5.2.2
INTERNAL CONTROL FRAMEWORK

Internal control is a complex and continuous process that includes the selection and application of various internal control measures, thereby increasing the efficiency and effectiveness of the company's activities. Managers and employees at all levels must participate in this process, examining risk factors and providing reasonable assurance that the overall objectives of the organisation are achieved. Internal control is not a single event or circumstance, but a set of actions applied on an everyday basis that cover the activities of the entire organisation.

Internal control is therefore not an addition to the company's activities: it is integrated into the activities of the organisation, rather than added to them.

Importance of internal control

Internal control helps to:

- Avoid surprises
- Assure the adequacy of process performance
- Perform jobs more efficiently and effectively
- Improve the overall quality of the business

There are various standards that define the functioning of internal control in an organisation:

- COSO Internal Control Framework (by COSO)
- ISO 31000 Risk management — Guidelines
- ISO 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- Global Internal Audit Standards (by IIA)
- COBIT – Control Objectives for Information and Related Technologies (by ISACA)
- Basel Framework (for the banking sector) (by BCBS)

One of the most widely used globally is the COSO Internal Control Framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).[10] It defines internal control as "a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives."

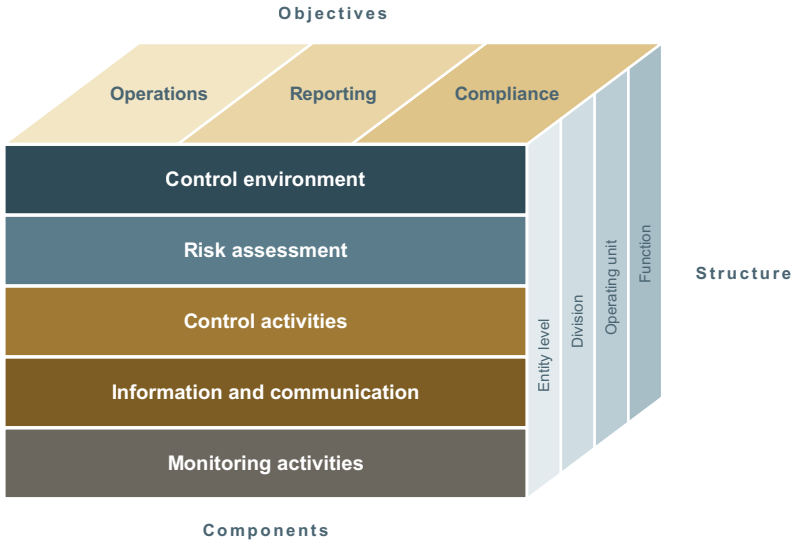
10 Committee of Sponsoring Organizations of the Treadway Commission (COSO), https://www.coso.org/.

Internal control is a process established to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance. It helps to ensure the reliability of financial reporting, promote operational efficiency, protect assets and ensure adherence to laws and regulations. Beyond compliance, robust internal controls build trust, improve decision-making and contribute to overall integrity and growth.

By applying COSO, a company can obtain many benefits, such as:

- Reduced production downtime and fewer workplace accidents.
- Accurate inventory, reducing financial misstatements.
- Assured compliance with environmental and labour regulations.
- Confidence of the Board and shareholders in reporting and risk management.

Figure 5.1 The COSO Internal Control Framework: the "COSO cube"



Source: BICG, based on COSO (2013), Internal Control – Integrated Framework.

The cube shows the three dimensions of the framework and how they relate: the three categories of objectives (operations, reporting and compliance) on the top face, the five components of internal control on the front face, and the structure of the organisation (entity level, divisions, operating units and functions) on the side. Every component applies to every objective and at every level of the organisation.

Control environment

1. The organisation demonstrates a commitment to integrity and ethical values.
2. The Board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

3. Management establishes, with Board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organisation demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organisation holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Examples:

- The Board approves a clearly defined code of conduct with which the company must comply, while management implements the code and provides ethics training for employees.
- The Board sets ethical values, for example zero tolerance of bribery in procurement.
- To ensure independence from management, the Board establishes an audit committee and appoints independent Board members to it.
- The Board ensures that the company has a clear and efficient organisational chart and job descriptions, that each role has defined authorities, and that accountability and an efficient flow of information are ensured.
- Management develops and executes rigorous recruitment, training and retention programmes in order to attract employees with the right values and expertise and to train them efficiently.

Risk assessment

6. The organisation specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The organisation identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.
8. The organisation considers the potential for fraud in assessing risks to the achievement of objectives.
9. The organisation identifies and assesses changes that could significantly affect the system of internal control.

More on risk management can be found in sub-chapter 5.2.3.

Control activities

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

11. The organisation selects and develops general control activities over technology to support the achievement of objectives.
12. The organisation deploys control activities through policies that establish what is expected and procedures that put policies into action.

Examples:

- Segregation of duties. To prevent fraud, the employee responsible for ordering raw materials is different from the one who receives the materials and from the one who approves the invoice for payment. This ensures that no single person can manipulate the purchasing process for personal gain.
- Safeguarding of data. All company data is backed up daily, with versioning (e.g. versions of the data are kept for the last 90 days).
- Policies and procedures. A food production company could have a “Sanitation and Hygiene Policy” stating that all personnel must maintain a hygienic environment to prevent food contamination.

Information and communication

13. The organisation obtains or generates and uses relevant, quality information to support the functioning of internal control.
14. The organisation internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The organisation communicates with external parties regarding matters affecting the functioning of internal control.

Examples:

- Financial data. An enterprise resource planning (ERP) system processes all of a company's transactions, from sales to raw material purchases. This system generates reports, like inventory levels or cost of goods sold, which are crucial for management to assess financial performance and ensure the accuracy of financial statements.
- Communicating internally and externally. A whistleblowing hotline through which an employee, supplier or any other person can anonymously report a colleague’s potential fraudulent activity or a safety violation without fear of retaliation.

Monitoring activities

16. The organisation selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organisation evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board, as appropriate.

Examples:

- The company's quality assurance system performs automated, real-time checks, immediately flags issues and can even stop the production line.
- Internal audit may audit a specific production process and provide recommendations on what should be improved.

Benefits of using the COSO framework

Instead of developing your own (customised) internal control framework, apply COSO in your organisation. This brings many benefits:

- shareholders, potential investors and other stakeholders will better understand how your internal controls are managed;
- auditing of internal controls will be smoother and more efficient;
- it will be easier for newcomers to understand your internal controls;
- The European Commission describes the COSO Framework as setting "the highest international standards" for internal control. [11]

The Board should lead this framework by establishing a governance structure and providing efficient oversight.

Weak, optimal and excessive internal control

Weak control measures increase the risk of losses and extra costs due to unexpected events in the company.

Optimal application of coordinated control procedures and measures supports successful operations.

Excessive controls create an excessive bureaucratic apparatus, which in itself may hinder the operational effectiveness of the company.

11 European Commission (2017), Revision of the Internal Control Framework, C(2017) 2373, https://commission.europa.eu/document/download/f163e193-bf9b-4823-bd4b-dceb8739f46e_en.

KEY TAKEAWAYS

A. Internal control is a continuous process, integrated into the company's activities rather than added to them, that provides reasonable assurance on the achievement of objectives relating to operations, reporting and compliance.

B. The COSO Internal Control Framework is the most widely used reference. Its five components are the control environment, risk assessment, control activities, information and communication, and monitoring activities, each with practical principles the Board can use to test the company's system.

C. Applying a recognised framework, rather than a home-made one, makes internal controls easier for shareholders, auditors and newcomers to understand and easier to audit.

D. Controls can be too weak or too strong: weak controls expose the company to losses and surprises, while excessive controls create bureaucracy that hinders operations. The Board should aim for an optimal, coordinated set of controls.

E. The Board leads the framework by establishing the governance structure and providing effective oversight; management designs and operates the controls.

QUESTIONS FOR THE BOARD

1. *Which internal control framework does the company apply, and can management explain how each of the five COSO components is covered?*
2. *Are objectives specified clearly enough for risks to them, including the risk of fraud, to be identified and assessed?*
3. *Are key controls such as segregation of duties, safeguarding of data and written policies in place for the processes that matter most, and are they documented?*
4. *Does the Board receive relevant, quality information on internal control, and are deficiencies reported and corrected in a timely manner?*
5. *Where are our controls too weak, and where are they excessive and slowing the business down?*
6. *How does the Board satisfy itself that the internal control system is present and functioning, and not only described on paper?*