

**PEMPAL GLOSSARY OF TERMS:  
INTERNAL CONTROL**

**June 2020**

**Copyright © 2020 PEMPAL IACOP**

All rights reserved. No part of this publication may be reproduced, transmitted, or distributed in any form without prior written permission from PEMPAL IACOP except for noncommercial uses permitted by copyright law. Any modification to the guidance provided on cooperation agreements in this publication requires a citation to the effect that this publication was used and that it was modified. Contact [iacop@pempal.org](mailto:iacop@pempal.org).



**Internal Audit Community of Practice (IACOP)**

T: +7 495 745 70 00 ext. 2002

E: [IACOP@pempal.org](mailto:IACOP@pempal.org)

W: [www.pempal.org](http://www.pempal.org)



# Contents

Acknowledgements.....	2
Acronyms.....	2
What are PEMPAL and IACOP?.....	3
Preface.....	4
Introduction.....	5
<b>SECTION A. FULL GLOSSARY.....</b>	<b>6</b>
<b>SECTION B. GLOSSARY BY TOPIC.....</b>	<b>15</b>
B1. GENERIC TERMS THAT RELATE TO PUBLIC INTERNAL FINANCIAL CONTROL.....	16
B2. TERMS THAT RELATE TO RISK MANAGEMENT.....	21
B3. TERMS THAT RELATE TO COSO INTERNAL CONTROL.....	24
B4. TERMS THAT RELATE TO THE ELEMENTS OF A PERFORMANCE MANAGEMENT FRAMEWORK.....	28



# Acknowledgements

This guidance was made possible by the contributions of Internal Audit Community of Practice (IACOP) members. Specifically, the IACOP would like to recognize the following key contributors: Edgar Mkrtchyan (Armenia), former IACOP Executive Committee (ExCom)

Chair; Petru Babuci (Moldova), IACOP ExCom Vice Chair; Giuli Chkuaseli (Georgia), IACOP ExCom member; Richard Maggs, World Bank consultant; Diana Grosu-Axenti, World Bank consultant; and Arman Vatyan, World Bank, PEMPAL Program Leader.



# Acronyms

<b>COSO</b>	Committee of Sponsoring Organizations of the Treadway Commission
<b>IACOP</b>	Internal Audit Community of Practice of PEMPAL
<b>PEMPAL</b>	Public Expenditure Management Peer Assisted Learning



## What are PEMPAL and IACOP?

Public Expenditure Management Peer Assisted Learning (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 the member countries through developing and disseminating information on good practices and their application.

The network is organized around three thematic communities of practice:

- Budget Community of Practice,
- Treasury Community of Practice, and
- Internal Audit Community of Practice.

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; key 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

This glossary is a product of knowledge sharing and collaboration among PEMPAL IACOP members.

The IACOP Internal Control Working Group identified that a glossary of terms relating to internal control, primarily for use by Central Harmonization Units and internal auditors, would help promote consistent understanding of key internal control terms.

The glossary focuses exclusively on internal control (rather than internal audit) terms and reflects an extensive collaborative process, including among practitioners and policymakers in PEMPAL member countries. PEMPAL members expect the glossary to add value in their countries by:

- Generating common understanding of technical terms amongst public sector officials and accounting and audit professionals.
- Ensuring accurate translation of technical terms. Internal control systems are new for many countries (which in the past were highly centralized) and if the terminology is not accurately translated the meaning of terms can be confusing.
- Promoting common understandings of the purpose of internal control amongst professionals, managers, and politicians,

especially as part of the process of internal control and internal audit reform.

- Helping harmonize national legislation with internationally recognized terminology and standards.
- Enhancing training – particularly in universities but also for public sector internal auditors, internal control coordinators, and managers and public servants involved in implementing internal control.
- Supporting raising awareness of internal control by helping explain the theory to managers, politicians, and others involved in internal control implementation.

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; and The Impact of COVID-19 on the Role and Activities of Internal Audit. All are available from [www.pempal.org](http://www.pempal.org).

June 2020



# Introduction

The PEMPAL glossary of terms has been developed based on (i) the glossary that accompanies the Institute of Internal Auditors International Standards for the Professional Practice of Internal Auditing (the standards); (ii) the terminology used by the European Union in promoting the concept of public internal control (including public internal financial control); (iii) the terms used by COSO in defining internal control and the related components of the Integrated Framework<sup>1</sup>; and (iv) the terms used in the COSO Enterprise Risk Management Framework. Where a term has not been obtained from one of these four main sources, the source of the glossary definition is explained in a footnote.

The glossary has been produced in two formats for ease of use.

- SECTION A contains a full glossary which includes all the terms proposed by PEMPAL where the terms included have been color coded as follows:

Generic terms that relate to public internal financial control

Terms that relate to risk management

Terms that relate to COSO-based internal control

Terms that relate to the elements of a performance management framework

- SECTION B contains a series of four individual glossaries where the color-coded sections noted above have been grouped together.

<sup>1</sup> The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control - Integrated Framework. Designed to help organizations better design, implement, and assess internal control. <http://www.coso.org/>

**SECTION**



**FULL GLOSSARY**



TERMINOLOGY	DEFINITION
<b>Accountability</b>	<p>The obligations of persons or entities, including public enterprises and corporations, entrusted with public resources to be answerable for the financial, managerial, and program responsibilities that have been conferred on the manager, and to report to those that have conferred these responsibilities.</p> <p>It means that persons are held responsible for carrying out a defined set of duties or tasks, and for conforming with rules and standards applicable to their posts. The person or body to which individuals answer for their actions is made explicit and they may be rewarded for good performance or suffer the consequences of inadequate performance.</p>
<b>Audit Evidence<sup>2</sup></b>	Information, which supports the opinions, conclusions, or reports of the auditors, internal audit services, or supreme audit institution. It should be sufficiently reliable and relevant to support the opinions and conclusions made.
<b>Audit Mandate</b>	The auditing responsibilities, powers, discretion, and duties conferred on any audit body (e.g. the supreme audit institution) under the constitution or other lawful authority of a country (as set out in primary or secondary national legislation).
<b>Audit Objective</b>	A precise statement of what the audit intends to accomplish and/or the question the audit will answer. This may include financial, regularity, or performance issues.
<b>Audit Procedures</b>	Tests, instructions, and details included in the audit program to be carried out systematically and reasonably.
<b>Audit Scope</b>	The framework or limits of the subject of an audit.
<b>Audited Entity</b>	The organization, program, activity, or functions subject to audit by the supreme audit institution or the (internal) audit service.

<sup>2</sup> EU definition corrected to reflect modern audit usage

Performance  
COSO  
Risk  
Generic

TERMINOLOGY	DEFINITION
<b>Board</b>	The highest-level governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization’s activities and hold senior management accountable. Although governance arrangements vary among jurisdictions and sectors, typically the board includes members who are not part of management. If a board does not exist, the word “board” in the standards refers to a group or person charged with governance of the organization. Furthermore, “board” in the standards may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee).
<b>Central Harmonization Unit</b>	A policy unit attached to the Ministry of Finance (and often reporting directly to the Minister of Finance) responsible for overseeing the status of public internal financial control in the entire public sector
<b>Conflict of Interest</b>	Any relationship that is, or appears to be, not in the best interest of the organization. A conflict of interest would prejudice an individual’s ability to perform his or her duties and responsibilities objectively.
<b>Control</b>	Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.
<b>Control Activities</b>	<p><b>One of the five components of the COSO <i>Internal Control Integrated Framework</i>.</b></p> <p>Control activities are the actions established through policies and procedures that help ensure that management’s directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.</p>

Performance

COSO

Risk

Generic

TERMINOLOGY	DEFINITION
<b>Control Environment</b>	<p><b>One of the five components of the COSO <i>Internal Control Integrated Framework</i>.</b></p> <p>The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control including expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its governance oversight responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.</p>
<b>Economy</b>	<p>Minimizing the cost resources used to achieve a certain level of outputs while having regard to quality - "spending less".<sup>3</sup></p>
<b>Efficiency</b>	<p>The relationship between the output from goods or services and the resources required to produce them - "spending well".<sup>4</sup></p>
<b>Effectiveness</b>	<p>The extent to which objectives are achieved and the relationship between intended and actual impact of a service - "spending wisely".<sup>5</sup></p>
<b>Enterprise Risk Management</b>	<p>The culture, capabilities, and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving, and realizing value.</p>

<sup>3</sup> UK National Audit Office

<sup>4</sup> UK National Audit Office

<sup>5</sup> UK National Audit Office

TERMINOLOGY	DEFINITION
<b>Ethics</b>	<p>Ethics in the public sector cover four main areas: setting public service roles and values as well as responsibilities and levels of authority and accountability; measures to prevent conflicts of interest and ways of resolving them; setting the rules (standards) of conduct of public servants; and setting rules for dealing with serious irregularities and fraud. Management responsible for the financial management and control system is expected to make use of tools promoting and raising awareness of ethical values in management and control.</p> <p>For internal auditors in particular, ethics imply the four principles of integrity, objectivity, confidentiality, and competency.</p>
<b>External Service Provider</b>	<p>A person or firm outside of the organization that has special knowledge, skill, and experience in a particular discipline.</p>
<b>External Environment</b>	<p>Anything outside of the entity that influences the ability to achieve its strategy and business objectives.</p>
<b>Financial Management &amp; Control</b>	<p>Term developed by the European Union which means the comprehensive internal control system that is established by and is the responsibility of the head of the entity, and which, together with risk management, provides reasonable assurances that the budget and other public funds will be used properly, economically, efficiently, and effectively in the accomplishment of relevant objectives of the entity.</p> <p>This term is closely related with the term internal control but is often used to also capture the generic accountability of public sector managers to their stakeholders.</p>
<b>Fraud</b>	<p>Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.</p>
<b>Governance</b>	<p>The combination of processes and structures implemented by the governing bodies to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives. That is: the systems and processes that ensure the overall effectiveness of an entity – whether a business, government, or multilateral institution.</p>

Performance

COSO

Risk

Generic

TERMINOLOGY	DEFINITION
<b>Impact</b>	The result or effect of an event. There may be a range of possible impacts associated with an event. The impact of an event may be positive (opportunities) or negative (risks) relative to the entity's strategy or business objectives. <sup>6</sup>
<b>Inherent Risk</b>	The risk to an entity in the absence of any direct or focused actions by management to alter its severity.
<b>Information &amp; Communication</b>	<p><b>One of the five components of the COSO Internal Control Integrated Framework.</b></p> <p>Information is necessary for the entity to carry out internal control responsibilities in support of achievement of its objectives. Communication occurs both internally and externally and provides the organization with the information needed to carry out day-to-day internal control activities. Communication enables personnel to understand internal control responsibilities and their importance to the achievement of objectives.</p>
<b>Information Technology Controls</b>	Controls that support business management and governance as well as provide general and technical controls over information technology infrastructures such as applications, information, infrastructure, and people.
<b>Information Technology Governance</b>	Consists of the leadership, organizational structures, and processes that ensure that the enterprise's information technology supports the organization's strategies and objectives.
<b>Internal Control</b>	A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.
<b>Likelihood</b>	The possibility that a given event will occur.

<sup>6</sup> COSO ERM definition modified to reflect event driven risk management terminology.

Performance	TERMINOLOGY	DEFINITION
COSO	<b>Monitoring Activities</b>	<p><b>One of the five components of the COSO <i>Internal Control Integrated Framework</i>.</b></p> <p>Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, are present and functioning. Findings are evaluated and deficiencies are communicated in a timely manner, with serious matters reported to senior management and to the board.</p>
Risk	<b>Opportunity</b>	<p>An action or potential action that creates or alters goals or approaches for creating, preserving, and realizing value.</p>
Generic	<b>Organization or Entity</b>	<p>Any form of for-profit and not-for-profit organization/entity or governmental body. An organization/entity may be publicly listed, privately owned, owned through a cooperative structure, or any other legal structure</p>
	<b>Outcome</b>	<p>The effects of a program or project measured at the highest meaningful level in proportion to the program or project (e.g. jobs created). In practice, there are always at least some external non-controllable elements which influence whether outcomes are achieved or not.</p>
	<b>Outputs</b>	<p>The directly tangible deliverables of a program or project insofar as they are, for practical purposes, completely under the control of the implementers of the project.</p>
	<b>Performance Management</b>	<p>The measurement of efforts to achieve or exceed the strategy and business objectives.</p>
	<b>Persistence</b>	<p>For how long a risk impacts an entity.</p>
	<b>Portfolio View</b>	<p>A composite view of risk the entity faces, which positions management and the board to consider the types, severity, and interdependencies of risks and how they may affect the entity's performance relative to its strategy and business objectives.</p>

Performance

COSO

Risk

Generic

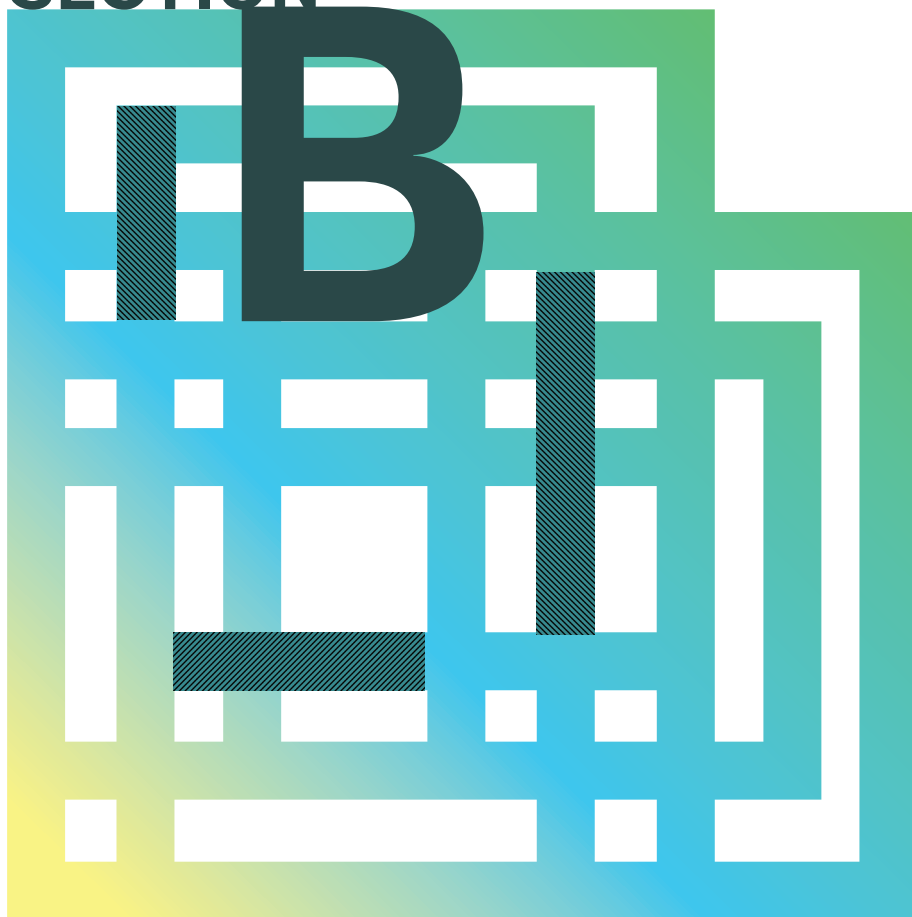
TERMINOLOGY	DEFINITION
<b>Public Internal Financial Control</b>	The terminology used by the European Commission during the process of enlargement to capture the need for the improvements in internal control, internal audit and central harmonization. This term has now been replaced by public internal control to reflect the fact that internal control is more than just financial control.
<b>Public Internal Control</b>	The term now often used in place of public internal financial control to express the three elements of internal control, internal audit, and central harmonization required for best practice financial management.
<b>Recovery</b>	The capacity of an entity to return to acceptable tolerance levels after the impact of a risk.
<b>Residual Risk</b>	The level of risk remaining after the application of control activities.
<b>Risk</b>	The possibility of an event occurring that will have an impact on the achievement of objectives. NOTE: "Risks" (plural) refers to one or more potential events that may affect the achievement of objectives. "Risk" (singular) refers to all potential events collectively that may affect the achievement of objectives.
<b>Risk Appetite</b>	The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of added value.
<b>Risk Assessment</b>	<p><b>One of the five components of the COSO Internal Control Integrated Framework.</b></p> <p>Risk assessment involves a dynamic and iterative process for identifying and analyzing risks to achieving the entity's objectives, forming a basis for determining how risks should be managed. Management considers possible changes in the external environment and within its own business model that may impede its ability to achieve its objectives. Risk assessment includes processes for risk identification, risk analysis, and risk response; that risk tolerances and an acceptable level of variation in performance should be considered in the assessment of acceptable risk levels; and that the discussion of risk severity includes velocity and persistence in addition to impact and likelihood.</p>

	TERMINOLOGY	DEFINITION
Performance	<b>Risk Capacity</b>	The maximum amount of risk that an entity is able to absorb in the pursuit of strategy and business objectives.
COSO	<b>Risk Management</b>	A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.
Risk	<b>Risk Profile</b>	A composite view of the risk assumed at a particular level of the entity, or aspect of the business that positions management to consider the types, severity, and interdependencies.
	<b>Risk Register</b>	A listing of all risks that impact an entity which may include proposed risk responses.
Generic	<b>Risk Tolerance</b>	The boundaries of acceptable variation in performance related to achieving business objectives.
	<b>Speed of Onset or Velocity</b>	The time it takes for a risk event to manifest itself or the time that elapses between the occurrence of an event and the point at which the organization first feels its effects.
	<b>Stakeholders</b>	Parties that have a genuine or vested interest in the entity.
	<b>Target Residual Risk</b>	The amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives, knowing that management will implement, or has implemented, direct or focused actions to alter the severity of the risk.
	<b>Value for Money</b>	Good value for money is the optimal use of resources to achieve the intended outcomes. 'Optimal' means 'the most desirable possible given expressed or implied restrictions or constraints'. Value for money is not about achieving the lowest initial price. <sup>7</sup>

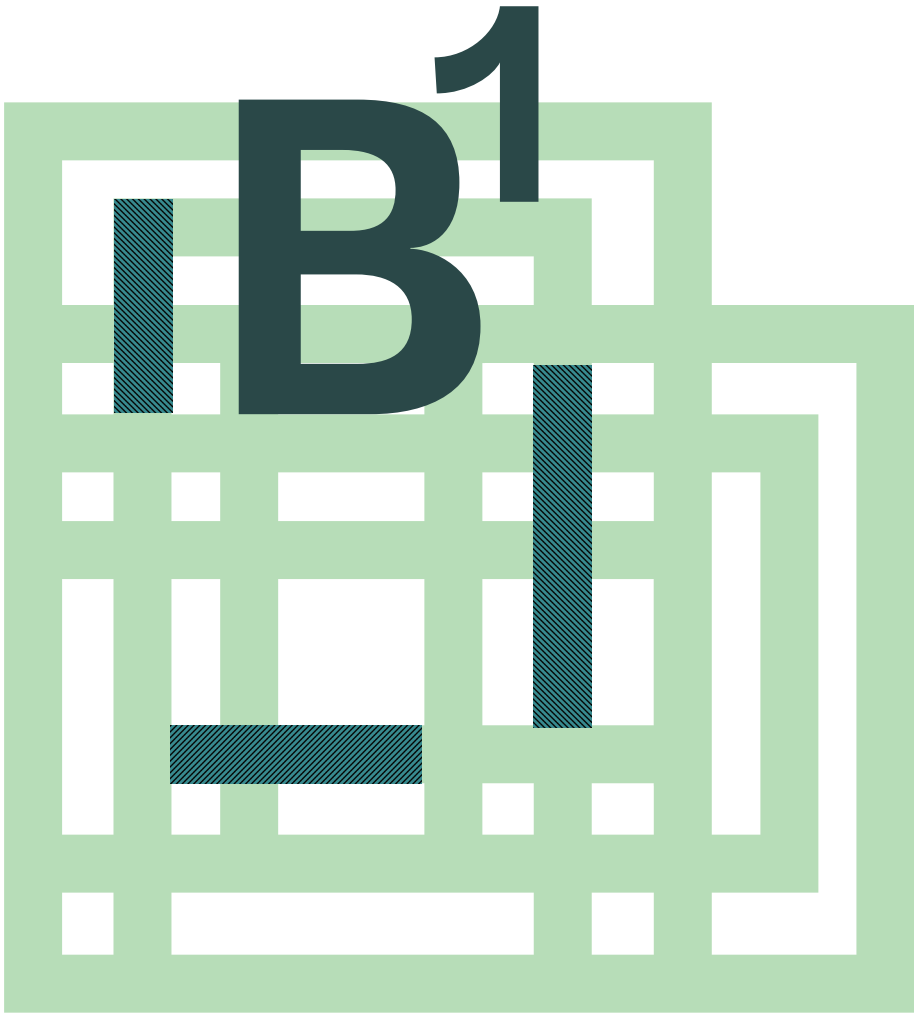
<sup>7</sup> UK National Audit Office.



**SECTION**



**GLOSSARY BY TOPIC**



**GENERIC TERMS THAT RELATE TO  
PUBLIC INTERNAL  
FINANCIAL CONTROL**

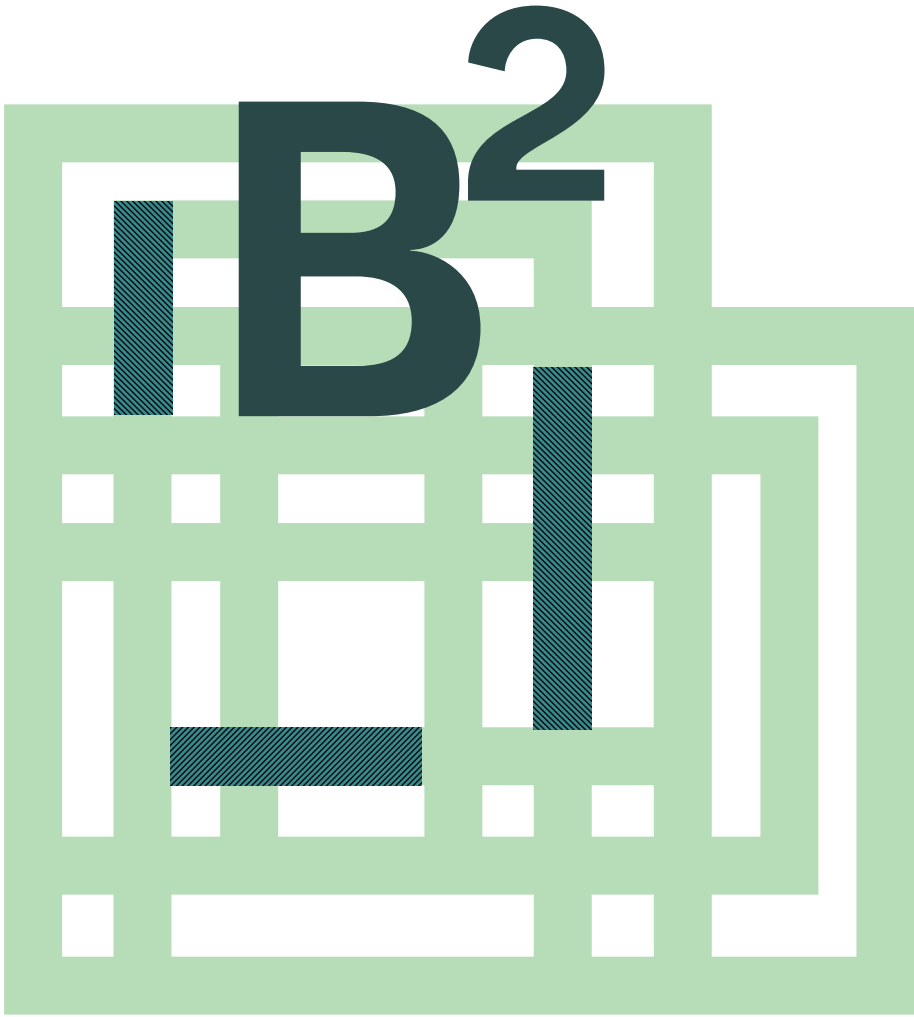
TERMINOLOGY	DEFINITION
<b>Accountability</b>	<p>The obligations of persons or entities, including public enterprises and corporations, entrusted with public resources to be answerable for the financial, managerial, and program responsibilities that have been conferred on the manager, and to report to those that have conferred these responsibilities.</p> <p>It means that persons are held responsible for carrying out a defined set of duties or tasks, and for conforming with rules and standards applicable to their posts. The person or body to which individuals answer for their actions is made explicit and they may be rewarded for good performance or suffer the consequences of inadequate performance.</p>
<b>Audit Evidence<sup>8</sup></b>	<p>Information which supports the opinions, conclusions, or reports of the auditors, internal audit services, or supreme audit institution. It should be sufficiently reliable and relevant to support the opinions and conclusions made.</p>
<b>Audit Mandate</b>	<p>The auditing responsibilities, powers, discretion, and duties conferred on any audit body (e.g. the supreme audit institution) under the constitution or other lawful authority of a country (as set out in primary or secondary national legislation).</p>
<b>Audit Objective</b>	<p>A precise statement of what the audit intends to accomplish and/or the question(s) the audit will answer. This may include financial, regularity, or performance issues.</p>
<b>Audit Procedures</b>	<p>Tests, instructions, and details included in the audit program to be carried out systematically and reasonably.</p>
<b>Audit Scope</b>	<p>The framework or limits of the subject of an audit.</p>
<b>Audited Entity</b>	<p>The organization, program, activity, or functions subject to audit by the supreme audit institution or the (internal) audit service.</p>

<sup>8</sup> EU definition corrected to reflect modern audit usage

TERMINOLOGY	DEFINITION
<b>Board</b>	The highest-level governing body (e.g., board of directors, supervisory board, or board of governors or trustees) charged with the responsibility to direct and/or oversee the organization's activities and hold senior management accountable. Although governance arrangements vary among jurisdictions and sectors, typically the board includes members who are not part of management. If a board does not exist, the word "board" in the standards refers to a group or person charged with governance of the organization. Furthermore, "board" in the standards may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee).
<b>Central Harmonization Unit</b>	A policy unit attached to the Ministry of Finance (and often reporting directly to the Minister of Finance) responsible for overseeing the status of public internal financial control in the entire public sector
<b>Conflict of Interest</b>	Any relationship that is, or appears to be, not in the best interest of the organization. A conflict of interest would prejudice an individual's ability to perform his or her duties and responsibilities objectively.
<b>Ethics</b>	<p>Ethics in the public sector cover four main areas: setting public service roles and values as well as responsibilities and levels of authority and accountability; measures to prevent conflicts of interest and ways of resolving them; setting the rules (standards) of conduct of public servants; and setting rules for dealing with serious irregularities and fraud. Management responsible for the financial management and control system is expected to make use of tools promoting and raising awareness of ethical values in management and control.</p> <p>For internal auditors in particular, ethics imply the four principles of integrity, objectivity, confidentiality, and competency.</p>
<b>External Service Provider</b>	A person or firm outside of the organization that has special knowledge, skill, and experience in a particular discipline.
<b>External Environment</b>	Anything outside of the entity that influences the ability to achieve its strategy and business objectives.

TERMINOLOGY	DEFINITION
<b>External Stakeholders</b>	Any parties not directly engaged in the entity's operations but who are affected by the entity, directly influence the entity's business environment, or influence the entity's reputation.
<b>Financial Management &amp; Control</b>	<p>Term developed by the European Union which means the comprehensive internal control system that is established by and is the responsibility of the head of the entity, and which, together with risk management, provides reasonable assurances that the budget and other public funds will be used properly, economically, efficiently, and effectively in the accomplishment of relevant objectives of the entity.</p> <p>This term is closely related with the term internal control but is often used to also capture the generic accountability of public sector managers to their stakeholders.</p>
<b>Fraud</b>	Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.
<b>Governance</b>	The combination of processes and structures implemented by the governing bodies to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives. That is: the systems and processes that ensure the overall effectiveness of an entity – whether a business, government, or multilateral institution.
<b>Organization or Entity</b>	Any form of for-profit and not-for-profit organization/entity or governmental body. An organization/entity may be publicly listed, privately owned, owned through a cooperative structure, or any other legal structure.
<b>Performance Management</b>	The measurement of efforts to achieve or exceed the strategy and business objectives.

TERMINOLOGY	DEFINITION
<b>Public Internal Financial Control</b>	The terminology used by the European Commission during the process of enlargement to capture the need for the improvements in internal control, internal audit and central harmonization. This term has now been replaced by public internal control to reflect the fact that internal control is more than just financial control.
<b>Public Internal Control</b>	The term now used in place of public internal financial control to express the three elements of internal control, internal audit, and central harmonization required for best practice financial management.
<b>Stakeholders</b>	Parties that have a genuine or vested interest in the entity.



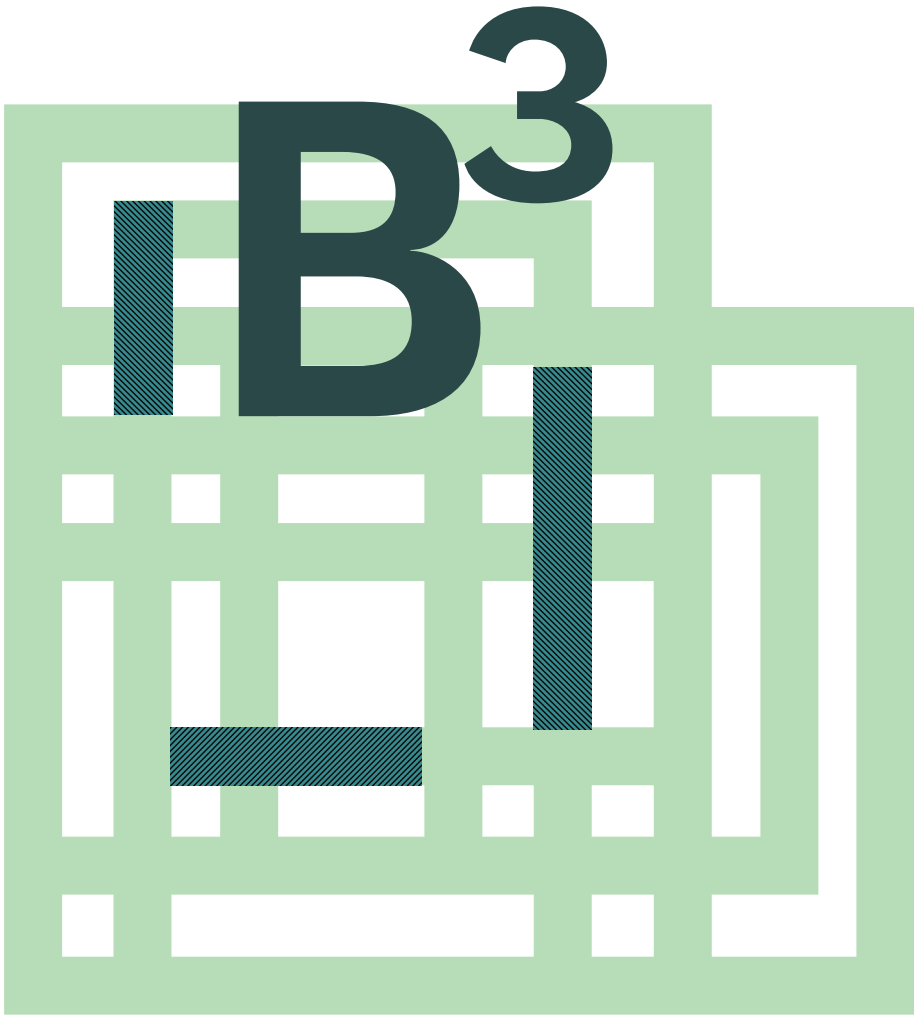
TERMS THAT RELATE TO  
**RISK MANAGEMENT**

TERMINOLOGY	DEFINITION
<b>Enterprise Risk Management</b>	The culture, capabilities, and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving, and realizing value.
<b>Impact</b>	The result or effect of an event. There may be a range of possible impacts associated with an event. The impact of an event may be positive (opportunities) or negative (risks) relative to the entity's strategy or business objectives. <sup>9</sup>
<b>Inherent Risk</b>	The risk to an entity in the absence of any direct or focused actions by management to alter its severity.
<b>Likelihood</b>	The possibility that a given event will occur.
<b>Opportunity</b>	An action or potential action that creates or alters goals or approaches for creating, preserving, and realizing value.
<b>Persistence</b>	How long a risk impacts an entity.
<b>Portfolio View</b>	A composite view of risk the entity faces, which positions management and the board to consider the types, severity, and interdependencies of risks and how they may affect the entity's performance relative to its strategy and business objectives.
<b>Recovery</b>	The capacity of an entity to return to acceptable tolerance levels after the impact of a risk.
<b>Residual Risk</b>	The level of risk remaining after the application of control activities.
<b>Risk</b>	The possibility of an event occurring that will have an impact on the achievement of objectives. NOTE: "Risks" (plural) refers to one or more potential events that may affect the achievement of objectives. "Risk" (singular) refers to all potential events collectively that may affect the achievement of objectives.

<sup>9</sup> COSO ERM definition modified to reflect event driven risk management terminology.



TERMINOLOGY	DEFINITION
<b>Risk Appetite</b>	The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of added value.
<b>Risk Capacity</b>	The maximum amount of risk that an entity is able to absorb in the pursuit of strategy and business objectives.
<b>Risk Management</b>	A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.
<b>Risk Profile</b>	A composite view of the risk assumed at a particular level of the entity, or aspect of the business that positions management to consider the types, severity, and interdependencies.
<b>Risk Register</b>	A listing of all risks that impact an entity which may include proposed risk responses.
<b>Risk Tolerance</b>	The boundaries of acceptable variation in performance related to achieving business objectives.
<b>Severity</b>	A measurement of considerations such as the likelihood and impact of events or the time it takes to recover from events.
<b>Speed of Onset or Velocity</b>	The time it takes for a risk event to manifest itself or the time that elapses between the occurrence of an event and the point at which the organization first feels its effects.
<b>Target residual risk</b>	The amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives, knowing that management will implement, or has implemented, direct or focused actions to alter the severity of the risk.

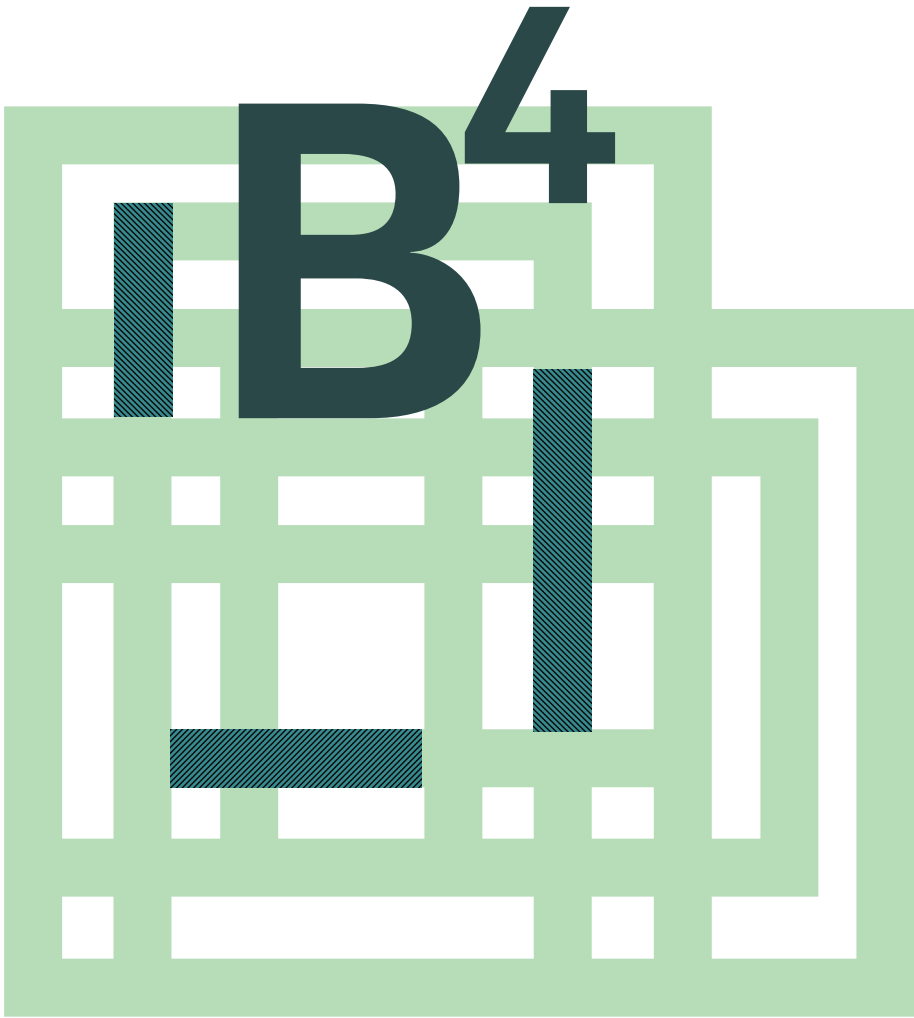


TERMS THAT RELATE TO  
**COSO INTERNAL  
CONTROL**

TERMINOLOGY	DEFINITION
<b>Control</b>	Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.
<b>Control Activities</b>	<p><b>One of the five components of the COSO <i>Internal Control Integrated Framework</i>.</b></p> <p>Control activities are the actions established through policies and procedures that help ensure that management’s directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.</p>
<b>Control Environment</b>	<p><b>One of the five components of COSO <i>Internal Control Integrated Framework</i>.</b></p> <p>The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control including expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its governance oversight responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.</p>

TERMINOLOGY	DEFINITION
<b>Information &amp; Communication</b>	<p><b>One of the five components of the COSO <i>Internal Control Integrated Framework</i>.</b></p> <p>Information is necessary for the entity to carry out internal control responsibilities in support of achievement of its objectives. Communication occurs both internally and externally and provides the organization with the information needed to carry out day-to-day internal control activities. Communication enables personnel to understand internal control responsibilities and their importance to the achievement of objectives.</p>
<b>Information Technology Controls</b>	<p>Controls that support business management and governance as well as provide general and technical controls over information technology infrastructures such as applications, information, infrastructure, and people.</p>
<b>Information Technology Governance</b>	<p>Consists of the leadership, organizational structures, and processes that ensure that the enterprise's information technology supports the organization's strategies and objectives.</p>
<b>Internal Control</b>	<p>A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.</p>
<b>Monitoring Activities</b>	<p><b>One of the five components of the COSO <i>Internal Control Integrated Framework</i>.</b></p> <p>Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, are present and functioning. Findings are evaluated and deficiencies are communicated in a timely manner, with serious matters reported to senior management and to the board.</p>

TERMINOLOGY	DEFINITION
<b>Risk Assessment</b>	<p><b>One of the five components of the COSO <i>Internal Control Integrated Framework</i>.</b></p> <p>Risk assessment involves a dynamic and iterative process for identifying and analyzing risks to achieving the entity's objectives, forming a basis for determining how risks should be managed. Management considers possible changes in the external environment and within its own business model that may impede its ability to achieve its objectives. Risk assessment includes processes for risk identification, risk analysis, and risk response; that risk tolerances and an acceptable level of variation in performance should be considered in the assessment of acceptable risk levels; and the discussion of risk severity includes velocity and persistence in addition to impact and likelihood.</p>



TERMS THAT RELATE TO  
**THE ELEMENTS OF A  
PERFORMANCE  
MANAGEMENT  
FRAMEWORK**

TERMINOLOGY	DEFINITION
<b>Economy</b>	Minimizing the cost resources used to achieve a certain level of outputs while having regard to quality - “spending less”. <sup>10</sup>
<b>Efficiency</b>	The relationship between the output from goods or services and the resources required to produce them – “spending well”. <sup>11</sup>
<b>Effectiveness</b>	The extent to which objectives are achieved and the relationship between intended and actual impact of a service – “spending wisely”. <sup>12</sup>
<b>Outcome</b>	The effects of a program or project measured at the highest meaningful level in proportion to the program or project (e.g. jobs created). In practice there are always at least some external non-controllable elements, which influence whether outcomes are achieved or not.
<b>Outputs</b>	The directly tangible deliverables of a program or project insofar as they are, for practical purposes, completely under the control of the implementers of the project.
<b>Value for Money</b>	Good value for money is the optimal use of resources to achieve the intended outcomes. ‘Optimal’ means ‘the most desirable possible given expressed or implied restrictions or constraints’. Value for money is not about achieving the lowest initial price. <sup>13</sup>

---

<sup>10</sup> UK National Audit Office

<sup>11</sup> UK National Audit Office

<sup>12</sup> UK National Audit Office

<sup>13</sup> UK National Audit Office



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