16 August 2019

Control

Chartered Institute of Internal Auditors

This page introduces the concept of control. It explains some of the terms and points to research resources including IIA guides that cover control and internal audit assurance.

Definition of control

Control is a broad concept that means different things to different people. The IIA definition, according to the International Standards 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.

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

These are the daily routines, checks and balances that make the organisation function. The IIA definition of control processes is:

The policies, procedures (both manual and automated) and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organisation is willing to accept.

The table illustrates two alternative ways of categorising controls, with some examples.

Control categories with examples

Segregation of duties Division of duties between the appointment and payment of staff	**Preventive** Segregation of duties, access controls, authorisation
Organisational Budgets, performance targets and KPIs	
Authorisation Authority levels, spending limits, passwords and user ID	**Detective** Exception reports, reconciliations, control totals, error reports
Personnel Recruitment and selection, staff appraisal procedures	
Supervision Day-to-day oversight of staff and physical activities	**Directive** Accounting manuals, documented procedures, training and supervision
Physical Door entry systems, restricted access to files	
Accounting Control account and bank reconciliation	**Corrective** Error, incident and complaint handling, Virus isolation
Management Team meetings and briefings, CRSA	

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'.

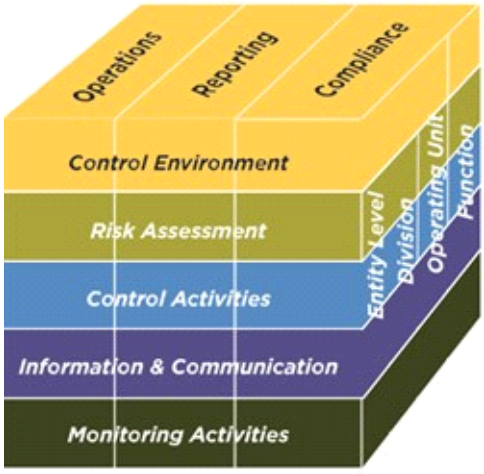
Every organisation operates differently, as is revealed by their organisational ethics, values, structure, reporting lines, authority, rules and the documentation of policy.

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. IIA Global has prepared a summary, Common Internal Control Frameworks, tracking their development.

Perhaps the most well-known of these is COSO's (the Committee of Sponsoring Organisations of the Treadway Commission) Internal Control – Integrated Framework, updated in May 2013.

It explains 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 function us 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 2013 update and relevance to internal audit

The original version of COSO's Internal Control - Integrated Framework released in 1992 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 was driven by the extent of change in the business environment over the past two decades, 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 November 2014.

Leveraging COSO across the three lines of defence

The COSO Internal Control—Integrated Framework has become a trusted and ubiquitous tool to help organisations understand the components, principles, and factors necessary to manage risks through effective internal controls.

However, it is largely silent on who in the organisation is responsible for specific duties outlined in the framework. A new white paper from COSO and The IIA released at the 2015 International Conference offers a remedy by examining how the framework can be leveraged across the three lines of defence model.

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

Performance Standard 2130 Control

Practice Advisory 2130-1: Assessing the adequacy of control processes
Further 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.

Culture and internal control
A free open course you can complete online in two hours.

COSO's Internal Control - Integrated Framework:

Executive Summary
Turning Principles Into Positive Action
Framework