,** the probability that an event will occur – for example the chances of being hit by a meteor or hit by a car.
- **Impact,** the consequence or seriousness if it occurs – for example, contrast the consequences of a plane crash landing against a car accident.
- **Velocity,** the pace at which an event happens. For example, contrast the warning period for a lightning strike and a major hurricane.

Having determined the significance of the risk, management must decide how to respond to it. There are four main risk responses:

- **Avoidance**. Stop doing the things that cause the risk (where this is possible). This may not be an option in some public sector organizations who are

required by law to carry out activities that are inherently risky, for example police, fire, and ambulance emergency services.

- **Control (or reduction).** Decide to take action to reduce the likelihood or impact of risk. For example, additional controls are put in place to address a serious risk of fraud by beneficiaries of social services.
- **Acceptance**. Decide to accept the consequences of the risk and take no action to alter its likelihood or impact. This will usually be the response to any risks that (a) have both minimal impact and low likelihood or (b) occur so slowly that it is possible to respond to the risk in real time.
- **Transfer (or sharing).** The likelihood or impact of a risk is shared or transferred to a third party. One common example is where an organization takes out insurance to reimburse some or all of its expenses should the event occur.

The difference between inherent risk and residual risk should be clearly understood. **Inherent risk** is the risk to an organization in the absence of any management actions (risk response) to alter the risk's likelihood or impact. **Residual risk** is the risk that remains after management's response to the risk. Risk assessment is first applied to inherent risks. Once risk responses have been developed, management then considers residual risk. Note that where the response is to avoid or accept the risk, inherent risk is the same as residual risk.

Criteria for assessing internal control effectiveness

Does the organization consider risks at different levels of the organization structure? For example:

- There is a requirement for formal risk assessment processes throughout the organization.
- The majority of organizational units carry out some form of risk assessment.
- There are separate risk registers for regional and headquarter offices.
- There are separate risk registers for organizational units operating as self-contained not for profit agencies who charge for their services or products.

- There are separate risk registers for every operating unit and a corporate risk register for the main risks facing the organization as a whole.

Does the organization consider internal and external events that may generate risks and opportunities? For example:

- There is a formal risk assessment policy that explains how to identify and assess the impact of internal and external events.
- Staff are provided with examples of the types of internal and external events that may lead to risks and opportunities.
- Staff are trained in how to carry out a formal risk assessment.

Does the organization ensure that all levels of staff are involved in risk assessment process? For example:

- Staff at different levels hold separate risk assessment meetings.
- Risk assessments are always carried out during meetings involving staff at all levels.

Does management estimate the significance of risks identified? For example:

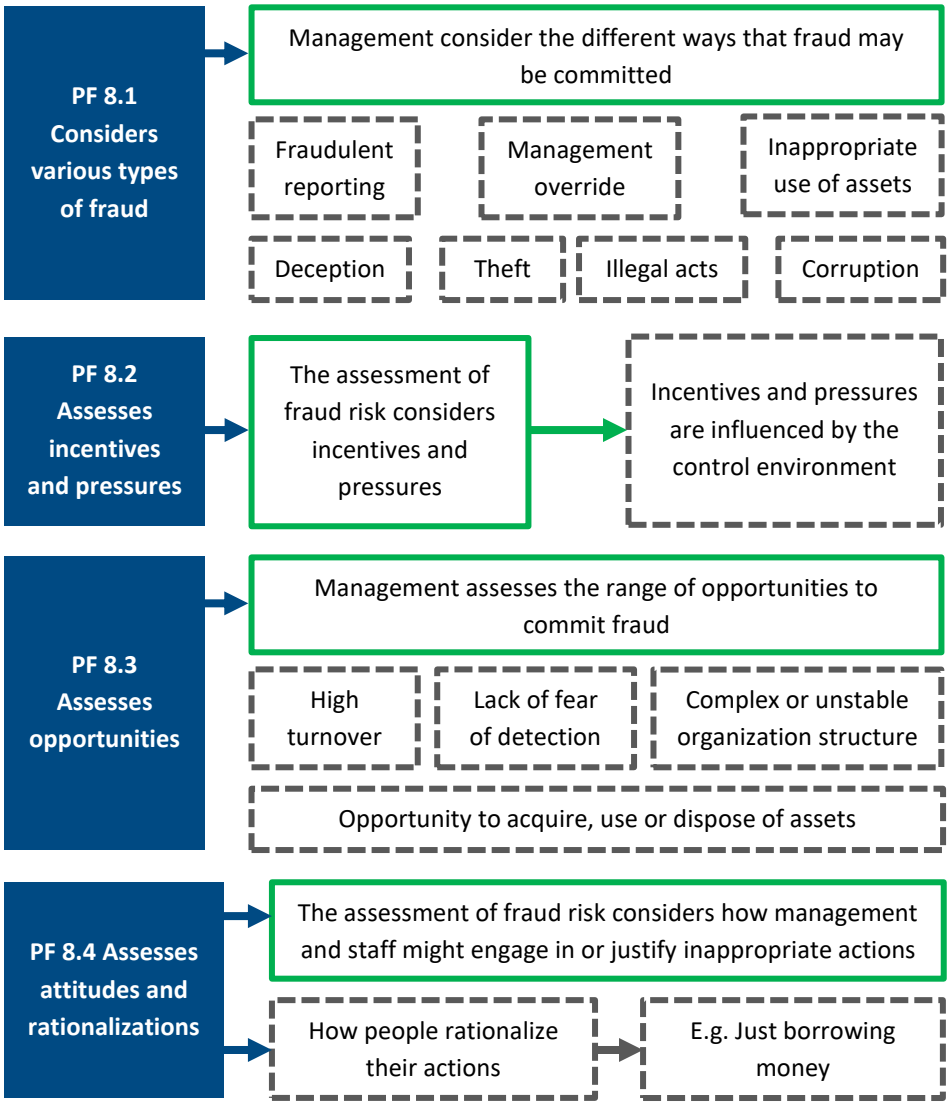
- The risk register contains assessments of the likelihood, impact, and velocity of all risks identified.
- There is a common system for scoring risks across the organization to determine the highest risks facing the organization by measuring likelihood, impact, and velocity.

Has management determined how to respond to risks identified? For example:

- The risk assessment policy provides for four possible risk responses - avoiding, transferring (sharing), accepting, or reducing (controlling) risk.
- The risk register includes the agreed risk response and references to control activities as appropriate.
- Management ensures that risks responses are cost-effective by making appropriate use of all four risk responses.

Principle 8. The organization considers the potential for fraud in assessing risks to the achievement of objectives

Figure 11. Interpretation of Principle 8



Commentary

The updated COSO framework in 2013 includes a specific principle on the need to address the potential for fraud to underline the need for this to be covered during the risk assessment process.

Why do people commit fraud and corruption? Most policemen will say that crime has two fundamental elements: motive and opportunity. Criminals balance opportunity (the gain involved) with the risk of detection and punishment. The higher the gain, the greater the risks they are prepared to take.

There is a significant difference between fraud and corruption. Fraud is an attack on the assets of the organization, whereas corruption is an attempt to influence decision-making processes in ways that benefit a third party. Since most organization have records of their assets, fraudulent action is usually visible from within the organization. Corruption, which involves a third party, may leave little trace internally and is inherently more difficult to identify and prosecute. One of the main defenses against fraud is to reduce the opportunity for an individual to steal assets without detection – e.g. by establishing control measures to detect unauthorized transactions. One of the main defenses against corruption is to limit the influence of any single individual on decisions that benefit third parties e.g. by segregating key functions to reflect the principle that *"four-eyes"* (i.e. at least two people) should review every major transaction.

COSO encourages managers to **consider the many types of fraud and corruption** that exist. This is an area where internal audit has considerable expertise and may therefore be able to assist management in identifying risks.

COSO also underlines **the importance of understanding the incentives, pressures, and opportunities** that may lead to fraud**.** There is no one profile of people who commit fraud and corruption. In many instances, fraud is carried out by people who are otherwise good colleagues. It is motive and opportunity that lead to crime. Common risk factors include:

- sudden changes in lifestyle;
- individuals experiencing severe financial difficulties;

- individuals that have strong personal relationships with major suppliers or contractors;
- staff who rarely take leave or allow others to do their work; and
- staff who are unwilling to be supervised or are uncooperative towards supervisors.

Finally, it is important to assess the attitudes of staff to fraud and corruption and the way they may rationalize their actions. For example: “How do they expect me to survive with the low salaries they pay me?”; “Everyone is corrupt in this organization!”; and so on.

Criteria for assessing internal control effectiveness

Does management consider the different ways that fraud may be committed? For example:

- There is an anti-fraud and anti-corruption policy that explains to staff the different ways that fraud and corruption may occur, for example theft, deception, inappropriate use of assets, fraudulent reporting, management override of controls, and illegal acts.
- All staff are provided with basic training on fraud and corruption awareness.
- Actual identified cases of fraud and corruption are reported to all staff to raise awareness of ways that fraud may be committed.

Does the assessment of fraud risk consider incentives and pressures to commit fraud and corruption? For example:

- All staff in managerial positions are required to provide a declaration of their financial status each year.
- There is adequate segregation of duties to ensure that managers cannot take decisions on their own: the four-eyes principle is followed.
- There are periodic checks for conflict of interest in making decisions.

Has management assessed the range of opportunities to commit fraud? For example:

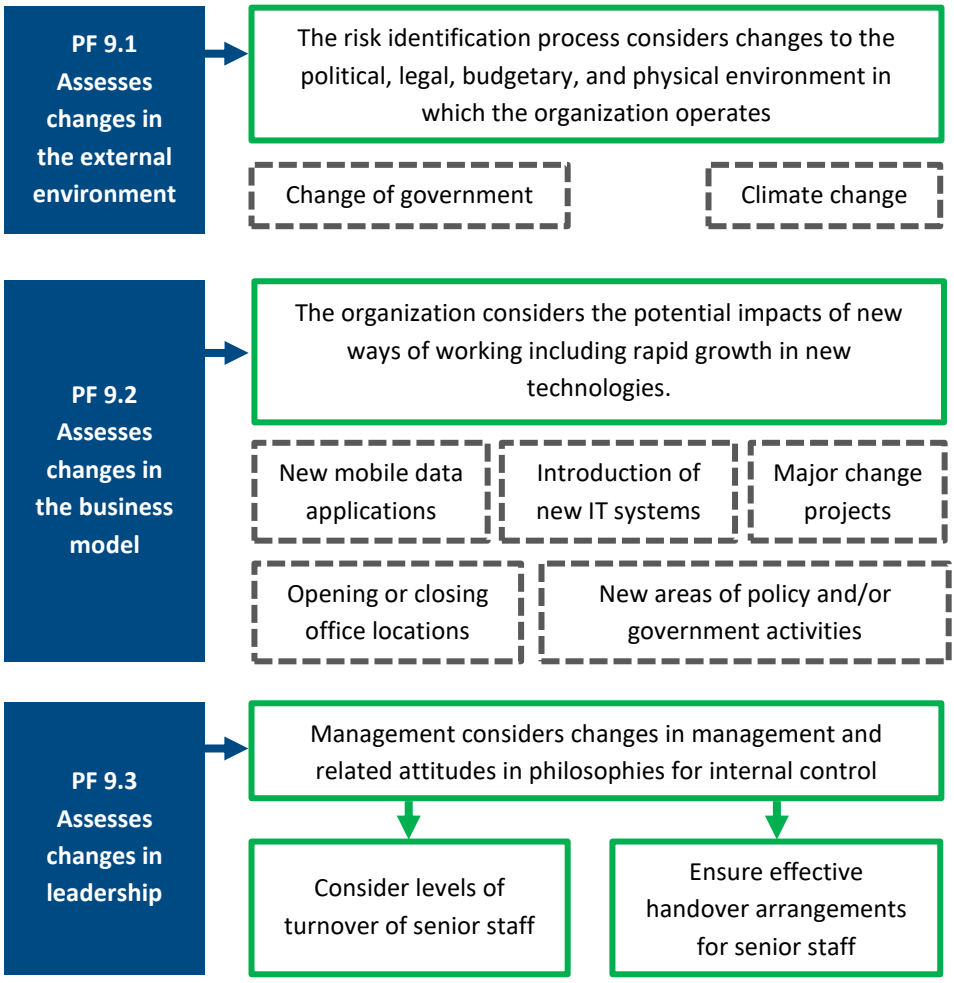
- Management includes assessments of fraud opportunities during risk assessment processes.
- The factors that lead to high turnover of staff in key roles have been identified.
- Management identify high-risk financial positions for additional levels of review.
- Management publicize all cases of fraud and corruption to increase the fear of detection of fraud or corrupt acts.

Does the assessment of fraud risk consider how management and staff might engage in or justify inappropriate actions? For example:

- All staff have had a minimum level of training in fraud and corruption awareness.
- There are periodic checks of personal behavior.
- There is an internal committee on anti-fraud practices.
- Internal audit undertakes third line reviews of the fraud and corruption risks.
- A risk register includes areas of major risk of fraud and corruption.

Principle 9. The organization identifies and assesses changes that could significantly impact the system of internal control

Figure 12. Interpretation of Principle 9



Commentary

COSO underlines the importance of assessing the risks that arise because of changes in the way an organization operates. The risks arising from change are so wide ranging and pervasive that COSO recommends that they are considered

as a separate principle of internal control. COSO recommends that managers focus on three types of change.

Change which happens outside the organization - the external environment. No organization, public or private, exists in a vacuum. What happens outside public sector organizations can have a significant impact on the way it operates or indeed its very existence. For example, changes in the law can result in the addition or the removal of major activities; a major social media campaign can help or hinder the implementation of key policies; etc.

Changes in the way organizations work – new business models. There is always an increase in risk associated with new ways of working. For example, the introduction of new technology; opening or closing offices; or increasing the level of decentralized decision-making.

Changes in the leadership of the organization. The person leading an organization has a major impact on the culture of that organization and consequently the all-important control environment. COSO therefore recommend that changes in leadership are considered during the risk assessment process.

Criteria for assessing internal control effectiveness

Does the risk identification process consider changes to the political, legal, budgetary, and physical environment in which the organization operates? For example:

- Management considers changes in (a) political leadership (government); (b) the global economic/political/geographical directions; (c) the regulatory framework; (d) major restructuring of the public sector – merger of ministries/agencies; and (e) ongoing or expected changes in public administration practices (i.e. PFM/ public sector internal control – PIC).
- Management considers changes resulting from resource availability (reduction in the civil service staffing numbers or other budgetary resources).
- Management considers changes in external environment beyond the control of the organization such as severe weather impacts.

- There is a unit within the organization that is responsible for monitoring change.

Does the risk identification process consider the potential impacts of new ways of working including rapid growth in new technologies? For example:

- Management considers major change projects resulting in changes in the key structures, functions, roles, services, and products delivered.
- Management considers changes to new technology - disruptive technologies including mobile data and their impact on internal processes and internal control.
- There are clear processes to deal with information and communication technologies/cyber security risks and operational availability through business continuity planning and/or disaster recovery planning.
- Management considers the staffing capacity relevant to new roles and objectives.
- There is a unit within the organization that is responsible for monitoring change.

Does the risk identification process consider changes in management and related attitudes in philosophies for internal control? For example:

- Management considers the impact of new managers with a new vision of PIC and different attitudes towards controls.
- Management considers the impact of high levels of turnover in management positions generally.
- There are specific jobs which have formal handover arrangements to ensure that information on key control activities are passed from one manager to another.
- There is a unit within the organization that is responsible for monitoring change.

ANNEX B3. CONTROL ACTIVITIES

This annex focuses on Component 3 – **Control Activities** which are the controls put in place to respond to risks, and the policies and procedures that help ensure that management directives are carried out. There are many choices open to management for ensuring that objectives are reached and that risks are addressed, if necessary, through control activities. The goal is to minimize the cost of controls in line with the risks involved. Controls should not only be effective, but also cost-effective. Moreover, the existence of too many controls may actually have a negative impact. For example, a report that is reviewed by a number of people in a chain may not be fully reviewed in detail by any one individual because each one believes that others are undertaking the main control action.

COSO identifies **three principles within this component**, which are listed in the table below.

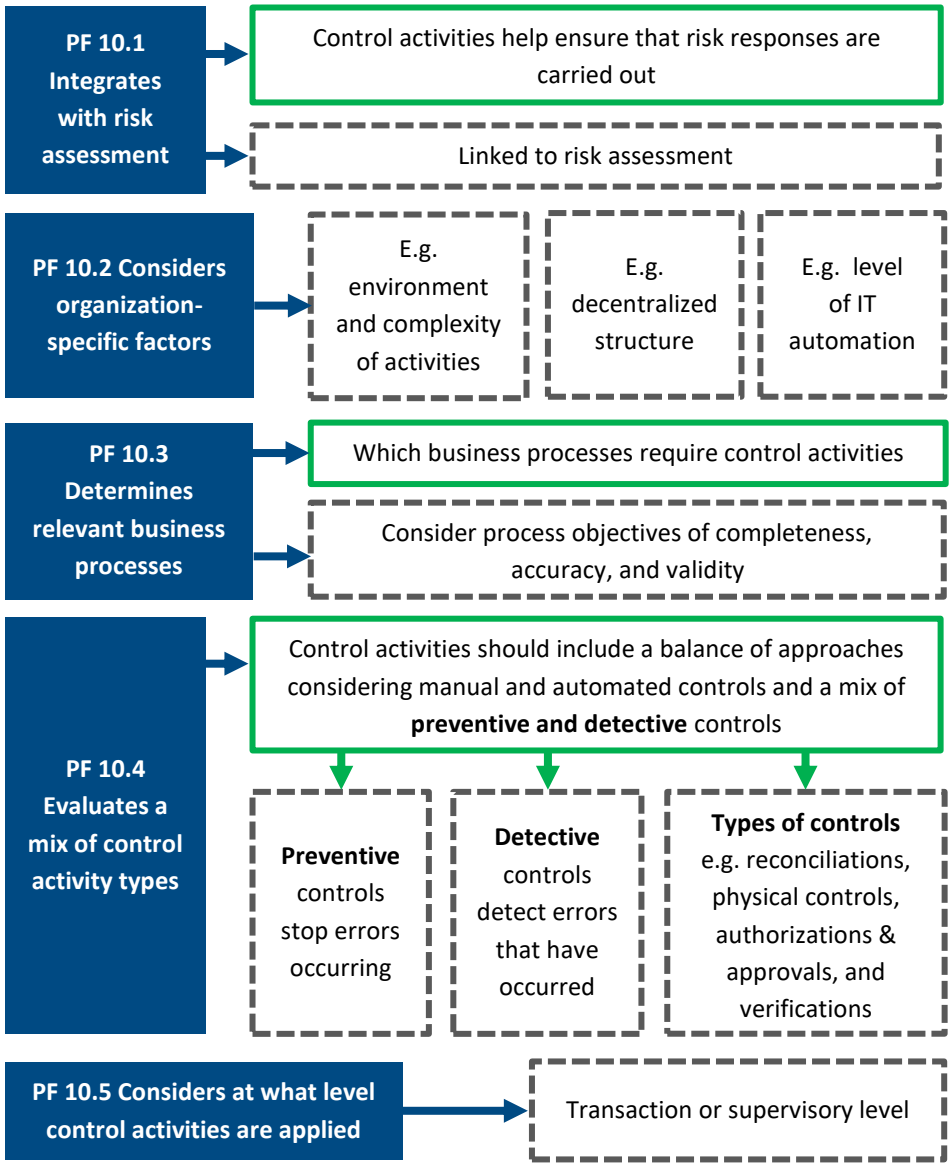
Table 5. The Principles and Points of Focus for Component 3 – Control Activities

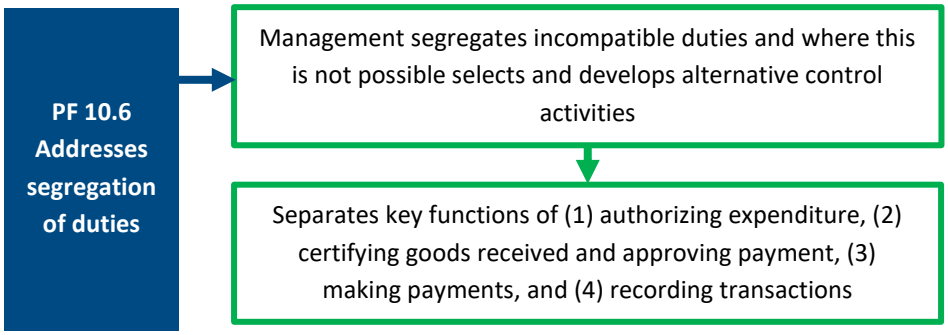
Principle		Points of Focus
10	The organization develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	10.1. Integrates with risk assessment.
		10.2. Considers organization-specific factors.
		10.3. Determines relevant business processes.
		10.4. Evaluates a mix of control activity types.
		10.5. Considers at what level activities are applied.
		10.6. Addresses segregation of duties.
		10.1. Integrates with risk assessment.

Principle		Points of Focus
11	The organization selects and develops general control activities over technology to support the achievement of objectives.	11.1. Determines dependency between the use of technology in business processes and technology general controls.
		11.2. Establishes relevant technology infrastructure control activities.
		11.3. Establishes relevant security management process control activities.
		11.4. Establishes relevant technology acquisition, development, and maintenance process control activities.
12	The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action.	12.1. Establishes policies and procedures to support deployment of management's directives.
		12.2. Establishes responsibility and accountability for executing policies and procedures.
		12.3. Performs in a timely manner.
		12.4. Takes corrective action.
		12.5. Performs using competent personnel.
		12.6. Reassesses policies and procedures.

Principle 10. The organization develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels

Figure 13. Interpretation of Principle 10





Commentary

Control activities are policies and procedures (the actions of people to implement the policies directly or using IT) to ensure that risk responses are carried out and risks to achieving the organization's objectives are addressed. **This link to risk assessment is critical to ensure that controls are addressing the most important risks**.

Management need to determine which business processes require control activities and develop a mix of preventive and detective controls:

- **Preventive controls** are designed to stop errors and omissions occurring before transactions happen (for example a validation check that payments are only being made to companies that have a supplier record in the IT system).
- **Detective controls** are designed to identify errors that have already occurred (for example a check which identifies any suppliers who have been paid twice).

All preventive controls and some detective controls operate at the first line of defense, while most detective controls operate as a second line of defense.

Management will often use many different types of controls, for example:

- **Information-processing controls**: These include checks of data entered, numerical sequences of transactions, and controls over access to data, files, and software.

- **Physical controls**: Equipment, inventories, cash, and securities are physically secured, periodically counted, and compared to control records.
- **Exception reports/routines**: Many control systems (particularly computerized systems) will reject transactions that fail certain tests requiring some form of management intervention/approval before the transaction can be processed.
- **Direct management actions**: regular line-management reviews of, for example, performance reports, exceptions reports, and reconciliations between different data sets.
- **Top- level reviews**: Senior management reviews of actual performance against budgets, forecasts, and previous periods. This includes the tracking of major initiatives to measure the extent to which targets are being achieved.
- **Performance measures and indicators**: Different datasets (e.g. financial and operations data) are compared and the relationships between them analyzed. By identifying unexpected results or unusual trends, management may identify weaknesses in controls. Investigation and corrective action serve as the control activity.

Segregation of duties is a key element of control activities. Roles and responsibilities are divided or ("segregated") among different people to reduce the risk of errors or inappropriate actions such as fraud and theft. For example, different individuals should be responsible for (1) authorizing expenditure; (2) certifying goods and services received and approving payment; (3) making payments; and (4) recording transactions.

Controls operate at different levels. Lower-level controls usually operate at the transaction level and can be regarded as the first line of defense against risks. However, higher-level controls such as performance indicators and exception reports provide managers with a far greater level of assurance that systems are working effectively and can also be used by the second line of defense. Senior managers will usually focus on higher-level controls whenever possible.

Criteria for assessing internal control effectiveness

Does the organization ensure that control activities are integrated with risk assessment? For example:

- All risk registers include references to the control activities that are intended to reduce inherent risks to an acceptable level.
- There is a corporate risk register which identifies the major risks facing the organization and the key control activities put in place to address those risks.

Has the organization considered organization specific factors (such as the level of decentralization and the extent of IT automation) in developing control activities? For example:

- The organization understands and applies the concept of the three lines model when designing its control activities.
- The organization uses the three lines model to establish effective controls over decentralized activities: there is a common set of guidance for managers of regional offices on the roles of the second and third lines in relation to regional activities.

Has the organization determined which business processes require control activities? For example:

- The understanding of which business processes require control activities ranges from basic to thorough depending on organizational maturity. The basic level includes policies specifying which types of contracts require competitive bidding and processes critical to the preparation of accurate financial statements.
- Business processes objectives cover **completeness** (that all transactions are processed), **accuracy** (that transactions are correctly valued and recorded), and **validity** (that transactions represent legitimate expenditure or revenue of the organization and have been properly authorized in accordance with the budget).

Does the organization have a balance of approaches considering manual and automated controls and a mix of preventive and detective controls? For example:

- There is a clear understanding of the differences between preventive and detective controls and a balanced approach to the use of each type of control.
- Management makes full use of different types of controls e.g. reconciliations, physical controls, authorizations & approvals, and third-party verifications.
- Basic attempts to reduce costs are made through limiting checks of transactions below a certain financial value.
- Management assesses the cost-effectiveness of different control activities before determining which control activities to implement.

Has the organization considered at what level control activities should be applied? For example:

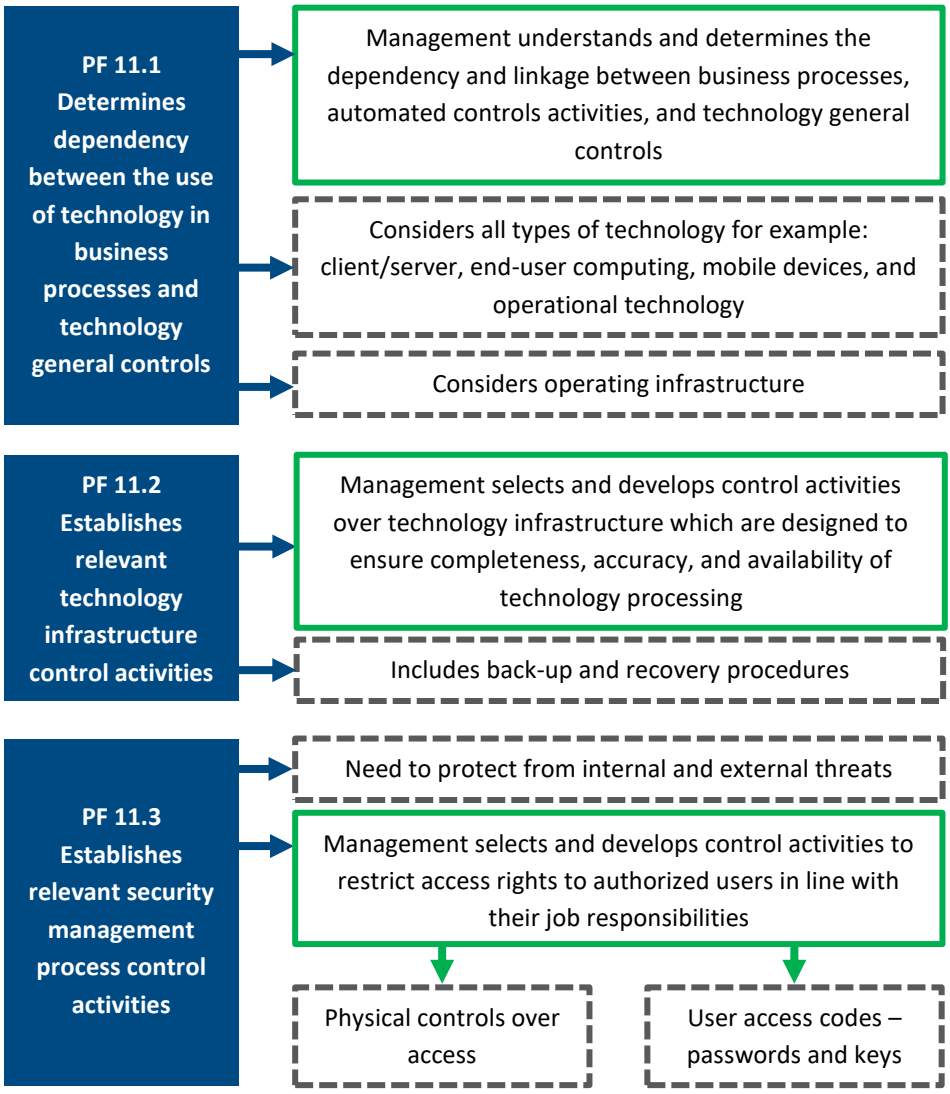
- There are separate requirements for control activities at the transaction and supervisory levels.
- Wherever possible, management focuses key controls at the supervisory level.

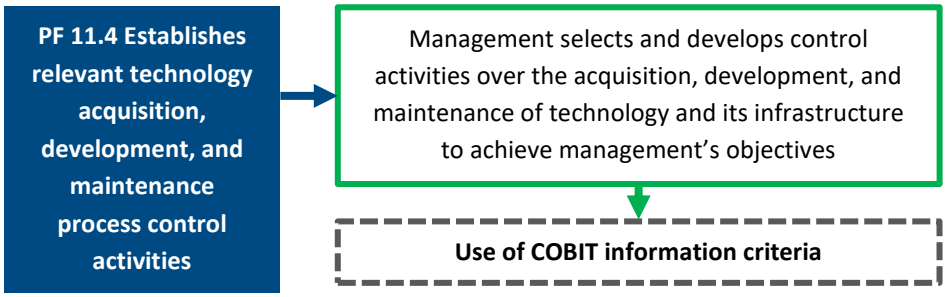
Has management segregated incompatible duties and where this is not possible selected and developed alternative control activities? For example:

- Management have identified four key functions that must be segregated – (1) authorizing expenditure, (2) certifying goods received and approving payment, (3) making payments, and (4) recording transactions.
- There are additional checks by a second line oversight unit when segregation is not practical because of the size of the business unit.
- Internal audit reviews the adequacy of segregation of duties as part of the third line of defense.

Principle 11. The organization selects and develops general control activities over technology to support the achievement of objectives

Figure 14. Interpretation of Principle 11





Commentary

Most organizations are highly reliant on information systems. Controls over information systems are therefore very important. However, the underlying concepts of control such as event identification, risk assessment, risk response, and the development and implementation of cost-effective control activities are the same for both manual and IT-based systems.

Management needs to understand and determine the dependency and linkage between business processes, automated control activities, and technology general controls. The main elements of IT in an organization are:

- **IT infrastructure**. Servers, networks, internet, Wi-Fi, and the operating system and application software.
- **Personal computing**. Business use of mobile devices and laptops, use of spreadsheet and other files and applications.
- **Outsourced IT**. Use of cloud computing, off-site service providers, back-up, and storage.
- **IT governance.** The structure set up to organize and manage the IT function.

There are two main types of control activity which seek to meet the information processing objectives of completeness, accuracy, and validity:

- **Application control activities** which include authorizations, verifications, reconciliations, physical access controls, and supervision of processes.
- **Technology general controls** over infrastructure and operations, security of data and software, and the system development life cycle.

This COSO principle focuses on **general control activities over technology** and specifically controls over IT infrastructure (including back up plans), IT security (access to IT systems and applications), and the acquisition and development of new technology. Controls that relate to specific applications would usually be considered as part of the achievement of the objectives of the policy for which the particular application was designed. For example, the controls in an IT application to process requests for passports should be designed to meet the risks related to the objective for issuing passports.

Criteria for assessing internal control effectiveness

Does management determine the dependency and linkage between business processes control activities and technology general controls? For example:

- There is a separate IT policy which identifies all the main elements of IT in use across the organization. The policy includes consideration of client/server technology, cloud-based data storage, end-user computing, mobile devices, and operating systems.
- Management understands and determines the dependency and linkage between business processes automated controls activities and technology general controls.
- Management uses the Control Objectives for Information and Related Technology (COBIT) 5 framework[6] for the governance and management of entity-wide IT systems and processes.

Does management establish relevant technology information controls? For example:

- Management selects and develops control activities over technology infrastructure which are designed to ensure completeness, accuracy, and availability of technology processing.
- There are clearly defined daily back-up and recovery procedures for all key data in the organization.

[6] Framework created by the Information Systems Audit and Control Association for IT governance and management

- There are procedures such as back-up electricity generators to ensure a high level of availability of corporate IT systems.

Has management established relevant security management process control activities? For example:

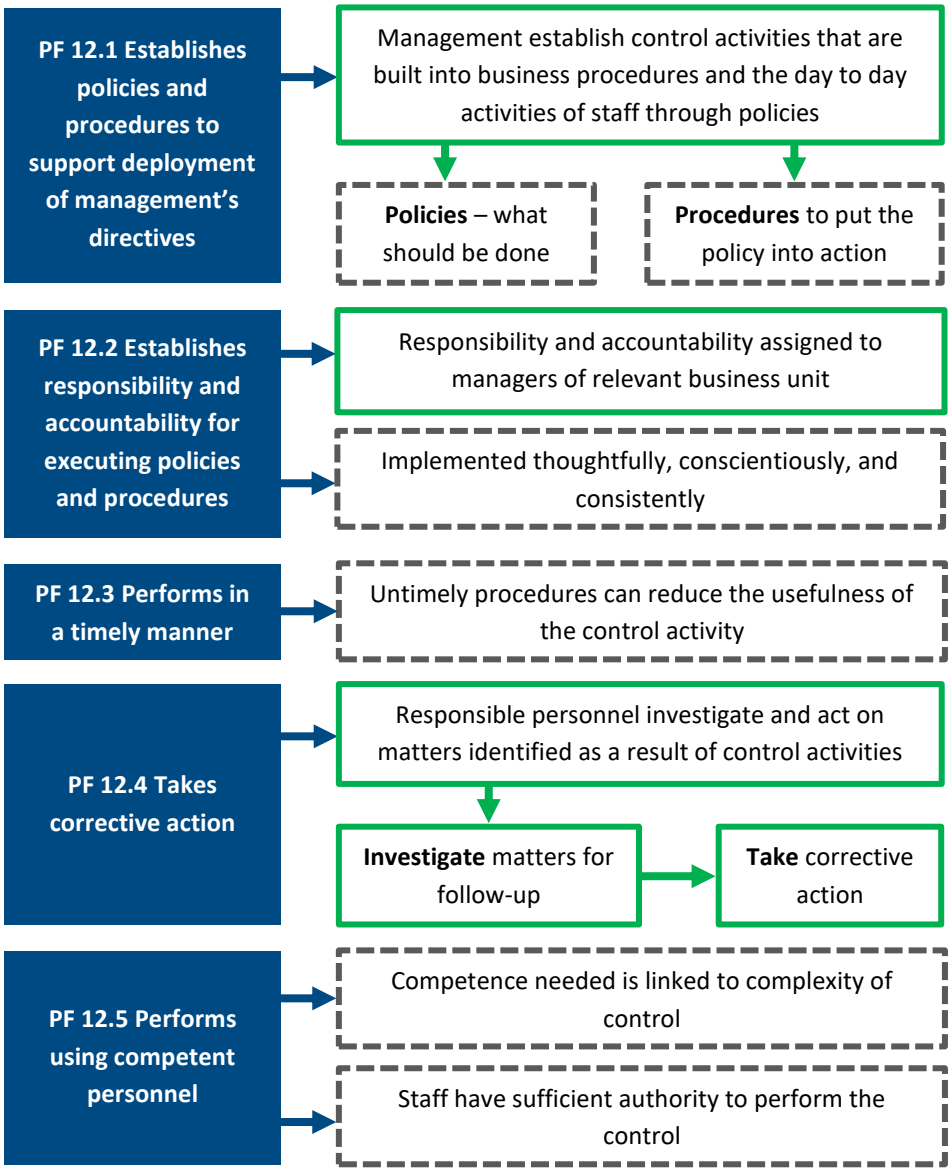
- Management selects and develops control activities to restrict access rights to authorized users in line with their job responsibilities by using physical controls over access to offices with IT infrastructure and user passwords to access IT systems.
- Stronger IT security controls include regular changes to access passwords and the use of strong password naming conventions.
- Optimally there are strict and automatic limitations of user access to only those applications that are essential for the performance of duties.

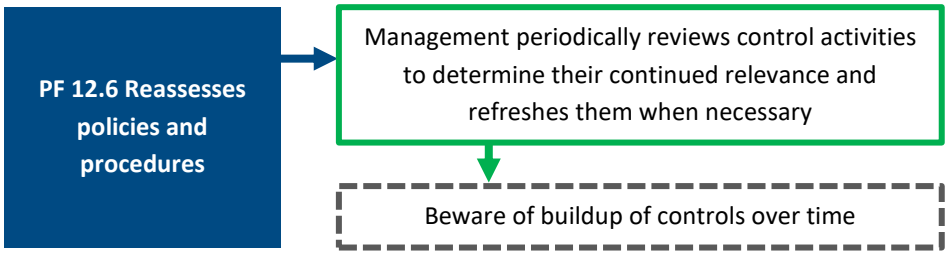
Does management select and develop control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives? For example:

- A specialized IT unit is responsible for acquisition, development, and maintenance of IT processes.
- A high-level committee oversees IT developments for the organization as a whole.
- The organization follows the COBIT 5 framework for all its IT acquisitions and disposals.

Principle 12. The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action

Figure 15. Interpretation of Principle 12





Commentary

Control activities consist of **policies** that describe what should be done and **control procedures** which put the policy into action. Control procedures usually have two elements: (i) the control process itself - what the person does; and (ii) the evidence that the control has been carried out – usually a signature by the person carrying out the control. The signature is only one element of a control procedure (e.g. supervisors must sign all travel authorizations). It is the actions of supervisors before they sign (the control process itself) that counts.

The responsibility and accountability for implementing control activities needs to be clearly assigned. Control policies must be implemented thoughtfully, conscientiously, and consistently. Procedures are not useful if they are carried out mechanically or without a sharp continuing focus. Control procedures have to be carried out at the appropriate time. Errors or problems identified as a result of the procedure must be investigated and appropriate corrective action taken.

Control activities must also be carried out by staff who are competent to carry out the control procedure. For example, a qualified electrician would be needed to carry out monthly checks of the functioning of a burglar alarm at a storage facility. Staff may also need a defined level of authority to carry out a particular control. For example, it would not be appropriate for a member of staff to approve the travel claim of his/her supervisor.

Systems of internal control degrade over time. Many organizations experience "control creep" where new controls are added without considering the effectiveness of existing control activities. Functions at the second line of control should be tasked with reviewing control activities periodically to determine their continued relevance, making changes as necessary.

Criteria for assessing internal control effectiveness

Has management established policies and procedures to support the deployment of management's directives? For example:

- There is a set of policies which identify what should be done in terms of control.
- There is documentation of the procedures (steps) to be followed to implement the policy.
- There is mandatory training for staff on implementing key controls.

Has management established responsibility and accountability for executing policies and procedures? For example:

- Responsibility for each element of the control process is allocated to named individuals.
- Managers and staff receive training on the importance of implementing controls thoughtfully, conscientiously, and consistently.

Does the organization perform control activities in a timely manner? For example:

- There are predefined standards for the time required to carry out critical control activities such as the time to process payments or the dates when bank reconciliations must be completed.
- There are regular reports to supervisors and managers on the timeliness of business processing.

Does the organization take corrective action on matters identified as a result of control activities? For example:

- Procedures exist for taking corrective action, but the level of adherence depends on the maturity of the organization.
- Higher-level supervisors must personally authorize the processing of all transactions that are rejected by IT validation checks.
- There are regular reports to supervisors and managers on areas where corrective action has not been taken.

Does the organization perform control activities with competent staff? For example:

- The level of competence and authority required to carry out each control activity is clearly defined.
- Managers and staff are aware of the competence and authority needed to carry out controls effectively.
- Expenditure over predetermined financial limits must be authorized by more senior staff.

Does the organization periodically review control activities to determine their continued relevance, refreshing them when necessary? For example:

- Management reviews the continued relevance of control activities on a regular basis.
- There is a clear timeframe for reviews of the continued relevance of control activities.
- Senior management agree with internal audit the frequency of systems-based audits of key business processes.
- All financial delegations have a sunset clause which specifies the date when they must be reviewed to determine their continued relevance.

ANNEX B4. INFORMATION & COMMUNICATION

This annex focuses on Component 4 – Information & Communication which ensures that pertinent information about an entity's activities is identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities:

- **Communication** is the continual iterative process of providing, sharing, and obtaining necessary information.
- **Information** is the data that is combined and summarized based on relevance to information requirements.

COSO identifies **three principles within this component**, which are listed in the table below.

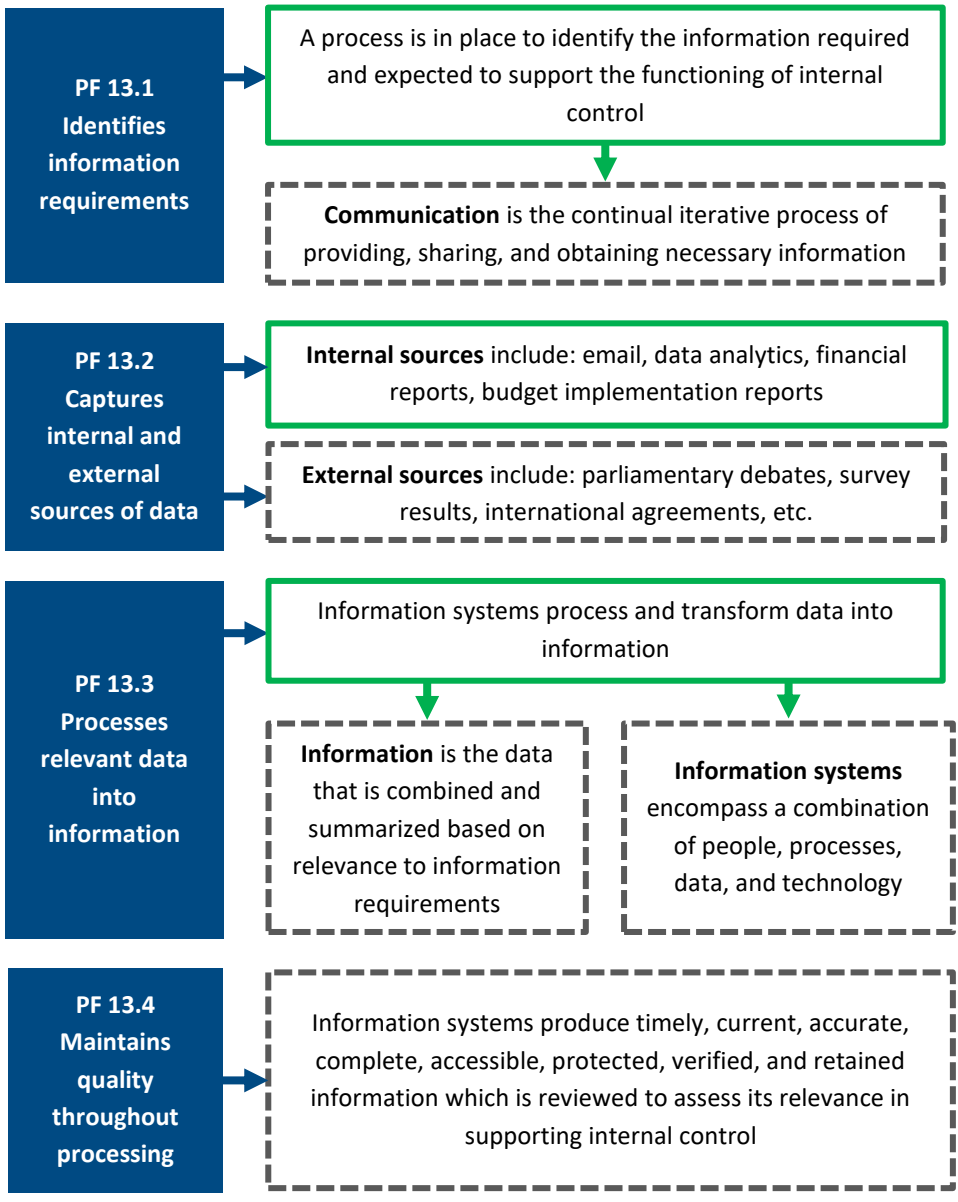
Table 6. The Principles and Points of Focus for Component 4 – Information & Communication

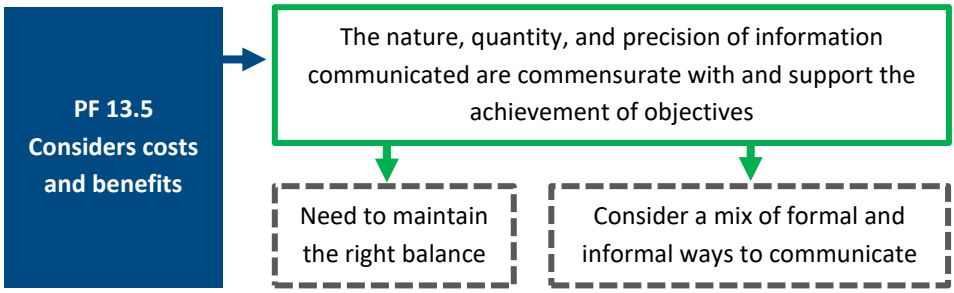
Principle	Points of Focus
13 The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.	13.1. Identifies information requirements.
	13.2. Captures internal and external sources of data.
	13.3. Processes relevant data into information.
	13.4. Maintains quality throughout processing.
	13.5. Considers costs and benefits.

Principle		Points of Focus
14	The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	14.1. Communicates internal control information.
		14.2. Communicates with governing bodies.
		14.3. Provides separate communication lines.
		14.4. Selects relevant methods of communication.
15	The organization communicates with external parties regarding matters affecting the functioning of internal control.	15.1. Communicates to external parties.
		15.2. Enables inbound communication.
		15.3. Communicates with governing bodies.
		15.4. Provides separate communication lines.
		15.5. Selects relevant methods of communication.

Principle 13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control

Figure 16. Interpretation of Principle 13





Commentary

The organization needs to identify its information requirements and then ensure that relevant information is obtained from internal and external sources.

The organization must capture and use historical and current data as necessary to support effective internal controls, particularly in its monitoring at the second line of defense. Specifically:

- The information infrastructure converts raw data into relevant information that assists personnel in carrying out their responsibilities.
- Information is provided in a readily usable form and in a timely manner according to specific needs – including the need to identify, assess, and respond to risk.
- Data are reliable and provided on time at the right place to enable effective decision-making.

Criteria for assessing internal control effectiveness

Has management established a process to identify the information required and expected to support the functioning of internal control? For example:

- The information needs of key controls are specified in internal manuals and procedures.
- The communication process of providing and sharing information works well.
- Individual staff are assigned responsibility for (a) defining information needs and (b) generating the data to meet these needs.

Does the organization have information systems that process and transform internal and external data into information? For example:

- Internal sources of data include emails, data analytics, financial reports, and budget implementation reports.
- External sources of data include public or parliamentary debates, government pronouncements, press coverage, the results of external surveys, and international agreements.
- The organization has systems for the collection and communication of internal and external data.
- There is a single system for processing all accounting data in the organization.
- Over time the process of capturing and communicating information is automated.

Does the organization process relevant data into information? For example:

- The organization has information systems to process critical data into usable information for managers.
- Data that does not meet criteria for accuracy are not included in management reports.

Does the organization maintain quality throughout its processing? For example:

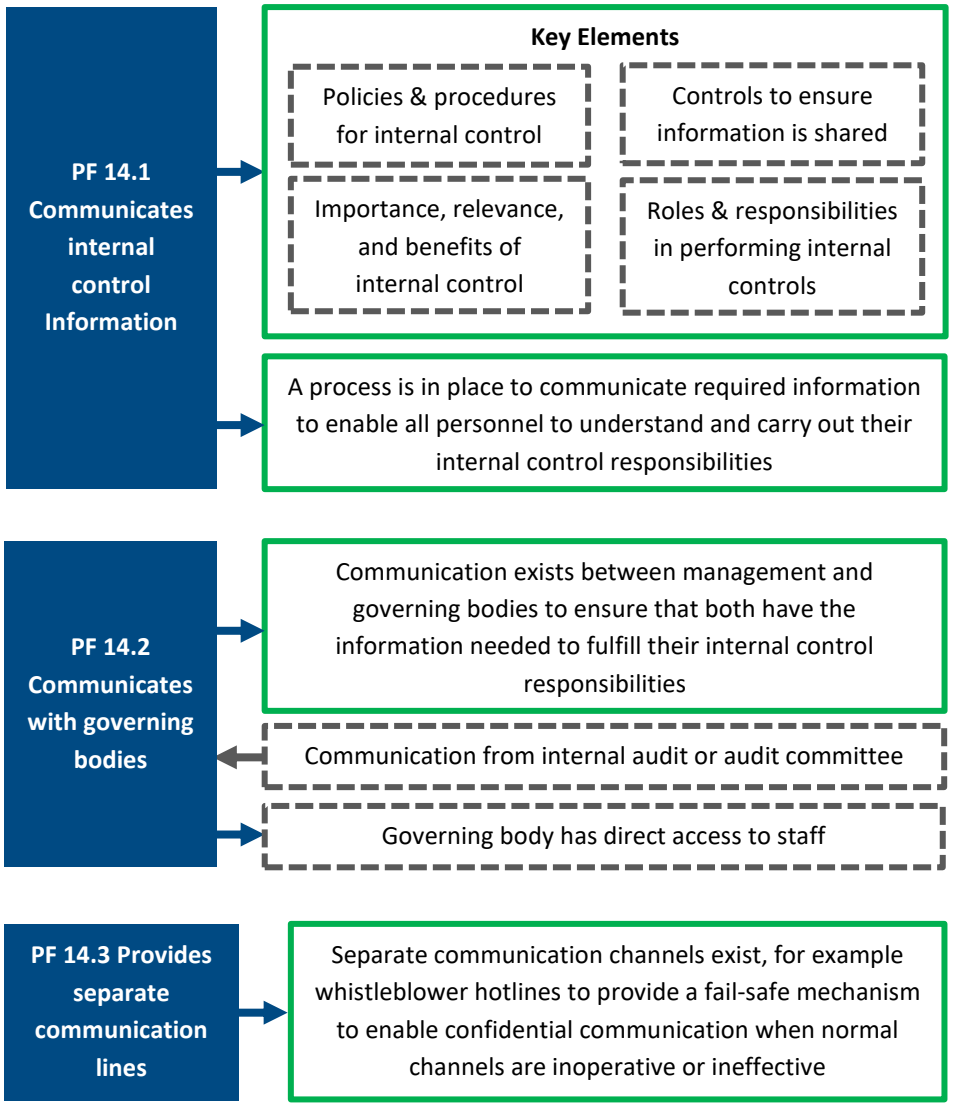
- The organizations' systems are designed to produce timely, current, accurate, complete, accessible, protected, verified, and retained information.
- All financial data entry systems have ways of validating original data (e.g. through double keying, supervisor sign off, etc.) before the data is accepted for processing.

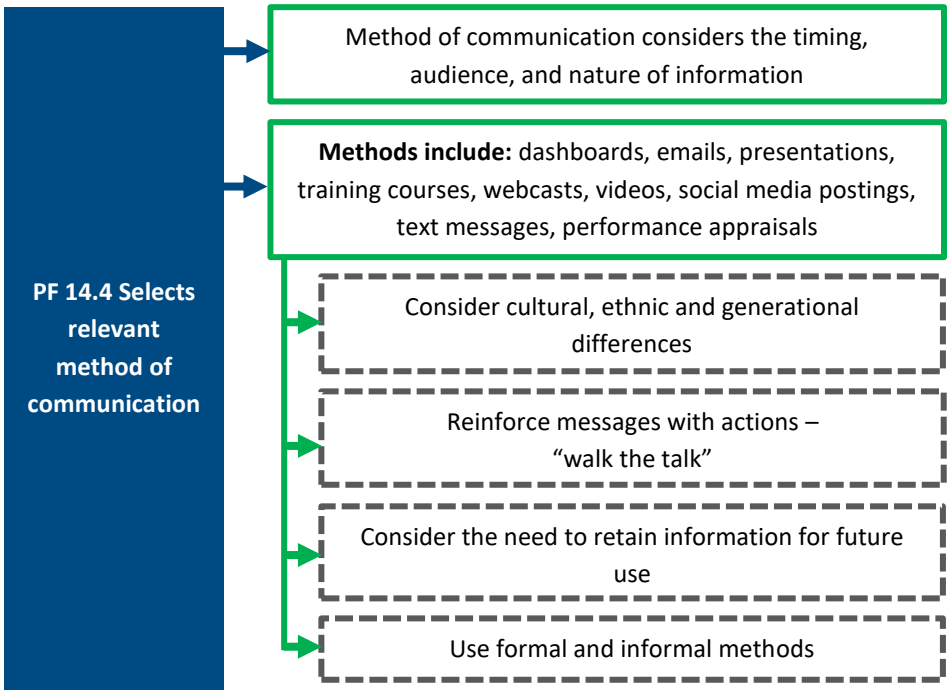
Does the organization consider the costs and benefits of information collection and dissemination? For example:

- Management reviews the nature, quantity, and precision of information communicated to check whether the costs of collecting information is consistent with the benefits gained.
- The organization identifies the cost of producing major reports on internal control effectiveness, including the direct costs of internal audit examinations.
- Internal audit carries out periodic audits of the value for money of information systems.
- Action is taken to stop collecting information that is no longer beneficial.

Principle 14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control

Figure 17. Interpretation of Principle 14





Commentary

Communication is inherent in information processing. Effective communication must occur up, down, and across the organization to enable all staff to understand and carry out their internal control responsibilities. Key issues include:

- Specific and directed communication to address behavioral expectations and responsibilities of staff;
- Communication about the policies and procedures needed for internal control;
- Processes and procedures that align with and underpin organizational culture;
- All staff receive clear messages from top management about the importance of internal control;
- All staff know how their activities relate to the work of others, enabling them to recognize problems, determine causes, and take corrective actions;

- There are open channels of communication and a willingness to listen, and staff believe their superiors truly want to know about problems and will deal with them effectively; and
- There must be effective communication between management and governing bodies to ensure that both can fulfil their internal control responsibilities. This should include formal reporting arrangements for the audit committee to governing bodies to reinforce the independence of internal audit. Communications channels should also exist outside normal reporting lines and personnel need to understand there will be no reprisals for reporting relevant information.

The way messages are communicated has a direct impact on how well the message is understood. There are many different channels available (see figure 17). The timing, audience, and the nature of what is being communicated must be considered. For example, it would not be appropriate to discuss the negative performance of one staff member in an email to all staff. Management also need to reinforce messages with actions and "walk the talk".

Criteria for assessing internal control effectiveness

Has management put in place processes to communicate required information to enable all personnel to understand and carry out their internal control responsibilities? For example:

- The internal control responsibilities of all staff are laid down in manuals and guidelines.
- Policies and procedures for internal control are specified in manuals and guidance available to all staff.
- Staff have been trained on the importance, relevance, and benefits of effective internal control.
- There are controls to ensure that key information is shared.

Does management communicate effectively with governing bodies? For example:

- There are formal and informal communication channels between management and governing bodies.
- Management communicates regularly with governing bodies.
- The governing bodies have direct access to staff of the organization as needed.
- The audit committee presents an annual report of its activities to governing bodies.
- Copies of internal audit reports are available to governing bodies.

Has management established separate communication channels? For example:

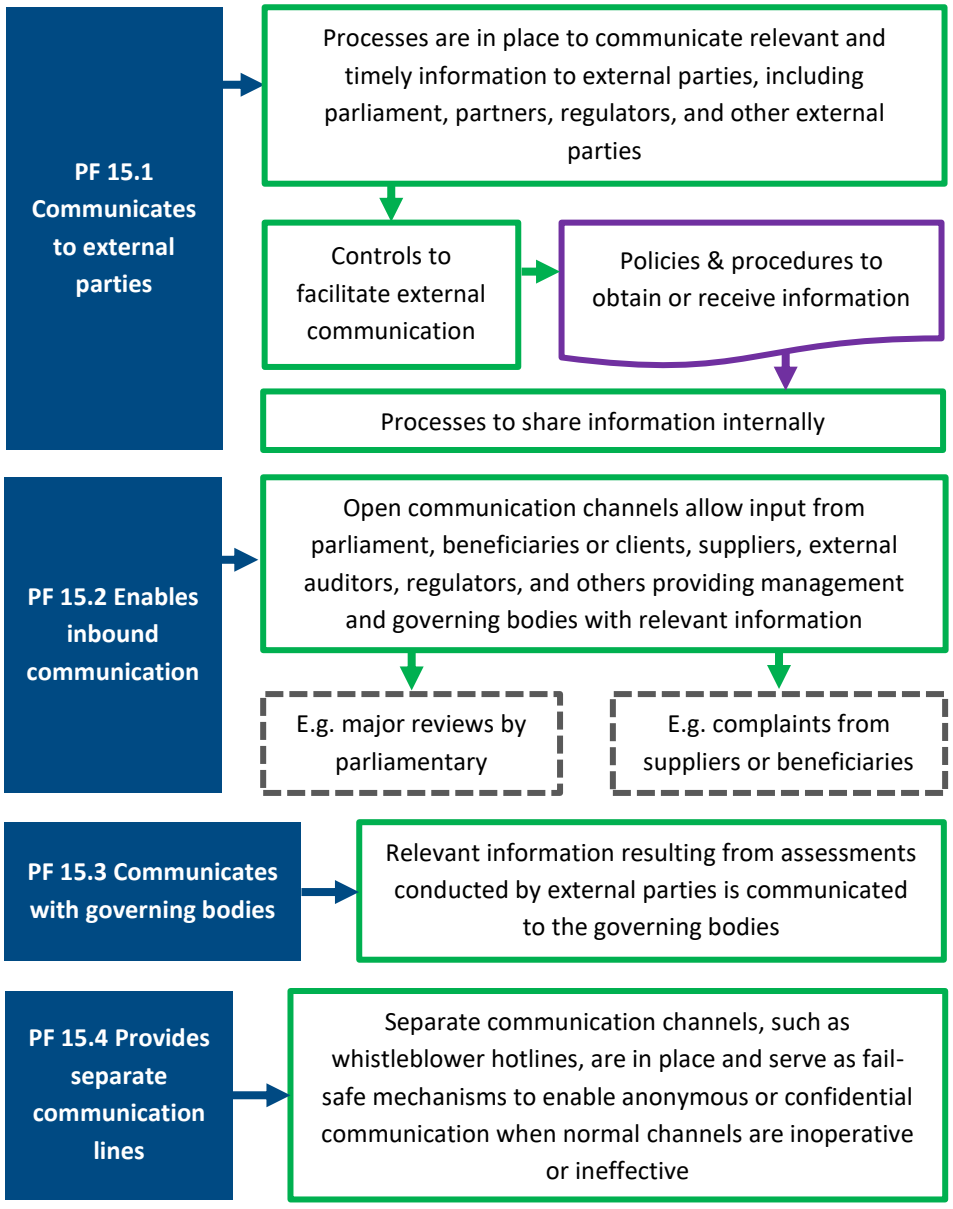
- There is a whistleblower hotline to provide a fail-safe mechanism to enable confidential communication when normal channels are inoperative or ineffective.
- There is a policy for the protection of all whistleblowers.
- Management promote extensively the existence of the hotline and the protection provided to whistleblowers.
- There is an annual report on the effectiveness of the whistleblower hotline, including statistics showing the extent of use and action taken to address issues raised.

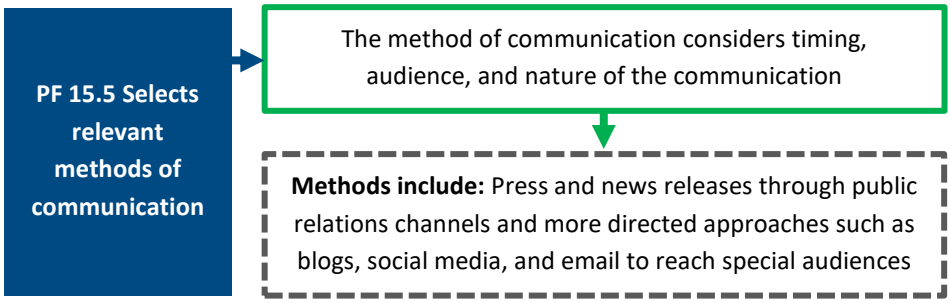
Does management select relevant methods of communication for its messages to staff? For example:

- Management chooses between a range of different communication methods depending on what needs to be communicated.
- Depending on the maturity level, such methods include management dashboards, emails, presentations, training courses, webcasts, videos social media postings, text messages, and the formal appraisal process.
- There are regular all staff meetings on important changes in the organization's functions, structure, and operational objectives.
- Management reinforces key messages with their own actions – they "walk the talk".

Principle 15. The organization communicates with external parties regarding matters affecting the functioning of internal control

Figure 18. Interpretation of Principle 15





Commentary

Strong processes of external communication are a crucial part of internal control. Organizations need to put in place processes to communicate relevant and timely information to external parties, including parliament, partners, regulators, and other external parties. But communication also takes place in a broader sense, dealing with expectations and responsibilities of individuals and groups.

Communicating effectively with governing bodies is particularly important. Establishing open communication channels allows stakeholders and suppliers to provide feedback to the organization. Organizations also need to ensure that separate communication channels, such as whistleblower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.

As with internal communication, the organization needs to use methods of communication that are appropriate to the message being delivered.

Criteria for assessing internal control effectiveness

Does the organization communicate effectively with external parties? For example:

- There are processes in place to communicate relevant and timely information to external parties, including parliament, partners, regulators, and other external parties.

- External communication includes regular reports on budgetary outturn; and an annual report on the financial statements of the organization.
- There are pubic reports on the performance of the organization in relation to its operational objectives.

Has management enabled inbound communication? For example:

- Management has established open communication channels that allow input from parliament, beneficiaries or clients, suppliers, external auditors, regulators, and others.
- Reports of the results of external audits by the SAI are sent to parliament and published in the official gazette.
- All complaints from beneficiaries or external suppliers are recorded for follow up and action.

Does the organization communicate effectively with its governing bodies? For example:

- Management ensures that relevant information from assessments conducted by external parties is communicated to governing bodies. These may include reports by regulators and/or auditors.
- The annual accounts including the report of the external auditor are presented directly to governing bodies (or audit committee if one exists) for consideration and review.
- There is an agreement between management and the governing bodies on what information related to assessments by external parties must be provided to governing bodies and the timeframe when this must be done.

Has the organization established separate communication channels to enable anonymous or confidential communication when normal channels are ineffective? For example:

- Separate communication channels, such as whistleblower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.

- There is a policy for the protection of all whistleblowers.
- Management extensively promote the existence of the whistleblower hotline and the protection provided to whistleblowers.
- Management issues a public report on the effectiveness of the whistleblower hotline, including statistics showing the extent of use and action taken to address issues raised.

Does the organization have a wide range of communication methods depending on the audience it is trying to reach? For example:

- Management chooses between a range of communication methods depending on what needs to be communicated.
- The method of communication considers the subject, timing, audience, and nature of communication.
- Methods include press and news releases through public relations channels and more directed approaches such as blogs, social media, and email to reach specific audiences.
- The organization uses social media (such as Facebook and Twitter, if relevant, to promote its policies).

ANNEX B5. MONITORING & EVALUATION

This annex focuses on Component 5 – Monitoring & Evaluation which encompasses the ongoing evaluation of internal control systems and the process of separate evaluations.

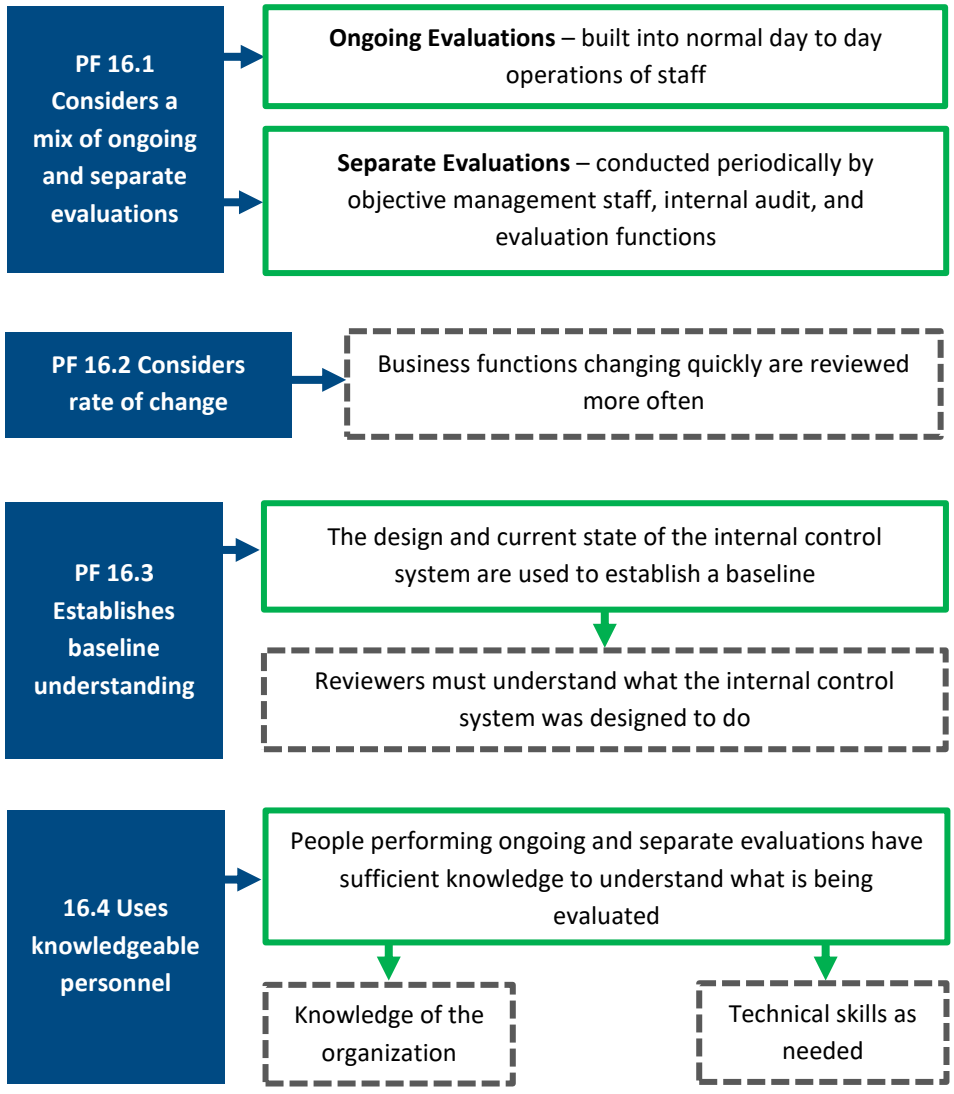
COSO identifies **two principles within this component**, which are listed in the table below.

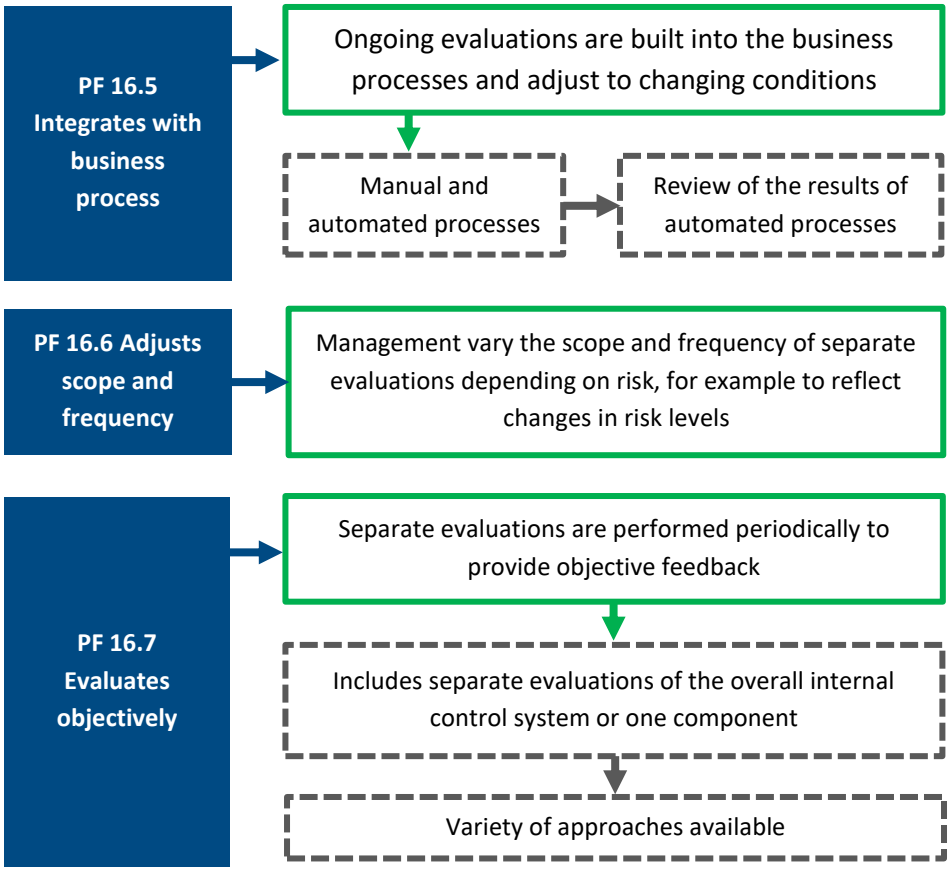
Table 7. The Principles and Points of Focus for Component 5 – Monitoring & Evaluation

Principle		Points of Focus
16	The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	16.1. Considers a mix of ongoing and separate evaluations.
		16.2. Considers rate of change.
		16.3. Establishes baseline understandings.
		16.4. Uses knowledgeable personnel.
		16.5. Integrates with business processes.
		16.6. Adjusts scope and frequency.
		16.7. Evaluates objectively.
17	The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and governing bodies, as appropriate.	17.1. Assesses results.
		17.2. Communicates deficiencies.
		17.3. Monitors corrective actions.

Principle 16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning

Figure 19. Interpretation of Principle 16





Commentary

Internal control is not something that can be assessed one day and forgotten the next. It requires continuous review. Internal control systems therefore need to be monitored – a process that assesses the quality of the system's performance over time. Monitoring ensures that internal control continues to operate effectively. It can be done in two ways – through ongoing monitoring or separate evaluations.

Ongoing evaluation (sometimes referred to as monitoring) activities monitor the effectiveness of internal control in the normal course of operations. Operating as a first line of defense, they include regular management and supervisory activities, comparisons, reconciliations, and other routine actions. The aim of ongoing evaluation activities is to determine how well internal

controls are functioning. These activities should be built into daily, recurring operations performed in the ordinary course of running the organization. They should be performed on a real-time basis and should react dynamically to changing conditions.

Separate evaluations include separate reviews carried out by second line of defense functions responsible for overseeing risk, control, and compliance. Internal audit may also carry out separate evaluations of the overall effectiveness of internal controls as part of systems-based audits.

Management needs to determine an appropriate balance between evaluation activities at the first and second lines**.** Business units that are subjected to too many separate evaluations may result in less ongoing monitoring, reducing the effectiveness of internal control. Risk and rate of change are two factors to consider when determining the frequency of evaluation. Processes which are high risk or are changing frequently may need more frequent, separate evaluations or a higher level of ongoing monitoring.

Criteria for assessing internal control effectiveness:

Has management put in place a mix of ongoing and separate evaluations? For example:

- There is an independent internal audit unit operating to IIA standards, which include reviews of the system of internal control.
- There is an independent audit committee reviewing the effectiveness of ongoing and separate evaluations at all three lines in accordance with best practice.
- There is a robust second line of defense by units responsible for: (a) ensuring effective risk management; and (b) compliance with key policies and standards including environmental standards.

Does management consider rate of change when determining which business functions and processes should be reviewed most often? For example:

- In general, business processes changing quickly are examined more often than those which change slowly.

- All major capital projects are subject to reviews at the planning stage.
- All major IT projects are subject to review in line with COBIT guidance.

Is the design and current state of the internal control system used to establish a baseline? For example:

- Management have a general understanding of the design and current state of the internal control system.
- There is full documentation of the design of the internal control system which is updated to reflect changes in system performance.
- Internal audit assesses and documents the maturity of internal controls as part of their systems-based audits.

Does the organization ensure that people performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated? For example:

- The competence required to carry out ongoing and separate evaluations is specified in job descriptions.
- All staff receive basic training in ongoing evaluations of internal control.
- All internal audit staff must have passed a certain level of competence in competency related examinations.
- Selected staff receive additional training on how best to carry out separate evaluations.

Are ongoing evaluations built into business processes and adjusted to meet changing conditions? For example:

- First line managers review processes based on the results of their performance of control activities.
- The second line of defense review of risks is carried out annually unless business units are subject to rapid change of leadership or business methods.
- The internal audit strategic and annual plans adjust the timing of reviews of business processes to reflect management reviews.

Does management vary the scope and frequency of separate evaluations depending on risk? For example:

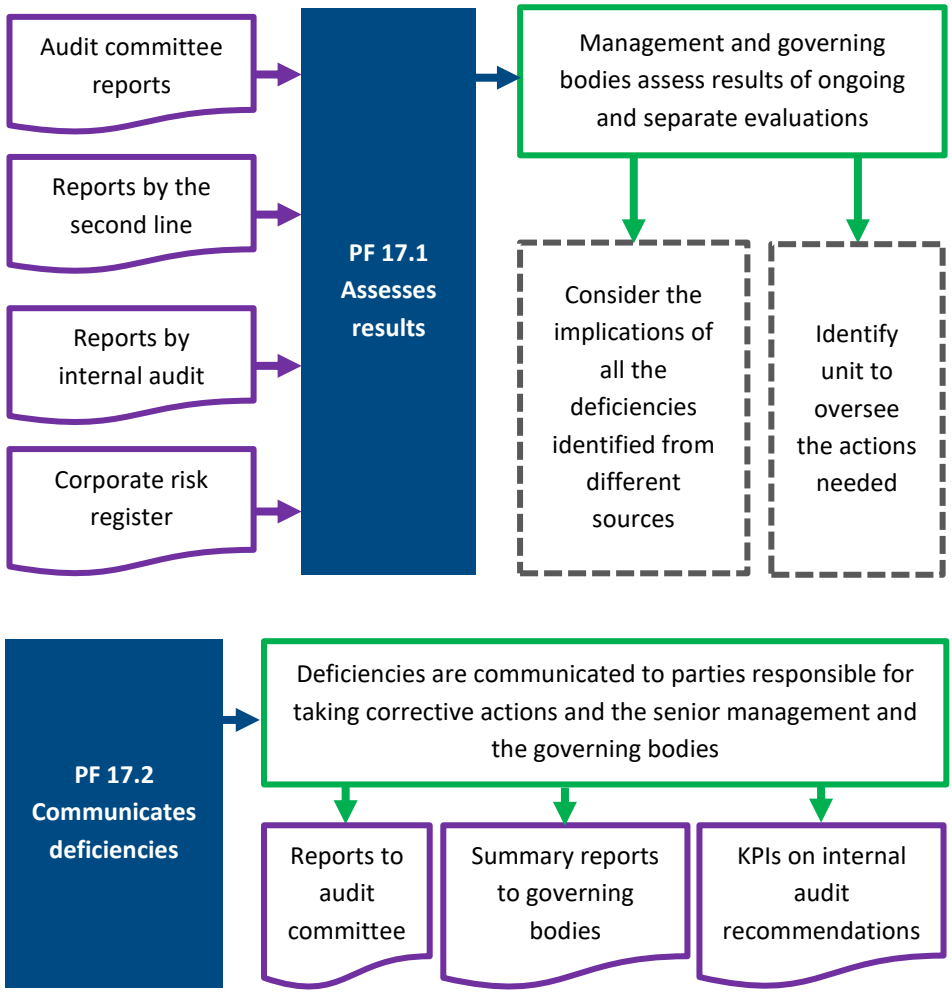
- Management varies the scope of separate evaluations based on size and time since last reviewed.
- The corporate risk register identifies the high risks to the organization and when related policies and processes were last reviewed.
- The internal audit strategic and annual plans are based on risk assessment.

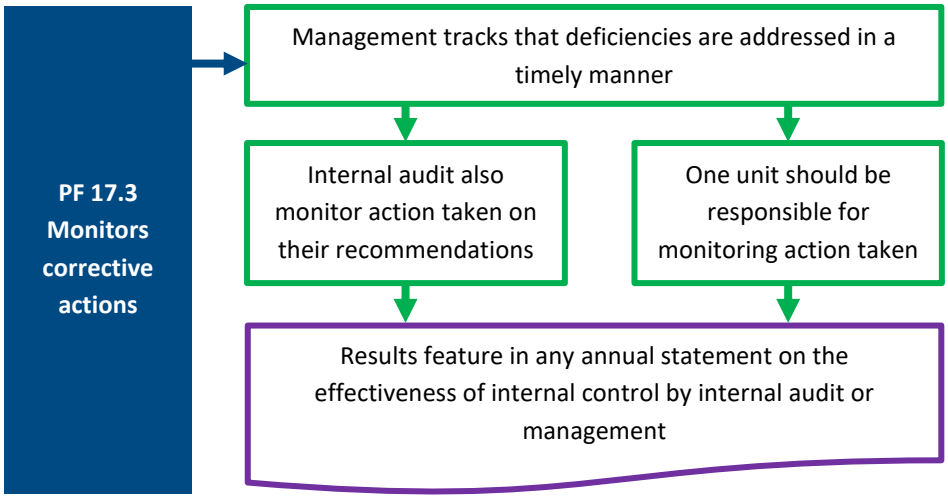
Are separate evaluations performed of the overall system of internal control or one of the five main components? For example:

- Management reviews components of the internal control system on a cyclical basis.
- Internal audit provides an annual assessment of the effectiveness of the system of internal control and each component thereof based on their examinations during the year.
- There is an annual statement of assurance based on certification of the effectiveness of internal control by individual managers.

Principle 17. The organization selects, evaluates, and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and governing bodies as appropriate

Figure 20. Interpretation of Principle 17





Commentary

Deficiencies in the internal control system may surface from many sources, including management monitoring at the first line of defense, oversight by the second line of defense, and evaluations by internal audit at the third line of defense. Deficiencies may also arise from reviews by the external auditor (usually the SAI) or by a financial inspection body[7]. A deficiency can be defined as a condition within an internal control system worthy of attention. It may represent a perceived, potential, or actual shortcoming of a control.

Deficiencies reported from both internal and external sources should be communicated to parties responsible for taking corrective actions as well as senior management and governing bodies. All deficiencies should be systematically monitored, and appropriate corrective action taken.

Criteria for assessing internal control effectiveness

Do management and governing bodies assess the results of ongoing and separate evaluations of internal control? For example:

[7] To understand the different roles of internal audit, SAI, and financial inspection bodies see the PEMPAL concept paper on cooperation among public sector audit and financial inspection entities *www.pempal.org/knowledge-product/iacop-concept-paper-among-public-sector-audit-and-financial-inspection*

- Management review of internal audit reports on the results of systems-based audits.
- Management review of reports by the second line of defense.
- Analysis of the causes of errors in the financial statements as identified by the SAI (external audit).
- Management review of the audit committee annual report on the effectiveness of internal control.
- Periodic review of the corporate risk register.

Are deficiencies communicated to the parties responsible for taking corrective actions and to senior management and governing bodies? For example:

- All internal audit reports are sent to the organizational units audited for review and to action recommendations made.
- Formal responses are required from the organizational unit audited for all recommendations made.
- Internal audit provides governing bodies with a list of all audit recommendations that have been outstanding (not implemented) for more than one year.

Does management track that deficiencies are addressed in a timely manner? For example:

- There is a focal point in the organization responsible for monitoring internal audit and second line of defense reports/recommendations relating to internal controls.
- Management reports to governing bodies on the reasons why internal audit recommendations have been outstanding for more than one year.
- Management provides an annual statement on the effectiveness of internal control to its governing bodies.

ANNEX C. ASSESSING THE MATURITY OF INTERNAL CONTROLS

This annex presents a framework for assessing the maturity of internal controls at four levels drawing on the criteria developed by PEMPAL for each principle and the points of focus as presented in Annexes B1-B5.

For most principles the levels are cumulative, with criteria at levels 3 and 4 being additional to that in level 2. In some situations, the maturity is determined by the extent to which the criteria have been applied, for example the application of the three lines model under PF 3.2.

Principle 1. The organization demonstrates a commitment to integrity and ethical values

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF1.1 Sets the tone at the top			
Behavior, values and operating style of senior management are not known by staff.	Staff have a general awareness of senior management behavior and operating styles.	Senior management inform all staff about their operating style and expected behavior. Values are published and well understood across the whole organization.	Managers have demonstrably high standards of personal behavior. They "walk the talk".

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 1.2 Establishes standards of conduct			
Minimal or no codes of conduct for staff. No ethical standards established.	Key codes of conduct exist and are made available to staff. Clear policies exist on fraud and corruption, sexual harassment, and whistleblower protection.	Staff are automatically reminded of the main standards of behavior expected as part of regular training actions.	Staff at all levels have a common understanding of standards expected. The *"way we do things around here"* is known to all staff.
PF1.3 Checks adherence to standards of conduct			
No or limited reviews of the application of codes of conduct.	Management reviews of standards in place. Investigations undertaken of standards met.	Checks are part of the annual performance assessment process.	360-degree reporting includes assessment of adherence to codes of conduct by peers and subordinates.
PF 1.4 Addresses deviations promptly			
No or limited disciplinary actions taken.	Data is kept on all deviations from the expected standards. Management are committed to taking action for all cases of deviations from standards expected.	All staff are notified each year of all disciplinary actions taken against staff.	Most staff believe that action will be taken against all those who fail to meet expected standards.

Principle 2. Governing bodies demonstrate independence from management and exercise oversight of the development and performance of internal control

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF2.1 Establishes oversight responsibilities			
Oversight arrangements are not defined.	There is a legal framework that clearly defines the oversight bodies for the organization.	Oversight includes an independent audit committee.	Oversight arrangements recognized as meeting the highest international standards.
PF2.2 Has access to relevant skills			
Oversight arrangements are not defined.	There is a clear process for appointing or recruiting members of governing bodies. Necessary skills and relevant experiences are defined and match the objectives of the organization.	Governing body consists of members with various skills and competencies that are appropriate (education and qualification).	Governing body has access to independent expertise as necessary. Governing body demonstrably supports the independence of internal audit as the third line of defense.

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF2.3 Operates Independently			
Oversight arrangements are not defined.	There is clear separation of the management decision making role from the oversight/advisory role.	The information required to exercise oversight is collected on time and reported in an accurate and reliable manner.	Oversight arrangements have been evaluated for efficiency and effectiveness by the SAI.
PF2.4 Provides oversight of the system of internal control			
Oversight arrangements are not defined.	There is an established system of internal control oversight. Management determines which information should be reported to governing bodies.	There are independent criteria for reporting internal control issues to governing bodies. There is a system established for providing a declaration concerning internal control system status within the organization.	There is an annual internal audit opinion on the effectiveness of internal control in the organization. The audit committee provides a public report on the effectiveness of internal control.

Principle 3. Management establishes, with governing body oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 3.1 Considers all structures of the organization			
The organizational structure is not clearly defined or easy to understand.	There is an approved organization structure. The structure established is clear and easy to understand.	Relationships with external partners are clearly defined by management. There are contracts in place for outsourced service providers that clearly specify the responsibilities of these providers in relation to internal control.	Governing bodies regularly review the effectiveness of the organizational structure.
PF3.2 Establishes reporting lines			
There is no formal organization chart. There is little or no awareness of the three lines model.	There are formal organization charts that specify reporting lines. There is basic awareness of the roles of the first and second lines.	There are few individuals with dual reporting responsibilities. All three lines are well understood and fully deployed.	The results of the third line are usable and actioned.

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 3.3 Defines, assigns, and limits authorities and responsibilities			
Authorities exist but have not been established for all levels of the organization or are unclear.	There is a clear written statement of delegated authorities of all staff. While these exist, they may not be available for review by all staff.	Staff are provided with manuals or other guidance where the limits of authority are defined.	Internal audit provides assurance on the clarity of authorities and responsibilities.

Principle 4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 4.1 Establishes policies and procedures			
Human resource policies exist without a clear overall strategy for developing people. Very basic human resource policies exist and relate mainly to salaries and allowances.	There is a human resource strategy document which outlines the goals of the human resource policies of the organization.	Circulars, manuals, and guides clearly identify the competence and skills needed for staff; using as necessary career frameworks, competency statements, job descriptions, etc.	Human resource strategy and policies are periodically reviewed by governing bodies.
PF4.2 Evaluates competence and addresses shortcomings			
There is no formal performance appraisal process in place.	There is a formal performance appraisal system which is applied to all staff.	The performance of staff is regularly assessed against the standards of competence expected.	There are formal tests required of the skills of staff in critical functions such as internal audit.

Level 1: Informal *Ad-hoc/Chaotic*	Level 2: Defined *Standard/ Repeatable*	Level 3: Managed & Monitored *Predictable*	Level 4: Optimized *Efficient/ Effective*
PF 4.3 Attracts, develops, and retains individuals			
Staff are recruited without an overall recruitment policy. There are limited training opportunities for staff. There are high levels of staff turnover.	There is a mechanism for recruitment with pre-defined and clear rules. There are clear qualifications required for all staff at the time of recruitment.	There is a training plan for the organization as a whole and personal development plans for individuals. The organization provides mentoring support to develop staff. Promotion requirements within the organization are related to additional skills needed at higher levels of the organization.	There is a mechanism to send staff to international seminars, conferences, and workshops such as PEMPAL. There are mechanisms to reward high levels of staff performance with both financial and non-financial rewards.
PF4.4 Plans and prepares for succession			
There are no succession planning arrangements in place.	The organization has identified key posts that should not be left unfilled.	The organization has identified positions where employee turnover is expected. There is a "succession plan" for filling key posts in the organization.	There is a policy of regular staff rotation to broaden the skills mix available. There is a mentoring program to help identify future leaders.

Principle 5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 5.1 Enforces accountability through structures, authorities, and responsibilities			
There is little or no accountability for internal control action.	Responsibilities are identified and allocated to individuals. There is a performance evaluation system that operates at different levels of the organization and focuses on how managers manage their region / offices / divisions / units.	Employees are aware of their responsibilities through job descriptions or other mechanisms. Responsibilities meet the internal control and business objectives of the organization. Well-understood chains of accountability exist and most staff are held to account for their internal control responsibilities.	Individual objectives are linked to higher-level objectives in the strategy or management plan. All staff are regularly held to account for their internal control responsibilities.

Level 1: Informal *Ad-hoc/Chaotic*	Level 2: Defined *Standard/ Repeatable*	Level 3: Managed & Monitored *Predictable*	Level 4: Optimized *Efficient/ Effective*
PF 5.2 Establishes performance measures, incentives, and rewards			
There are very limited performance measures in place.	There is a policy for setting objectives and KPIs **at the entity level.**	The policy for setting objectives and KPIs **extends to business units and individuals**.	All staff are actively involved in setting their performance objectives and related KPIs.
PF 5.3 Evaluates performance measures, incentives, and rewards for ongoing relevance			
There are very limited performance measures in place.	The second line of defense is responsible for reviewing the relevance of performance measures.	The quality and relevance of performance measures is regularly assessed by internal audit (third line of defense).	Management attest to the relevance of their performance measures.
PF 5.4 Considers excessive pressures			
There are very limited performance measures in place.	There is a formalized procedure/mechanism for measuring the workload of staff which identifies situations of overload or underload and mechanisms to	Management identify staff who are not taking enough time off from their duties. Staff suffering from stress-related illnesses are identified and changes made to workload to reduce such stress.	There are staff counselling arrangements to identify staff facing undue pressures.

Level 1: Informal *Ad-hoc/Chaotic*	Level 2: Defined *Standard/ Repeatable*	Level 3: Managed & Monitored *Predictable*	Level 4: Optimized *Efficient/ Effective*
	address these disparities.		
PF5.5 Evaluates performance and rewards or disciplines individuals			
There is no formal performance appraisal system in place.	There is a formal performance appraisal system which is applied to all staff.	The appraisal system results in formal performance reports. There is consistency between the level of duties undertaken and the rewards provided.	The performance appraisal results in rewarding staff positively and negatively (both financially and non-financial).

Principle 6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 6.1 Operations objectives			
Operational objectives exist in laws and related policy documents but are not captured within an overall strategy for the organization.	There is a high-level strategy for the organization which contains the objectives of the organization as a whole. Organizational objectives reflect management and political level choices on how best to respond to policy challenges.	The high-level strategy is supported by targets and KPIs. Each business unit in the organization sets annual objectives with targets and related KPIs.	Operations objectives form the basis for setting the budget of the organization. There is a clear statement of the overall risk appetite of the organization. Risk tolerance levels are identified for all main objectives and measured through relevant KPIs.

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 6.2 External reporting objectives			
External reporting is ad hoc and unstructured.	The organization maintains records of income and expenditure against the budget allocated and reports on budget outturn to the ministry of finance. Reports on performance are provided when requested by governing bodies.	The organization is required to prepare annual financial statements in line with the accounting standards adopted for the organization as a whole. There is a system for the preparation of annual reports on the performance of the organization against its stated objectives.	There is an automated accounting system that supports the accurate preparation of accounts to reflect underlying transactions to an acceptable level of materiality.
PF 6.3 Internal reporting objectives			
There is limited internal reporting.	Internal reports are prepared by units within the organization when they consider it appropriate to do so.	Internal reports are prepared to an appropriate level of precision and reflect underlying transactions.	Senior management decides what level of internal reporting is appropriate for different aspects of budgeting and financial management.

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 6.4 Compliance objectives			
There is limited awareness of compliance objectives.	There is a policy explaining how managers should set objectives to comply with government-wide standards. Compliance objectives can be wide ranging and include environmental issues, the need for competition, safety and security regulations, and fundamental staffing policies such as minimum rates of pay and harassment.	Compliance objectives are included in the high-level strategy for the organization. The organization meets all main compliance objectives.	There is a high level of awareness in the organization of the importance of compliance objectives.

Principle 7. The organization identifies risks to the achievement of its objectives across the organization and analyzes risks as a basis for determining how the risks should be managed

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 7.1 Includes organization and main structures			
There is no formal risk assessment in place, so management reacts to risks and opportunities as they arise.	There is a requirement for formal risk assessment processes throughout the organization. The majority of organizational units carry out some form of risk assessment.	There are separate risk registers for regional and headquarter offices. There are separate risk registers for organizational units operating as self-contained not for profit agencies who charge for their services or products.	There are separate risk registers for every operating unit and a corporate risk register for the main risks facing the organization as a whole.
PF 7.2 Analyzes internal and external factors			
There is no formal risk assessment in place.	There is a formal risk assessment policy that explains how to identify and assess the impact of internal and external events.	Staff are provided with examples of the types of internal and external events that may lead to risks and opportunities.	Staff are trained in how to carry out a formal risk assessment.

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 7.3 Involves appropriate levels of management			
Senior management may not be involved in responding to risks arising.	Risk assessments may involve staff at different levels in some organizational units.	In most units, staff at different levels normally hold separate risk assessment meetings.	Risk assessments are always carried out during meetings involving staff at all levels.
PF 7.4 Estimates significance of risks identified			
The significance of risks arising may not be fully understood.	The risk register contains assessments of the **likelihood** and **impact** of all risks identified.	The **velocity** of risk is also considered and measured during the risk assessment process.	There is a common system for scoring risks across the organization to determine the highest risks facing the organization by measuring likelihood, impact, and velocity.

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 7.5 Determines how to respond to risk			
Management reacts to risks and opportunities as they arise.	The risk assessment policy provides for four possible risk responses - avoiding, transferring (sharing), accepting, or reducing (controlling) risk.	The risk register includes the agreed risk response and references to control activities as appropriate.	Management ensures that risk responses are cost-effective by making appropriate use of all four risk responses.

Principle 8. The organization considers the potential for fraud in assessing risks to the achievement of objectives

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 8.1 Considers various types of fraud			
There is minimal understanding of the causes of fraud and corruption.	There is an anti-fraud and anti-corruption policy that explains to staff the different ways that fraud and corruption may occur, for example theft, deception, inappropriate use of assets, fraudulent reporting, management override of controls, and illegal acts.	All staff are provided with basic training on fraud and corruption awareness.	Actual cases of fraud and corruption identified are reported to all staff to raise awareness of ways that fraud may be committed.
8.2 Assesses incentives and pressures			
There are limited assessments of the incentives and pressures to commit fraud.	There is adequate segregation of duties to ensure that managers cannot take decisions on their own: the four-eyes principle is followed.	There are periodic checks for conflicts of interest in making decisions.	All staff in managerial positions are required to provide a declaration of their financial status each year.

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 8.3 Assesses opportunities			
There are limited assessments of the opportunities to commit fraud.	Management includes assessments of fraud opportunities during risk assessment processes.	The factors that lead to high turnover of staff in key roles have been identified. Management identify high-risk financial positions for additional levels of review.	Management publicize all cases of fraud and corruption to increase the fear of detection of fraud or corrupt acts.
PF 8.4 Assesses attitudes and rationalizations			

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
There is limited consideration of attitudes and rationalizations.	All staff have had a minimum level of training in fraud and corruption awareness.	Risk register includes areas of major risk of fraud and corruption.	There are periodic checks of personal behavior. An internal committee on anti-fraud practices is in place. Internal audit undertakes third line reviews of the fraud and corruption risks.

Principle 9. The organization identifies and assesses changes that could significantly impact the system of internal control

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 9.1 Assesses changes in the external environment			
There is limited consideration of major changes in the	Management considers changes resulting from resource	Management considers changes in (a) political	There is a unit within the organization that is

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
external environment.	availability (reduction in the civil service staffing numbers or other budgetary resources). Management considers changes in external environment beyond the control of the organization such as severe weather impacts.	leadership (government); (b) the global economic/political/geographical directions; (c) the regulatory framework; (d) major restructuring of the public sector – merger of ministries/agencies; and (e) ongoing or expected changes in public administration practices or PFM/PIC.	responsible for monitoring change.

Level 1: Informal *Ad-hoc/Chaotic*	Level 2: Defined *Standard/ Repeatable*	Level 3: Managed & Monitored *Predictable*	Level 4: Optimized *Efficient/ Effective*
PF 9.2 Assesses changes in the business model			
There is limited consideration of major changes in the business model.	Management considers major change projects resulting in changes in the key structures, functions, roles, services, and products delivered. Management considers changes to new technology -disruptive technologies including mobile data and their impact on internal processes and internal control.	There are clear processes to deal with information and communication technologies/ cyber security risks and operational availability through business continuity planning and/or disaster recovery planning. Management considers the staffing capacity relevant to new roles and objectives.	There is a unit within the organization that is responsible for monitoring change.
PF 9.3 Assesses changes in leadership			
There is limited consideration of changes in leadership.	Management considers the impact of new managers with a new vision of PIC and different attitudes towards control.	Management considers the impact of high levels of turnover in management positions generally.	There is a unit within the organization that is responsible for monitoring change.

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
		There are specific jobs which have formal handover arrangements to ensure that information on key control activities are passed from one manager to another.	

Principle 10. The organization develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 10.1 Integrates with risk assessment			
There is no formal risk assessment to integrate with controls	Most risk registers include some references to the control activities that are intended to reduce inherent risks to an acceptable level.	There are references to control activities in all risk registers.	There is a corporate risk register which identifies the major risks facing the organization and the key control activities put in place to address those risks.
PF 10.2 Considers organization-specific factors			
There is little consideration of organizational factors such as the levels of decentralization and IT automation when designing controls.	The organization has a basic understanding of the first and second lines when designing control activities.	The organization understands and applies the concept of the three lines when designing its control activities	The organization uses the three lines to establish effective controls over decentralized activities: there is a common set of guidance for managers of regional offices on the roles of

Level 1: Informal *Ad-hoc/Chaotic*	Level 2: Defined *Standard/ Repeatable*	Level 3: Managed & Monitored *Predictable*	Level 4: Optimized *Efficient/ Effective*
			the second and third lines in relation to regional activities.
PF 10.3 Determines relevant business processes			
Control activities are defined and applied in a standard manner in the public sector, regardless of the business process.	There is a basic understanding of which business processes require control activities. These include policies specifying which types of contracts require competitive bidding and processes critical to the preparation of accurate financial statements.	Business processes objectives cover **completeness** (that all transactions are processed), **accuracy** (that transactions are correctly valued and recorded) and **validity** (that transactions represent legitimate expenditure or revenue of the organization and have been properly authorized in accordance with the budget.)	There is a thorough understanding of which business processes require control activities.

Level 1: Informal *Ad-hoc/Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 10.4 Evaluates a mix of control activity types			
Management does not evaluate the mix of control activities.	There is a clear understanding of the differences between preventive and detective controls and a balanced approach to the use of each type of control.	Management makes full use of different types of controls e.g. reconciliations, physical controls, authorizations & approvals, and third-party verifications. Basic attempts are made to reduce costs through limiting checks of transactions below a certain financial value.	Management assesses the cost-effectiveness of different control activities before determining which control activities to implement.
PF 10.5 Considers at what level control activities are applied			
Management does not consider the level of control activities.	There are separate requirements for control activities at the transaction and supervisory levels in most business processes.	There are separate requirements for control activities at the transaction and supervisory levels in all business processes.	Wherever possible management focuses key controls at the supervisory level.

Level 1: Informal *Ad-hoc/Chaotic*	Level 2: Defined *Standard/ Repeatable*	Level 3: Managed & Monitored *Predictable*	Level 4: Optimized *Efficient/ Effective*
PF 10.6 Addresses segregation of duties			
There is limited segregation of duties.	Management have identified four key functions that must be segregated – (1) authorizing expenditure, (2) certifying goods received and approving payment, (3) making payments, and (4) recording transactions.	There are additional checks by a second line oversight unit when segregation is not practical because of the size of the business unit.	Internal audit reviews the adequacy of segregation of duties as part of the third line of defense.

Principle 11. The organization selects and develops general control activities over technology to support the achievement of objectives

Level 1: Informal *Ad-hoc/ Chaotic*	Level 2: Defined *Standard/ Repeatable*	Level 3: Managed & Monitored *Predictable*	Level 4: Optimized *Efficient/ Effective*
PF 11.1 Determines dependency between the use of technology in business processes and technology general controls			
There is no assessment of the dependency on IT.	There is a separate IT policy which identifies all the main elements of IT in use across the organization. The policy includes consideration of client/server technology, cloud-based data storage, end-user computing, mobile devices, and operating systems.	Management understands and determines the dependency and linkage between business processes automated controls activities and technology general controls.	Management uses the COBIT 5 framework for the governance and management of entity-wide IT systems and processes.
PF 11.2 Establishes relevant technology infrastructure control activities			
There are limited controls over technology infrastructure.	Management selects and develops control activities over technology infrastructure, which are designed to ensure completeness,	There are clearly defined daily back-up and recovery procedures for all key data in the organization.	There are procedures such as back-up electricity generators to ensure a high level of availability of

Level 1: Informal *Ad-hoc/ Chaotic*	Level 2: Defined *Standard/ Repeatable*	Level 3: Managed & Monitored *Predictable*	Level 4: Optimized *Efficient/ Effective*
	accuracy, and availability of technology processing.		corporate IT systems.

PF 11.3 Establishes relevant security management process control activities

There are minimal IT security controls.	There are basic control activities to restrict access rights to authorized users in line with their job responsibilities by using physical controls over access to offices with IT infrastructure and user passwords to access IT systems.	There are strong IT security controls which include regular changes to access passwords and the use of strong password naming conventions.	There are strict and automatic limitations of user access to only those applications that are essential for the performance of duties.

PF 11.4 Establishes relevant technology acquisition, development, and maintenance process control activities

There are no special procedures for controlling IT acquisition development and maintenance processes.	A specialized IT unit is responsible for acquisition, development, and maintenance of IT processes.	A high-level committee oversees IT developments for the organization as a whole.	The organization follows the COBIT 5 framework for all its IT acquisitions and disposals.

Principle 12. The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action

Level 1: Informal *Ad-hoc/ Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 12.1 Establishes policies and procedures to support deployment of management's directives.			
There are no clear policies and procedures related to control activities.	For most controls, there is (a) a set of policies which identify what should be done in terms of control and (b) documentation of the procedures (steps) to be followed to implement the policy.	Policy and procedures are documented for all controls.	There is mandatory training for staff on implementing key controls.
PF 12.2 Establishes responsibility and accountability for executing policies and procedures			
There is no clear allocation of responsibility for control activities.	Responsibility for most elements of the control process is allocated to named individuals.	All elements of the control process are allocated to named individuals.	Managers and staff receive training on the importance of implementing controls thoughtfully, conscientiously, and consistently.

Level 1: Informal *Ad-hoc/ Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 12.3 Performs in a timely manner			
There are no standards for the timeliness of control actions.	There are predefined standards for the time required to carry out critical control activities such as the time to process payments or the dates when bank reconciliations must be completed. However, standards are not always followed.	There is a high level of compliance with timeliness standards for control activities.	There are regular reports to supervisors and managers on the timeliness of business processing.
PF 12.4 Takes corrective action			
Corrective action may not always be taken.	Procedures exist for taking corrective action and are followed most of the time.	Procedures for corrective action are always taken. Higher-level supervisors must personally authorize the processing of all transactions that have been rejected by system validation checks.	There are regular reports to supervisors and managers on areas where corrective action has not been taken.

Level 1: Informal *Ad-hoc/ Chaotic*	Level 2: Defined *Standard/ Repeatable*	Level 3: Managed & Monitored *Predictable*	Level 4: Optimized *Efficient/ Effective*
PF 12.5 Performs using competent personnel			
There is no guarantee that competent staff will be assigned to control activities.	The level of competence and authority required to carry out each control activity is clearly defined and usually applied.	Managers and staff are aware of the competence and authority needed to carry out controls effectively.	Expenditure over predetermined financial limits must be authorized by more senior staff.
PF 12.6 Reassesses policies and procedures			
Policies and procedures may not be reassessed.	Management reviews the relevance of control activities, but this may not be done on a regular basis.	There is a clear timeframe for reviews of the continued relevance of control activities. Senior management agree with internal audit the frequency with which they carry out systems-based audits of key business processes.	All financial delegations have a sunset clause which specifies the date when they must be reviewed to determine their continued relevance.

Principle 13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control

Level 1: Informal *Ad-hoc/ Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 13.1 Identifies information requirements			
The information requirements of internal control are unclear.	The information needs of the most important controls are specified in internal manuals and procedures. The communication process of providing and sharing information works most of the time.	The information needs of all controls are specified in internal manuals and procedures. The communication process functions very well.	Individual staff are assigned responsibility for (a) defining information needs and (b) generating the data to meet these needs.
PF 13.2 Captures internal and external sources of data			
The process of capturing internal and external sources of data does not work well.	The organization has basic systems for the collection of internal data (emails, financial reports, and budgets) and external data (parliamentary debates and press coverage.	The organization has more sophisticated systems for the collection of internal and external data. There is a single system for processing all accounting data in the organization.	The process of capturing and communicating information is highly automated.

Level 1: Informal *Ad-hoc/ Chaotic*	Level 2: Defined *Standard/ Repeatable*	Level 3: Managed & Monitored *Predictable*	Level 4: Optimized *Efficient/ Effective*
PF 13.3 Processes relevant data into information			
There is limited processing of data into information. Only raw data is communicated.	The organization has information systems to process critical data into usable information for managers. These exist for some but not all business processes.	The organization has information systems to process critical data into usable information for managers for all business processes.	Data that does not meet criteria for accuracy are not included in management reports.
PF 13.4 Maintains quality throughout processing			
There are limited checks on the quality of processing.	The most important systems are designed to produce timely, current, accurate, complete, accessible, protected, verified, and retained information.	All systems are designed to produce timely, current, accurate, complete, accessible, protected, verified, and retained information.	All financial data entry systems have ways of validating original data (e.g. through double keying, supervisor sign off, etc.) before the data is accepted for processing.
PF 13.5 Considers costs and benefits			
There is no consideration of the cost and benefits of collecting information.	For main business processes, management reviews the nature, quantity, and precision of information	Management reviews costs and benefits for all business processes. The organization identifies the	Internal audit carries out periodic audits of the value for money of information systems.

Level 1: Informal *Ad-hoc/ Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
	communicated and checks whether the cost of collecting information is consistent with the benefits gained.	cost of producing major reports on internal control effectiveness, including the direct costs of internal audit examination.	Action is taken to stop collecting information that is no longer beneficial.

Principle 14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control

Level 1: Informal *Ad-hoc/ Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 14.1 Communicates internal control information			
There are few formal processes in place to ensure staff understand their internal control responsibilities.	The internal control responsibilities of all staff are laid down in manuals and guidelines. Policies and procedures for internal control are specified in manuals and guidance available to all staff.	Staff have been trained on the importance, relevance, and benefits of effective internal control.	There are controls to ensure that key information is shared.
PF 14.2 Communicates with governing bodies			
There is limited communication on internal control between management and governing bodies.	There are formal and informal communication channels between management and governing bodies. Management mainly uses formal communication channels.	Management makes use of both formal and informal communication channels. Governing bodies have direct access to staff of the	The audit committee presents an annual report of its activities to governing bodies. Copies of internal audit reports are made available

Level 1: Informal *Ad-hoc/ Chaotic*	Level 2: Defined *Standard/ Repeatable*	Level 3: Managed & Monitored *Predictable*	Level 4: Optimized *Efficient/ Effective*
		organization as needed.	to governing bodies.
PF 14.3 Provides separate communication lines			
There are no separate communication lines.	There is a whistleblower hotline to provide a fail-safe mechanism to enable confidential communication when normal channels are inoperative or ineffective.	There is a policy for the protection of all whistleblowers. Management extensively promote the existence of the hotline and the protection provided to whistleblowers.	There is an annual report on the effectiveness of the whistleblower hotline, including statistics showing the extent of use and action taken to address issues raised.
PF 14.4 Selects relevant method of communication			
The organization uses a limited number of traditional ways of communicating with staff.	Management chooses between a range of traditional communication methods depending on what needs to be communicated. Such methods include emails, presentations, training courses,	Management has more ways of communicating with staff, for example: management dashboards, webcasts, videos social media postings, and text messages.	Management reinforces key messages with their own actions – they "walk the talk".

Level 1: Informal *Ad-hoc/ Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
	and the formal appraisal process.	There are regular all staff meetings on important changes in the organization's functions, structure, and operational objectives.	

Principle 15. The organization communicates with external parties regarding matters affecting the functioning of internal control

Level 1: Informal *Ad-hoc/ Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 15.1 Communicates to external parties			
There is limited communication with external parties	There are processes in place to communicate relevant and timely information to external parties, including parliament, partners, regulators, and other external parties.	External communication includes regular reports on budgetary outturn and an annual report on the financial statements of the organization.	There are public reports on the performance of the organization in relation to its operational objectives.
PF 15.2 Enables inbound communication			
Management does not encourage inbound communication.	Management has established open communication channels that allow input from parliament, beneficiaries or clients, suppliers, external auditors, regulators, and others.	Reports of the results of external audits by the SAI are sent to parliament and published in the official gazette.	All complaints from beneficiaries or external suppliers are recorded for follow up and action.

Level 1: Informal *Ad-hoc/ Chaotic*	Level 2: Defined *Standard/ Repeatable*	Level 3: Managed & Monitored *Predictable*	Level 4: Optimized *Efficient/ Effective*
PF 15.3 Communicates with governing bodies			
There is limited communication with governing bodies on the results of assessments by external parties.	Management ensures that relevant information from assessments conducted by external parties is communicated to governing bodies. These may include reports by regulators and or auditors.	The annual accounts, including the report of the external auditor, are presented directly to governing bodies (or audit committee if one exists) for consideration and review.	There is agreement between management and the governing bodies on what information related to assessments by external parties must be provided to governing bodies and the timeframe for this.
PF 15.4 Provides separate communication lines			
There are no separate communication lines.	Separate communication channels, such as whistleblower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal	There is a policy for the protection of all whistleblowers. Management extensively promote the existence of the whistleblower hotline and the protection provided to whistleblowers.	Management issues a public report on the effectiveness of the whistleblower hotline, including statistics showing the extent of use and action taken

Level 1: Informal *Ad-hoc/ Chaotic*	Level 2: Defined *Standard/ Repeatable*	Level 3: Managed & Monitored *Predictable*	Level 4: Optimized *Efficient/ Effective*
	channels are inoperative or ineffective.		to address issues raised.
PF 15.5 Selects relevant methods of communication			
The organization has limited methods of external communication.	Management chooses between a range of traditional communication methods depending on what needs to be communicated. The method of communication considers the subject, timing, audience, and nature of communication. Methods include press and news releases through public relations channels.	Management has more directed approaches such as blogs, social media and email to reach specific audiences.	The organization uses social media such as Facebook and Twitter to promote its policies.

Principle 16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning

Level 1: Informal *Ad-hoc/ Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 16.1 Considers a mix of ongoing and separate evaluations			
There are limited ongoing and separate evaluations.	There is an independent internal audit unit operating to IIA standards, which include reviews of the system of internal control.	There is an independent audit committee reviewing the effectiveness of ongoing and separate evaluations at all three line of defense in line with best practice.	There is a robust second line of defense by units responsible for: (a) ensuring effective risk management; and (b) compliance with key policies and standards including environmental standards.
PF 16.2 Considers rate of change			
There are limited ongoing and separate evaluations.	In general, business processes changing quickly are examined more often than those which change slowly.	All major capital projects are subject to reviews at the planning stage.	All major IT projects are subject to review in line with COBIT guidance.

Level 1: Informal *Ad-hoc/ Chaotic*	Level 2: Defined *Standard/ Repeatable*	Level 3: Managed & Monitored *Predictable*	Level 4: Optimized *Efficient/ Effective*
PF 16.3 Establishes baseline understanding			
There are limited ongoing and separate evaluations.	Management have a general understanding of the design and current state of the internal control system.	There is full documentation of the design of the internal control system which is updated to reflect changes in system performance.	Internal audit assesses and document the maturity of internal controls as part of their systems-based audits.
16.4 Uses knowledgeable personnel			
There are limited ongoing and separate evaluations.	The competence required to carry out ongoing and separate evaluations is specified in job descriptions.	All staff receive basic training in ongoing evaluations of internal control. All internal audit staff must have passed a certain level of competence to undertake audit work.	Selected staff receive additional training on how best to carry our separate evaluations.
PF 16.5 Integrates with business process			
There are limited ongoing and separate evaluations.	First line managers review processes based on the results of their performance of control activities.	The second line of defense review of risks is carried out annually unless business units are subject to rapid change of leadership or business methods.	The internal audit strategic and annual plans adjust the timing of reviews of business processes to reflect management reviews.

Level 1: Informal *Ad-hoc/ Chaotic*	Level 2: Defined *Standard/ Repeatable*	Level 3: Managed & Monitored *Predictable*	Level 4: Optimized *Efficient/ Effective*
PF 16.6 Adjusts scope and frequency			
There are limited ongoing and separate evaluations.	Management varies the scope of separate evaluations based on size and time since last reviewed.	The corporate risk register identifies the high risks to the organization and when related policies and processes were last reviewed.	The internal audit strategic and annual plans are based on risk assessment.
PF 16.7 Evaluates objectively			
There are limited ongoing and separate evaluations.	Management reviews components of the internal control system on a cyclical basis.	Internal audit provides an annual assessment of the effectiveness of the system of internal control and each component thereof based on their examinations during the year.	There is an annual statement of assurance based on certification of the effectiveness of internal control by individual managers.

Principle 17. The organization selects, evaluates, and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the governing bodies as appropriate

Level 1: Informal *Ad-hoc/ Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
PF 17.1 Assesses results			
There are limited reviews of the results of ongoing and separate evaluations.	Management review of internal audit reports of the results of systems-based audits.	Management review of reports by the second line of defense. Analysis of the causes of errors in the financial statements as identified by the SAI (external audit).	Management review of audit committee annual report on the effectiveness of internal control. Periodic review of the corporate risk register.
PF 17.2 Communicates deficiencies			
Deficiencies are not communicated to governing bodies.	All internal audit reports are sent to the audited organizational units for review and to action	Formal responses are required from the audited organizational unit for all	Internal audit provides governing bodies with a list of all audit recommendations that have been

Level 1: Informal *Ad-hoc/ Chaotic*	**Level 2: Defined** *Standard/ Repeatable*	**Level 3: Managed & Monitored** *Predictable*	**Level 4: Optimized** *Efficient/ Effective*
	recommendations made.	recommendations made.	outstanding (not implemented) for more than one year.
PF 17.3 Monitors corrective actions			
There is no monitoring of corrective action.	There is a focal point in the organization responsible for monitoring internal audit and second line of defense reports/recommendations relating to internal controls.	Management reports to governing bodies on the reasons why internal audit recommendations have been outstanding for more than one year.	Management provides an annual statement on the effectiveness of internal control to its governing bodies.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Economic Affairs SECO

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

MINISTRY OF FINANCE
OF THE RUSSIAN FEDERATION