# PEMPAL Discussion Paper on the Control Environment

# Introduction

1. There are five components to COSO based internal control as shown in the diagram below:

|  |
| --- |
| Figure 1 The five Components of COSO |

1. **This discussion paper 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.
2. **The component contains five principles** identified by COSO:

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

2 ‐ The Governing Bodies demonstrate independence from management and exercises oversight of the development and performance of internal control.

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

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

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

## Principles and Points of Focus for the Control Environment

1. To help people understand the nature of each principle, COSO has identified explanatory areas of focus for each principle. (These are known as “points of focus” in COSO guidance). See figure 2.

|  |
| --- |
| Figure 2 The Principles and Points of Focus for Component 1 – The Control Environment. |

1. Annex 1 lists the principles and “points of focus” in detail for the five principles noted above. The section below considers each principle. There is a diagram for each principle illustrating how the points of focus might be interpreted. This is followed by a short commentary and a list of the questions that might be asked by Internal Audit when reviewing the control environment. The draft document will be updated to reflect discussion at the Georgia meeting.

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

|  |
| --- |
| Figure 3: Interpretation of principle 1 |

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 organisation provided its staff with guidance that explains the standards expected. This should include provisions to protect individuals that report wrongdoing (known as whistle-blowers). Having established clear standards of behaviour it is essential that actual behaviour is reviewed and that any deviations are fully investigated with discipline action when needed.
2. Possible questions for auditors:
* Does the organization have one or more policies that define expected standards of behavior?
* Are staff regularly reminded of the need to carry out their duties with integrity in ways that that meets the ethical standards established?
* Are there processes in place to evaluate the performance of individuals and teams in meeting the ethical standards expected?
* Are deviations from the standards expected investigated and is action taken to address shortcomings?

## Principle 2: The Governing Bodies demonstrate independence from management and exercise oversight of the development and performance of internal control.

|  |
| --- |
| Figure 4: Interpretation of principle 2 |

1. 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. Options for oversight can include:
* Parliamentary Committees tasked with overseeing the actions of the entity;
* A Government Department providing oversight of subsidiary bodies (for example the Department of Health overseeing hospitals).
* Ministerial oversight mechanisms.

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 the Governing Bodies must operate independently and have the skills to work effectively. It is also essential that the Governing Bodies actually review the operation of internal controls. This can often be done by review of the reports generated at the Second and Third lines of defence.

1. Possible questions for auditors:
* Is there an independent Board of Directors responsible for oversight of management?
* If not, what level of independent oversight exists of the actions of management?
* Does the Board (or other governing body) have the expertise to oversee the work on the Organization?
* Is the Board (or other governing body) independent of management?
* Does the Board (or other governing body) provide oversight of management’s implementation of the system of internal control?

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

|  |
| --- |
| Figure 5: Interpretation of principle 3 |

1. Commentary. The way an organization is organized 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 organisation charts. There should be a clear definition of the authority and responsibility of all the individuals in the organisation. These should be clearly laid out in manuals and guides. Many organisations also have separate lists of all delegated authorities. Current best practice is to use the “three lines of defence” as an internal organisational model. These differentiate between (b) 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 internal control and review adherence to such guidance; and (c) Independent functions such as internal audit who provide a third line of defence by assessing and reporting on the effectiveness of internal control.
2. Possible questions for auditors:
* Has management established clear internal structures including as necessary subsidiary units such as regional offices?
* Has management clearly defined its relationships with its external partners?
* Are there contracts in place for outsourced service providers that special clearly the responsibilities of these providers in relation to internal control?
* Do internal structures result in clear reporting lines?
* Are there formal organization charts that specify reporting lines?
* Is there a clear statement of delegated authorities in manuals or guides?
* Does the organization understand and use the concept of three lines of defence in maintaining effective internal control?
* How effective are actions taken at the second and third line of defence?

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

|  |
| --- |
| Figure 6: Interpretation of principle 4 |

1. Commentary. You need good people to implement internal controls effectively. Organizations who have a high turnover of staff or who cannot attract and retain staff of the right calibre will have difficulty running effective internal control systems. It is also important to prepare for the succession of people in important posts.
2. Possible questions for auditors:
* Is there a clear statement of the Human Resource policies and practices of the organization, for example through circulars, manuals and guides?
* Does the organization clearly identify the competence and skills needed for its staff, for example through career frameworks, competency statements, job descriptions etc?
* Can the organization attract staff of sufficient quality to perform its functions?
* Does the organization provide the mentoring and training support needed to develop staff?
* How effective is the organization at retaining key staff?
* Has the organization identified key posts that should not be left unfilled?
* Is there a “succession plan” for filling key posts in the organization?

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

|  |
| --- |
| Figure 7: Interpretation of principle 5  |

1. 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.
2. Possible questions for auditors:
* Is there a staff performance management policy that provides for staff to be regularly assessed in terms of achieving their objectives?
* Does this result in formal performance reports?
* Are all staff (including managers) included in the staff performance management system?
* Does management consider excessive pressures that may impact the way people undertake their duties?

## Conclusion – to be added after PEMPAL meeting

# Annex A: Internal Control Principles and Points of Focus

1. COSO has provided guidance for each of the 17 principles which includes supporting details which it calls “points of focus”. The following table includes the “Points of Focus” that may be relevant in understanding the application of the principles to the Public Sector.

| PRINCIPLES | POINTS OF FOCUS |
| --- | --- |
| Control Environment |
| 1 ‐ The organization demonstrates a commitment to integrity and ethical values. | Sets the tone at the top The Governing Bodies[[1]](#endnote-1) and management at all levels demonstrate through their directives, actions and behaviour the importance of integrity and ethical values to support the functioning of the system of internal control.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.Evaluates 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.Addresses deviations in a timely manner. 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. | Establishes oversight responsibilitiesThe Governing Bodies identify and accept their oversight responsibilities in relation to established requirements and expectations.Applies relevant expertiseThe 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.Operates independently The Governing Bodies have sufficient members who are independent from management and objective in evaluations and decision-making.Provides oversight on the system of internal control The Governing Bodies retain oversight responsibility for management’s design, implementation, and conduct of internal controlFor 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 establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | Considers all structures of the organisation 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.Establishes reporting linesManagement designs and evaluates lines of reporting for each organisational structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the organization.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 organisation:* Governing Bodies: retain authority over significant decisions and reviews 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 the organization and its subunits;
* *Personnel* - understands the organization’s standards of conduct, assessed risks to objectives, and the related control activities at their respective levels of the organisation, the expected information and communication flow and monitoring activities relevant to their achievement of objectives;
* *Outsourced service providers* – Adheres to management’s definition of the scope of authority and responsibility for all non-employees engaged.
 |
| 4 ‐ The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | Establishes policies and practicesPolicies and practices reflect expectations of competence necessary to support the achievement of objectives.Evaluates competence and addresses shortcomings**.** The Governing Bodies and management evaluate competences across the organisation and in outsourced services providers in relation to established policies and practices, and act as necessary to address shortcomings.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.Plans and prepares for successionSenior management and the Governing Bodies develop contingency plans for assignments of responsibility important for Internal Control. |
| 5 ‐ The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | **Enforces accountability through structures, authorities, and responsibilities** Management and the Governing Bodies establish the mechanism to communicate and hold individuals accountable for performance of internal control responsibilities across the organization and implement corrective actions as necessary. **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.**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.**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.**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. |

1. 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. [↑](#endnote-ref-1)