# Chapter 6
## Internal Control

### Chapter learning objectives:

<table>
<thead>
<tr>
<th>Lead</th>
<th>Component</th>
<th>Indicative syllabus content</th>
</tr>
</thead>
</table>
| **A.3 Ways of managing risk.** | (a) Discuss roles and responsibilities | • Role of board and others in the organisation for identifying and managing risks  
• Risk mitigation including TARA – transfer, avoid, reduce, accept  
• Assurance mapping  
• Risk register  
• Risk reports and responses  
• Ethical dilemmas associated with risk management |
| **C.1 Internal controls systems** | (a) Discuss roles and responsibilities for internal controls  
(b) Discuss the purpose of internal control  
(c) Analyse the features of internal control systems | • Role of risk manager as distinct from internal auditor  
• Control systems in functional areas  
• Operational features of internal control systems |
| **C.2 Recommend internal controls for risk management** | (a) Discuss the COSO internal control framework.  
(b) Assess control weakness  
(c) Assess compliance failures  
(d) Recommend internal controls for risk management | • Governance and culture  
• Strategy and objective setting  
• Performance  
• Review and revision  
• Information, communication and reporting  
• Identifying and evaluating control weakness and compliance failures |
1. **Internal control systems**

Businesses need to set up an internal control system in order to manage the risks they face. Internal controls apply across all areas of the business.

An internal control system is a system through which management can control certain risks and thereby help the business achieve its objectives.

Internal control is a process effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives.  

- COSO

**Internal controls vs risk management**

- Internal controls (IC) care part of the risk reduction method of responding to risk.
- A solid IC system and risk management are both components of good corporate governance.
- In the UK, the Corporate Governance Code requires the board of directors to review the system of IC and decide whether it is sufficient.

2. **The Turnbull Report**

The two main sources of guidance for IC are the COSO (Committee of Sponsoring Organizations of the Treadway Commission) in the USA and the Turnbull Report in the UK.

**Objectives of Internal Control (IC)**

- A company’s system of IC plays a key role in the management of risks that are significant to the fulfilment of its business objectives.
- Since profits are in part the reward of successful risk-taking, the purpose of IC is to control risk appropriately rather than to eliminate it.
- Ensure effective and efficient operations.
- Ensure the reliability of internal and external reporting.
- Assist compliance with laws and regulations.
- Safeguard the shareholders’ investment and the company’s assets.

**Notes:**

- The IC system should be embedded within the company’s operations and culture.
- A sound system if IC reduces, but cannot eliminate, the possibility of poor judgement in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseen circumstances.
• A sound IC system should provide reasonable (not absolute!) assurance that the company will achieve its business objectives.

Responsibilities

• The board of directors (BOD) is responsible for the company’s system of IC. The BOD should set up appropriate IC policies and evaluate how the IC system operates on a regular basis.

• All employees have responsibility for IC. They should, therefore, have the necessary knowledge, skills, information and authority to establish, operate and monitor the IC system.

3. Features of internal control systems

5 elements by COSO (image above):

**Control environment** - management’s attitude, actions and awareness of the need for internal controls. Commitment to controls can be shown via:

• acting with integrity and acting ethically,
• an appropriate company culture,
• an appropriate structure (reporting lines) for internal audit,
• segregation of duties,
• employing skilled staff.
Risk Assessment - should identify:

- **controllable risks**, so that specific control procedures can be established,
- **uncontrollable risks**, so that they can be minimised appropriately. E.g. inflation or natural disasters - insurance could transfer the risk.

Control Activities - for controllable risks. Examples include:

- having a defined organisational structure,
- having proper employment contracts,
- establishing appropriate policies,
- setting up a suitable discipline and reward system,
- having an appropriate performance appraisal and feedback system.

Information & Communication - managers need information to make decisions, so a good information system must be in place. Information should be delivered in a timely manner, and it should be accurate, understandable and relevant.

Monitoring Activities - the control environment is changing, so the internal control system should be monitored so that it can be adjusted and to make sure risks are managed. The internal audit function is usually the key monitor of the IC system.
4. Details of control

Specific control activities should be undertaken to reduce risks. Some samples of organisational controls include:

**Segregation of duties** - this reduces the risk of fraud and error. Processes can be split into parts, and a different person can perform each part (or at least two people should be responsible for dealing with a particular process). For example, the 3-way-match principle, which means that one person cannot initiate a purchase order, approve receipt of goods (confirming that goods have arrived) and pay for the goods.

**Physical controls** - designed to protect physical assets against theft/unauthorised access/use. Examples include using badges to enter/exit a building, a safe/vault for cash, annual/cyclical checks on inventory.

**Authorisation and approval** - prevents a transaction from proceeding until an appropriate level of approval is given, e.g. spending limits may have assigned authorisation limits.

**Management control** - performed by the management based on the information provided:

- top-level review - senior management reviews how the organisation progresses toward its goals.
- activity controls - reports reviewing performance or highlighting exceptions. Questions should be asked by the management to initiate the control activity, for example budget variance reports.

**Supervision** - making sure that individuals do the tasks they are required to do.

**Organisation** - controls provided by the organisation’s structure, e.g. delegating authority or establishing reporting lines.

**Arithmetic and accounting** - e.g. making sure that transactions are recorded properly and can be traced, and checking subtotals.

**Personnel controls** - control the selection and training of employees to make sure that the right person is on the job and that they have received the appropriate induction and training. Internal Controls training should also be given.

**Note**: controls costs should be less than the benefits they bring.
CLASSIFICATION OF CONTROLS

<table>
<thead>
<tr>
<th>Financial</th>
<th>Quantitative non-financial</th>
<th>Qualitative non-financial</th>
</tr>
</thead>
</table>
| Express financial targets and spending limits.  
  • Budgets  
  • Standard costs  
  • Variance analysis  
  • Ratio analysis  
  • Transfer pricing policy | Focus on targets against which performance can be measured and monitored.  
  • Performance indicators  
  • Error measurement  
  • Project tracking  
  • Balanced scorecard  
  • Activity-based management measures  
  • TQM measures | Day-to-day controls, performed by all of the employees.  
  • Organisational structures  
  • Social cultures  
  • Rules and guidelines  
  • Documentation requirements  
  • Physical access controls  
  • Strategic plans  
  • Rewards/incentives  
  • Human resource policies  
  • Corporate governance  
  • Project management  
  • Post-completion audits |

Another means of classification divides internal controls into:

- **Prevent controls** - to stop risk from occurring in the first place (e.g. not paying for an invoice until receipt of the goods).
- **Detect controls** - retrospective controls, identifying risks once they have occurred (e.g. fraud has happened).
- **Correct controls** - reduce the impact of errors (e.g. having a backup of the transactional files).
- **Direct controls** - guide behaviour towards a desired action (e.g. training).
- **Input controls** - what goes into the process (e.g. quality of the raw materials).
- **Process controls** - focus on the process itself (e.g. optimal performance, KPIs).
- **Output controls** - assess whether outputs have met the required standard and if not, why.
ACCOUNTING INTERNAL CONTROLS

You need to ask:

1. What is the process (what are the steps)?
2. What is the risk (what could go wrong)?
3. How can it be controlled (how can the adverse outcome be prevented)?

This can be illustrated by the following examples:

**Sales cycle**

<table>
<thead>
<tr>
<th>Process</th>
<th>Risks</th>
<th>Control procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>receive an order</td>
<td>the customer cannot pay for the order</td>
<td>credit check</td>
</tr>
<tr>
<td>send goods to the customer</td>
<td>the wrong goods are sent</td>
<td>pick up list together with the customer’s original order</td>
</tr>
<tr>
<td>cash received</td>
<td>an incorrect amount was paid</td>
<td>agree cash receipt back to the invoice</td>
</tr>
</tbody>
</table>

**Bank and cash (treasury) controls**

<table>
<thead>
<tr>
<th>Process</th>
<th>Risks</th>
<th>Control procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>safeguard the cash</td>
<td>cash is stolen from the office</td>
<td>use vaults, physical access controls</td>
</tr>
<tr>
<td>safeguard the cash</td>
<td>money is taken from the bank for unauthorised purposes</td>
<td>restricted list of signatories</td>
</tr>
</tbody>
</table>
5. Evaluation of an internal control system

Developing an adequate control system

- Determine the objectives of the particular system (e.g. HR - retaining good employees).
- Identify the current systems in place (e.g. interviews with employees).
- Determine what process inputs are required to meet the desired objective (e.g. appraisal review when good employees leave the company).
- Benchmark the process (e.g. target employee turnover rate).
- Any identified issues with the process must now be fixed through the implementation of new controls.

Costs vs benefits

The costs (as in any other business activity) should not outweigh the benefits. This may be difficult to assess, however, as the costs are sometimes non-financial.

Costs may include time spent by the management, training of new staff members, maintenance of the system, upgrades, monitoring, etc.

Benefits will be found in the reduction of the risks and achievement of the business objectives.

Limitations of internal control systems

The system can only provide reasonable assurance: there will always be risks, omissions and mistakes.

We cannot eliminate human nature (a bad manager will still be a bad manager).
6. Internal control applied to fraud

What is fraud

- Dishonestly obtaining an advantage, avoiding an obligation or causing a loss to another party.
- Fraud is a crime.
- There is a distinction between fraud and errors (unintentional mistakes).

Some examples of fraud:

- Crimes against customers, e.g. pyramid schemes; selling counterfeit goods.
- Employee fraud against employers, e.g. falsifying expense claims.
- Crimes against investors, consumers and employees, e.g. FS fraud.
- Crimes against financial institutions, e.g. fraudulent insurance claims.
- Crimes against government, e.g. social security benefit claims fraud; tax evasion.
- Crimes by professional criminals, e.g. money laundering; advance fee fraud.
- e-crime by people using computers, e.g. spamming, copyright crimes, hacking.

Prerequisites for fraud

- An ability to rationalise the fraudulent action and hence act with dishonesty.
- A perceived opportunity to commit fraud.
- A motive, incentive or pressure to commit fraud.
Fraud risk management strategy

Fraud prevention

- Anti-fraud culture
- Risk awareness
- Whistleblowing
- Sound internal control systems

A fraud policy statement, effective recruitment policies and good internal controls can minimise the risk of fraud.

Fraud detection

- Performing regular checks.
- Warning signals/fraud risk indicators:
  - failures in internal control procedures,
  - lack of information provided to auditors,
  - unusual behaviour by individual staff members,
  - accounting difficulties.
- Whistleblowers.
Fraud response

- Response plan:
  - internal disciplinary action,
  - civil litigation,
  - criminal prosecution,
  - responsibilities.

7. Chapter summary