5.2.1

CONTROL ENVIRONMENT

The control environment of an organisation refers to the **collective attitude, awareness and actions** of the Board, management and employees towards internal controls. It establishes the **tone at the top** for the entire company's control system and influences how employees perform their duties.

A strong control environment is one in which employees understand their roles, act within their authority and are committed to doing things correctly. It is fundamental to a company's health and sustainability, supporting **risk management, operational efficiency, regulatory compliance and accountability**. Ultimately, it builds **confidence among the Board and shareholders** that the company can achieve its goals while protecting its assets and upholding ethical standards.

For the Board, an effective control environment provides greater confidence that the company is well managed, key risks are identified, financial and non-financial information is reliable, and decisions are implemented responsibly. For the company, it supports better performance, fewer surprises, stronger accountability and a more disciplined use of resources. For shareholders and other stakeholders, it strengthens trust that the company acts lawfully, ethically and in line with its long-term interests.

The control environment consists of several **connected elements**. These include the company's values, ethics and culture; clear roles and responsibilities; the organisational structure; the competence and integrity of management and employees; policies and procedures; risk management practices; internal controls; reporting and escalation mechanisms; and the work of internal audit, external audit and compliance functions where applicable. A good control environment is not only a set of documents or formal procedures. It is also about **how people actually behave**, how decisions are made, how issues are reported, and whether accountability is applied consistently across the company.

The Board and management have different but complementary responsibilities in ensuring an effective control environment.

The **Board is responsible** for setting expectations, approving key policies, overseeing risk management and internal control systems, challenging management, and regularly assessing whether the control environment remains appropriate for the company's size, complexity, strategy and risk profile.

Management is responsible for designing, implementing and operating the control environment in practice. This includes establishing procedures, assigning responsibilities, monitoring compliance, addressing weaknesses, and ensuring that employees understand and follow the expected standards.

The Board should not manage controls on a daily basis, but it must ensure that management takes this responsibility seriously and that the Board receives reliable information on material risks and control issues.

Establishing and improving an effective control environment requires clear tone from the top, well-defined responsibilities, risk-based policies and controls, competent people, reliable reporting, effective assurance, timely correction of weaknesses and continuous review as the company and its risks evolve.

Key steps in establishing and improving an effective control environment are:

1. **Set the right tone at the top**
   The Board and management should clearly communicate that integrity, accountability, risk awareness and compliance are expected in all decisions and behaviours.
2. **Define clear roles and responsibilities**
   The company should clearly allocate decision-making authority, approval rights, reporting lines and accountability between the Board, management, control functions and employees.
3. **Assess key risks and control needs**
   The company should identify the main strategic, financial, operational, compliance, sustainability and reputational risks, and determine what controls are needed to manage them effectively.
4. **Establish policies and procedures**
   Key areas such as finance, procurement, conflicts of interest, delegations of authority, risk management, compliance, data protection, whistleblowing and reporting should be covered by clear and practical policies approved by the Board.
5. **Ensure competent people and adequate resources**
   The company should have people with the necessary skills, experience and authority to operate controls, manage risks and report issues properly.
6. **Create reliable reporting and escalation channels**
   Management and the Board should receive timely, accurate and relevant information on risks, incidents, breaches, control weaknesses and corrective actions.

7. **Monitor how controls work in practice**
   Controls should not only exist on paper. Management should regularly test whether they are actually followed and whether they remain effective.
8. **Use internal audit, external audit and compliance functions effectively**
   Where appropriate, independent assurance should help the Board and management understand whether the control environment is reliable and where improvements are needed.
9. **Address weaknesses and follow up on actions**
   Identified control gaps, audit findings or incidents should lead to clear corrective actions, responsible owners and deadlines, with regular follow-up.
10. **Review and improve continuously**
    The control environment should be updated when the company grows, changes strategy, enters new markets, digitalises processes, faces new risks or operates under new regulation.

Several well-known tools and frameworks can help a company to establish and maintain a sound control environment. The most useful for Boards are the following:

- **COSO Internal Control Framework**. This provides a structured approach to internal control, covering the control environment, risk assessment, control activities, information and communication, and monitoring. It is one of the most widely used internal control frameworks.
- **Three Lines Model**. This clarifies the roles of management, the risk and compliance functions and internal audit in managing and assuring risks and controls. It helps the Board to understand who is responsible for what.
- **ISO 31000 risk management standard**. This provides principles and guidance for identifying, analysing, evaluating, treating, monitoring and communicating risks across the organisation.
- **Delegation of authority matrix**. This sets clear approval rights for key decisions, such as investments, contracts, hiring, financing, procurement and transactions with related parties. It reduces confusion and strengthens accountability.
- Corporate governance **policies** and other **documents**, such as the risk appetite statement, Board and committee charters, code of conduct, ethics policy, conflict of interest policy and register, risk register and internal control register, internal audit plan, and whistleblowing policy and mechanism.

More on internal control and risk management can be found in sub-chapters 5.2.2 and 5.2.3.

The **success of a strong control environment** depends on several practical factors:

- First, there must be a clear tone at the top: the Board and management should consistently demonstrate integrity, accountability and respect for rules;
- Second, responsibilities must be clear, so that people know who is authorised to decide, approve, monitor and report;
- Third, the company needs reliable information flows, including timely reporting of risks, incidents, control failures and corrective actions;
- Fourth, the control environment should be proportionate: it should support the business and decision-making, not create unnecessary bureaucracy.

Finally, it should be regularly reviewed and improved, especially when the company grows, changes strategy, enters new markets, faces new regulation or experiences significant incidents. A strong control environment is therefore not a one-time exercise, but a continuous governance discipline.

KEY TAKEAWAYS

A. The control environment is the collective attitude, awareness and behaviour of the Board, management and employees towards internal control. It sets the tone for the whole control system and shows in how people actually behave, not only in the documents.

B. The Board sets expectations, approves key policies, oversees risk management and internal control, challenges management and regularly assesses whether the control environment fits the company's size, complexity, strategy and risk profile. Management designs and operates the controls.

C. A sound control environment rests on tone at the top, clear roles and responsibilities, risk-based policies and controls, competent people, reliable reporting and escalation, effective assurance, timely correction of weaknesses and continuous review.

D. Recognised tools help: the COSO Internal Control Framework, the Three Lines Model, ISO 31000, a delegation of authority matrix and a coherent set of governance policies.

E. The control environment should be proportionate, supporting the business and decision-making rather than creating bureaucracy, and it should be reviewed whenever the company grows, changes strategy, enters new markets, faces new regulation or experiences a significant incident.

QUESTIONS FOR THE BOARD

1. *Does the Board consistently demonstrate, in its own conduct and decisions, the integrity, accountability and respect for rules that it expects from the organisation?*
2. *Are decision-making authority, approval rights and reporting lines clearly allocated between the Board, management, control functions and employees, and documented in a delegation of authority matrix?*
3. *Which key policies has the Board approved, when were they last reviewed, and do they cover the areas that matter most for our risks?*
4. *Does the Board receive timely and reliable information on risks, incidents, control weaknesses and corrective actions, and what happened after the last significant finding?*
5. *Do we know whether our controls are actually followed in practice, and who tests this?*
6. *Is our control environment proportionate to our size and risks, and when did we last review it after a change in the business?*