Chartered Institute of Internal Auditors

24 March 2023

Control - Information guidance

Chartered Institute of Internal Auditors

This information guidance introduces the concept of control. It explains some of the terms and signposts research resources.

Definition of control

Control is a broad concept that means different things to different people. The formal definition, according to the International Professional Practices Framework (IPPF) glossary, is:

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, organises and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

The 2013 Committee of Sponsoring Organisations of the Treadway Commission (COSO) Internal Control – Integrated Framework, uses the term control activities (page 4) and explains these as:

"…….. 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."

Purpose of control

In the UK and Ireland, we tend to see control as deriving its purpose and value from the management of risk. Controls are there if there is a risk to be managed. There is no point having a control without a risk to manage.

This view is compatible with the Financial Reporting Council's guidance on risk management, internal control and related financial and business reporting, which was published in September 2014 to replace the Turnbull Guidance.

The FRC's guide is primarily directed at companies with the specific aim of embedding best practice on risk management and internal control into business processes, in order to achieve

objectives.

Appendix C to the guide contains questions that may assist boards and or internal auditors in assessing how responsibilities are carried out, the culture of the company, and the effectiveness of the risk management and internal control systems.

Control processes

In the UK and Ireland, we tend to see control as deriving its purpose and value from the management of risk. Controls are there if there is a risk to be managed. There is no point having a control without a risk to manage.

Risk management should not only be about protecting an organisation and its assets but also making the most of opportunities. Controls should help the organisation achieve both objectives.

This view is compatible with the Financial Reporting Council's guidance on risk management, internal control and related financial and business reporting, published in September 2014 to replace the Turnbull Guidance. The FRC's guide is primarily directed at companies with the specific aim of embedding best practice on risk management and internal control into business processes, in order to achieve objectives.

The table sets out three different types of control with some examples:

Type of Control	Automated/Manual	Examples
Preventive – a control that limits the possibility of an undesirable outcome	Manual	**Segregation of duties** between staff approving invoices and processing the payments
	Automated	**System enforced user access rights** that limit system functionality based on an individual's role
	Manual	**Supervisor review** to confirm that all required checks have been completed prior to releasing funds to customer
Detective – a control that identifies errors, after the event	Automated report/ Manual correction	**Error report** that flags data errors after a transaction has been processed; corrective action is then taken to remediate errors
	Manual	**Reconciliation** of a bank account to a ledger; corrective

		action taken to reassign reconciling errors
	Automated alert/ Manual correction	**Key performance indicator** that provides an alert when a budget figure is close to or has been exceeded; corrective action may then be taken to reduce spending
Directive – a control designed to cause or encourage a desirable event to occur	Manual	**Training** provided to staff before they commence a new role/activity to instruct them on the requirements of their role
	Manual	**Policy and procedures** that staff are required to read and confirm that they will comply with
	Manual	**Financial incentives** to be paid to staff who meet minimum expectations for the quality of their work

Control maturity

Control maturity is a phrase used to describe the efficient and effective development of controls over time - typically from manual to integrated.

The authoritative guidance on control is produced by COSO. Their 2013 Internal Control-Integrated Framework provides a useful maturity matrix which can be applied to the overall control environment or individual controls.

Maturity Level 1: Informal or Ad-hoc	**Maturity Level 2: Standard**
• Control activities fragmented • Control activities may be managed in “silo” situations • Control activities dependent upon individual heroics • Inadequate documentation and reporting methods • Inadequate monitoring methods	• Control awareness exists • Control activities designed • Control activities in place • Some documentation and reporting methodology exists • Automated tools and other control measures may exist, but are not necessarily integrated within all functions

Control environment

The control environment refers to the way the board and senior management set the tone of the organisation. It is part of the organisation's culture, influencing how risk is viewed and the 'control consciousness' of its people. It is an expression of the 'way things are done'.

Every organisation operates differently, as is revealed by their organisational ethics, values, structure, reporting lines, authority, rules and the documentation of policy.

The IPPF definition of the control environment is:

the attitude and actions of the board and management regarding the importance of control within the organisation. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:

- Integrity and ethical values.
- Management's philosophy and operating style.
- Organisational structure.
- Assignment of authority and responsibility.
- Human resource policies and practices.
- Competence of personnel.

A control environment encompasses the attitudes and actions of the board and management regarding the significance of control within the organisation (or a function). It provides the discipline and structure to achieve the objectives of the system of internal control. Here is a useful mnemonic to help remember the elements:

- M - Management’s philosophy and operating style
- O - Organisational structure
- H - Human Resource policies and practices
- I - Integrity and ethical values
- C - Competence of personnel
- A - Assignment of authority and responsibility
- N - Non-executive directors – relates to the Audit Committee and their role in approving the internal audit plans both strategic and the risk based operational plan.

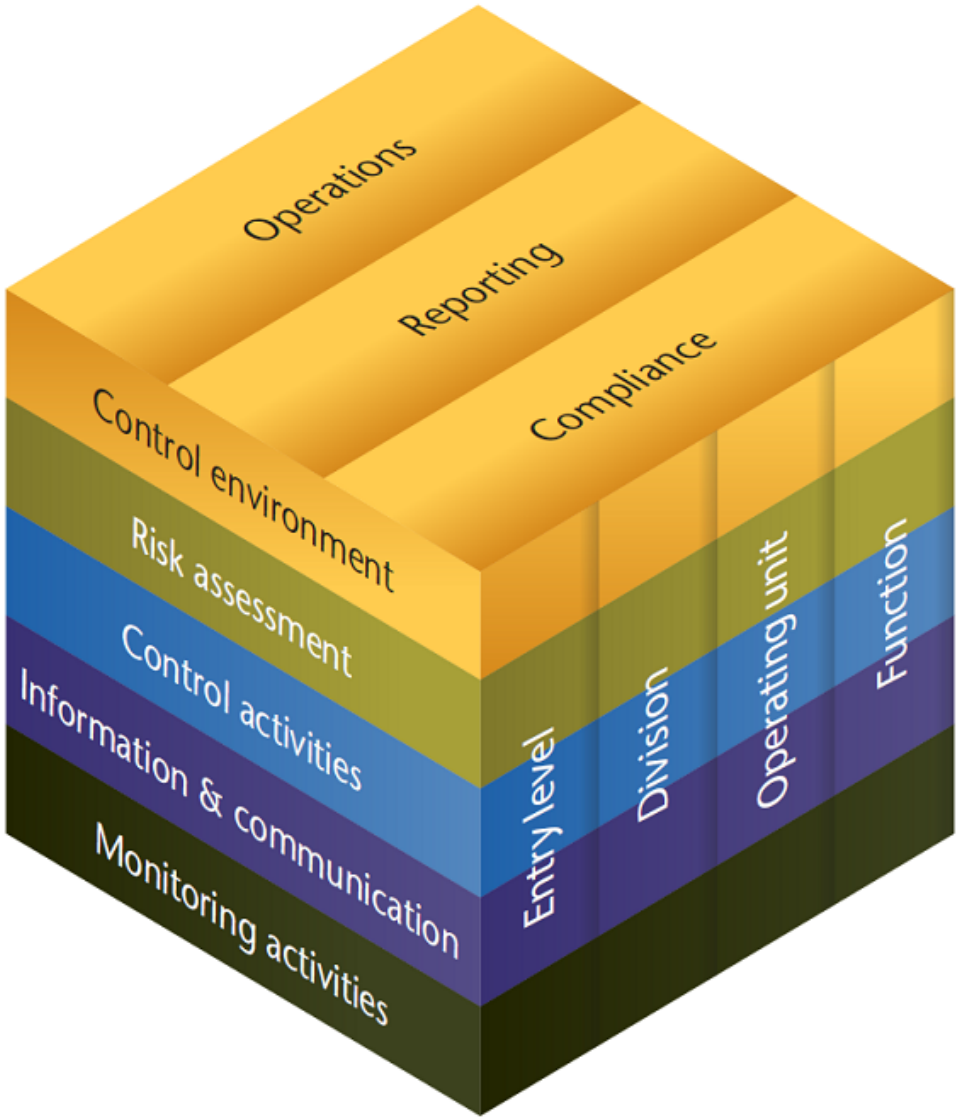
Control models and guidance

These help managers understand the interrelationship between governance, risk management and control. They can also be used as a reference point to review and refine the control environment of the organisation.

Perhaps the most well-known of these is COSO’s 2013 Internal Control – Integrated Framework.

It explains that there is a direct relationship between organisational structure, objectives and components represented in the diagram below. There are three types of objectives (columns) and

five components (rows), which have a set of 17 supporting principles designed to achieve effective control.



1. Control environment
Setting the 'tone at the top' with appropriate structures and reporting lines.

2. Risk assessment

Identification and analysis of relevant risks and assessment of changes.

3. Control activities
To address identified risks e.g. implementation of policies and procedures.

4. Information and communication
Internal and external communication of information.

5. Monitoring
Reviewing and managing control systems to ensure the components of internal control are present and functioning.

An organisation that has all the components working well is therefore more likely to achieve its objectives and have a strong and sustainable future. Some internal audit functions use the five components as the basis for setting objectives for audit engagements. Control is therefore relevant to all managers from executive director downwards, as well as risk managers and internal auditors.

COSO and relevance to internal audit

The original, 1992 version of COSO's Internal Control - Integrated Framework gained broad acceptance and has been widely used as the predominant framework for reporting on internal control over financial reporting in accordance with Sarbanes-Oxley. However, the decision to update it in 2013 was driven by the extent of two decades worth of change in the business environment, including:

- More expectations for governance oversight especially following large-scale internal control and compliance breakdowns.
- Risk-based approaches receiving more attention.
- Globalisation of markets and operations.
- Third-party risks emerging including from the use of outsourcing and strategic suppliers.
- Enhanced technology creating new and different risks.
- And the continuing and increasing demands and complexities in laws, regulations, and standards.

The most significant change is the explicit articulation of the 17 principles that provide the foundation associated with the five components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring activities. All the principles apply to each category of the three objectives.

COSO decided to make these 'principles' explicit to enhance management's understanding as to what comprises effective internal control. Then supporting each principle are points of focus (77 in all) that are intended to provide guidance to management in designing and implementing internal controls.

For internal auditors the principles and points of focus can be used to review all or selected parts of corporate governance and performance management on a path to better achieve strategic objectives over the long term. Although we would also highlight our specific guidance on how to audit corporate governance published in June 2019.

In 2017, COSO's Enterprise Risk Management – Integrated Framework was also updated (first

published 2004) in response to the evolution of risk management, focusing on the importance of the consideration of risk in strategy setting and driving performance. This document complements the Internal Control – Integrated Framework, with guidance on designing, implementing, conducting and assessing internal control relevant for these emerging risk areas.

Control assurance

Internal audit's responsibility in respect of control is set out in the International Standards. Performance Standard 2130 says:

The internal audit activity must assist the organisation in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

The purpose of this is to provide the board and management with assurance on the adequacy and effectiveness of control. This enables them to understand how the organisation is managing its risk and how likely it is to achieve its objectives.

Further reading

Implementation Guidance 2130: Control
Detail on the focus of control assurance and the practical approach to evaluating control processes.

Auditing the control environment
How the control environment is structured in further detail and offers practical considerations for an internal audit.

Well-being of Future Generations Act
Novel thinking on the role internal audit can have in helping their organisation think about future generations in decision-making.

International Standards Glossary