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?*

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."

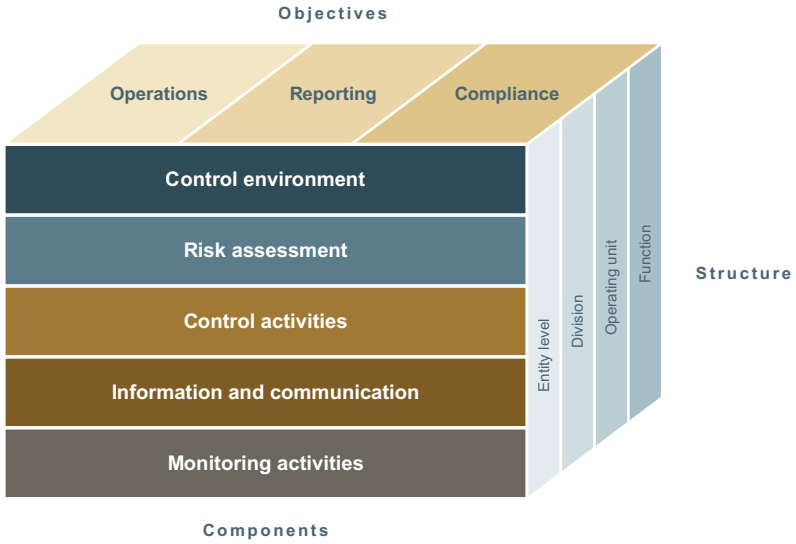
10 Committee of Sponsoring Organizations of the Treadway Commission (COSO), https://www.coso.org/.

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?*

5.2.3

RISK GOVERNANCE, THREE LINES MODEL

The complexity of the business environment and growing uncertainty demand from companies and their Boards a deep understanding of the link between risk and reward in achieving the strategic objectives. Effective risk management enables the Board to pursue the company's strategic objectives with a clear understanding of the risks it is willing to take, reducing surprises and losses, clarifying accountability, strengthening resilience and stakeholder confidence, and revealing opportunities as well as threats.

In the process of risk governance and management it is important to clearly define the roles of the Board, the Board committee responsible for risk oversight, the CEO, the risk officer, management, employees and internal audit.

The Board bears ultimate responsibility for the establishment and oversight of the risk governance system within the company, setting the risk appetite and risk tolerance levels, as well as for making strategic decisions and involving itself in approving or guiding major strategic risks. The Board sets the tone of the risk culture within the company.

The Board risk committee (or any other relevant Board committee involved in risk governance) is a corporate body that **assists** the Board in performing risk oversight by monitoring the risk management processes in greater depth, conducting regular reviews of the effectiveness of the company’s risk management processes, evaluating the identification, assessment and mitigation of risks, participating in the development and review of risk management policies and procedures, providing guidance and recommendations to the Board on risk-related decisions, and remaining accountable to the Board.

The Chief Executive Officer (CEO) has ultimate responsibility for the overall success of the risk management process at the operational, day-to-day level. The CEO ensures the effectiveness of risk management and emphasises its importance throughout the organisation.

The Chief Risk Officer (CRO) coordinates and supports the risk management process within the company. The CRO helps to identify and assess risks across the various aspects of the business, develops and helps to implement strategies to

mitigate identified risks, and reports regularly to the CEO, the relevant Board committee and the Board on the status of risks and risk management efforts.

Employees should be aware of, understand and manage the risks associated with their roles and the functions for which they are responsible. They are expected to report potential risks or issues to their supervisors and the Chief Risk Officer.

Internal audit is responsible for the independent evaluation of the quality and effectiveness of the risk management system as a whole. Internal audit is accountable not to the CEO but directly to the Board, and provides reports, insights and recommendations directly to the Board and the relevant Board committee.

Risk appetite

- Risk appetite is the amount of risk an entity is willing to accept in pursuit of value.
- Risk appetite is directly related to the entity's strategy. It is considered in strategy-setting, where the desired return from a strategy should be aligned with the entity's risk appetite. Different strategies expose the entity to different risks.
- The entity's risk appetite guides resource allocation. Management allocates resources across business units with consideration of the entity's risk appetite and each business unit's strategy for generating the desired return on invested resources.

Risk tolerance

- Risk tolerances are the **acceptable levels of variation relative to the achievement of objectives**.
- Risk tolerances can be measured, and are often best measured in the same units as the related objectives. Performance measures are aligned to help ensure that actual results remain within the acceptable risk tolerances.
- In setting risk tolerances, management considers the relative importance of the related objectives and aligns the risk tolerances with the risk appetite.

The four steps of risk management

Risk management is a continuous cycle that the company repeats as its business and environment change: identify the risks, evaluate them, decide how to respond and monitor the result. Management runs the cycle; the Board sets its direction and oversees it. Good practice starts with a clear statement of risk appetite, approved by the Board, which defines how much risk the company is willing to take in pursuit

of its objectives and gives each of the four steps a common reference point. A Board that understands the cycle well is able to judge whether management performs each step properly, to ask the right questions at each stage and to recognise the moments when its own decision is required. There are four key steps in the risk cycle.

Step 1. Identify

The first step is to establish what could prevent the company from achieving its objectives, and what opportunities it might be missing. This is done by management, ideally with the involvement of people from across the business, since the risks that matter most are often visible only to those closest to operations, customers or technology. Sources include strategic reviews, workshops, incident and near-miss records, audit findings, external reports and scenario analysis. The output is a risk register: a living list in which each risk has a description, a category (strategic, financial, operational, compliance, reputational, technology, sustainability) and a named owner. For the Board, the practical questions are whether the register is complete rather than long, whether it looks forward as well as backward, and whether emerging risks such as cyber threats, regulatory change, climate transition or a concentration of key suppliers or customers have been considered. A register that has not changed in two years is a warning sign in itself.

In practice, risk owners often find it difficult to identify the risks in the processes for which they are responsible. To help with this initial task, see Annex 3, Risk categories and types.

Step 2. Evaluate

Each identified risk is then assessed by its likelihood and its potential impact, taking into account the controls that already exist. The result is usually expressed on a simple scale and plotted on a likelihood–impact matrix, which allows the company to distinguish the few risks that require Board attention from the many that management handles in the ordinary course of business. Evaluation should consider the inherent risk (before controls) and the residual risk (after controls), because the gap between the two shows how much the company depends on its controls working. It should also consider velocity, that is how quickly a risk could materialise, and the possibility of several risks occurring together. The Board should expect the evaluation to be honest rather than comfortable, should challenge scores that seem too optimistic or too high (a useful check is to compare how similar risks have been scored by different units) and should ask how the residual risk compares with the risk appetite and tolerances it has set.

Step 3. Respond

For each significant risk the company chooses a response: avoid the risk by stopping or not starting the activity that creates it; reduce it through controls, procedures and training; transfer all or part of it to a third party through insurance, contract, outsourcing or hedging; or accept it knowingly and keep it under watch. The choice is guided by the risk appetite and by the cost of the response compared with its benefit. Some responses require the Board's own decision, for example withdrawing from a market, changing the capital structure or entering into a major insurance or hedging programme, while most are decided by management within the limits the Board has set. Whatever the choice, it should be recorded in the risk register with the responsible owner, the actions to be taken and the deadline. The most common failure at this step is a response that exists on paper only; the Board should ask not only what the response is but whether it has actually been implemented. Risks may also present opportunities, and a good response considers whether the company could take more of a well-understood risk rather than less.

Step 4. Monitor

The final step keeps the cycle alive. Management tracks the risks through key risk indicators, reviews the register at least quarterly and reports material changes, incidents and near misses to the Board or its risk or audit committee. Internal audit, as the third line, independently tests whether the controls and responses work as intended, and the external auditor and other assurance providers add their own perspective. Monitoring is also where learning happens: every incident should be followed by a short review of what the risk register said before it happened and what needs to change. The Board's role is to receive reporting that is timely and integrated rather than fragmented, to see that the actions agreed at step 3 are completed, and to review at least once a year whether the risk management system as a whole, including the risk appetite, still fits the company's strategy, size and environment. It is good practice for the Board to review the principal risks and the progress of the risk responses each quarter, while the risk or audit committee conducts the deeper analysis. The recommended elements of a risk register are listed in Annex 4.

What the Board should do

In practice the Board's involvement in the cycle comes down to a few recurring actions: set and periodically revisit the risk appetite and tolerances; approve the risk management policy and the allocation of roles under the Three Lines Model; review the principal risks and their responses at least once a year and the risk register more often through a committee; take the decisions that are reserved for it; and

obtain independent assurance that the cycle operates in reality and not only in the documents. A Board that does these things consistently will rarely be surprised, and when it is, it will be in a position to respond quickly.

Figure 5.2 **Risk matrix: evaluating risks by likelihood and impact**



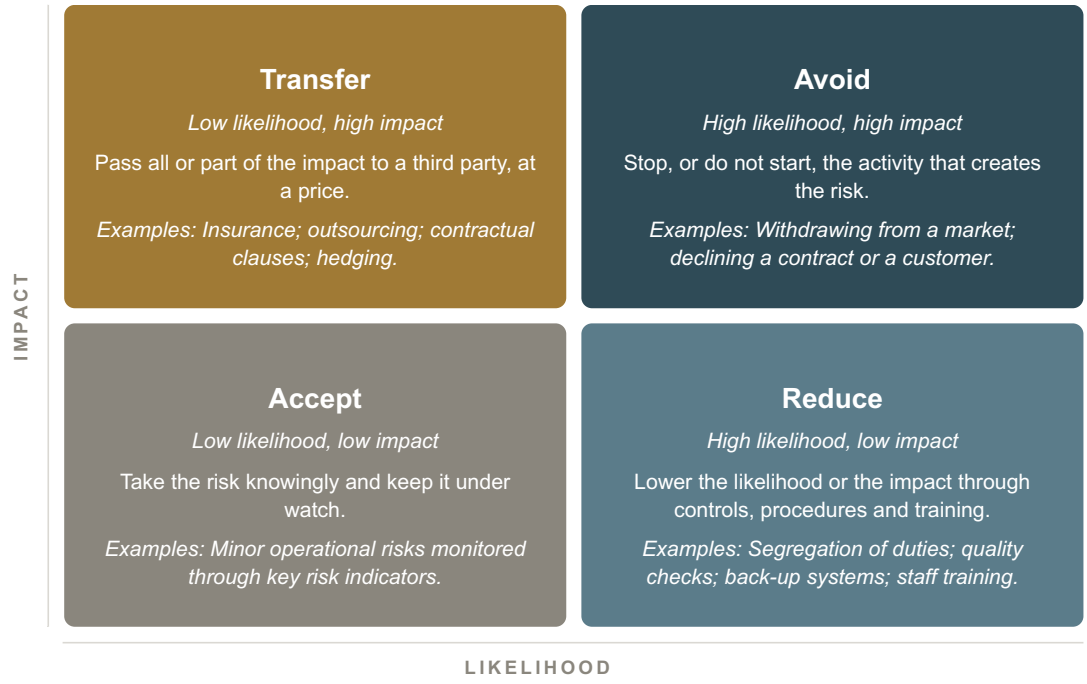
Score = likelihood (1–5) × impact (1–5). The scales, thresholds and colours should be adapted to the company's size and risk appetite.

The risk matrix is the most common tool for the second step of the risk management cycle. Each risk is scored for likelihood and for impact on a scale of one to five, and the product of the two places it in one of four levels. Risks in the low band are accepted and monitored; risks in the medium band are managed through controls and reported by their owners; risks in the high band require an action plan and the attention of the risk or audit committee or the Board; and risks in the extreme band are outside the risk appetite and call for immediate action and a Board decision. The matrix should be applied to the residual risk, after existing controls, and the scales, thresholds and colours should be defined in the company's risk management policy and adapted to its size and risk appetite.

Four strategies for risk response

Once a risk is assessed by likelihood and impact, the company chooses one of four responses: avoid, reduce, transfer or accept. The choice should reflect the Board-approved risk appetite and the cost-benefit of the response. Each response should be recorded in the risk register, assigned to a risk owner and monitored through appropriate indicators and assurance activities.

Figure 5.3 **Four strategies for risk response by likelihood and impact**



Avoiding a risk means eliminating the threat entirely by choosing not to engage in the activity that carries the risk. For instance, a company may decide not to expand into a new country with an unstable political climate, to avoid the risk of asset seizure or business disruption.

Transferring a risk means shifting the financial and/or operational burden of a risk to a third party, for example by purchasing an insurance policy or outsourcing the company's IT services to a specialised firm, thereby transferring the technical risks associated with network security and maintenance to the third-party provider.

Reducing, or mitigating, a risk involves taking steps to lower the probability or the impact of a risk. This is the most common strategy and is used when a risk cannot be avoided completely but its effects can be managed. A construction company might reduce the risk of on-site injuries by enforcing strict safety protocols and providing personal protective equipment; to reduce the risk of a data breach, a company might invest in stronger cybersecurity software, implement multi-factor authentication and provide mandatory training for all employees on phishing.

Accepting a risk involves making a conscious decision to take no action to reduce or transfer the risk, and simply to absorb the consequences if it occurs. This is typically done for risks with low probability and low impact, where the cost of a response would be greater than the potential damage. A company might accept the minor risk of currency fluctuations when doing a small amount of business abroad, as the cost of hedging would outweigh the potential losses. Similarly, a project

manager might accept the risk of a minor, non-critical task running a day late, knowing that it will not affect the project's overall deadline.

Risk management frameworks

There are several risk management frameworks. The most widely used are the COSO Enterprise Risk Management – Integrating with Strategy and Performance and the ISO 31000 standard.

ISO 31000 is an international standard recognised globally. It provides a common language for risk management, making it easier for companies operating in different countries or industries to communicate about risk. The standard is known for its flexibility: it provides principles and guidelines rather than specific requirements, allowing organisations to adapt the framework to their specific needs and contexts. [12]

COSO provides a comprehensive framework that covers internal control, enterprise risk management and fraud deterrence. It is well established and widely used. It integrates risk management with internal control, which can be beneficial for companies looking to align risk management with broader governance and control activities. The framework focuses on aligning risk management with the achievement of organisational objectives, helping organisations to better understand and manage the risks that might affect their goals.

The suitability of a particular framework depends on the organisation's needs, industry and preferences.

Enterprise risk management: the culture, capabilities, and practices integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving and realizing value. [13]

12 ISO 31000:2018, Risk management – Guidelines. Introductory materials: https://practicalrisktraining.com/iso31000; https://pecb.com/whitepaper/iso-31000-risk-management--principles-and-guidelines.
13 COSO (2017), Enterprise Risk Management – Integrating with Strategy and Performance, https://www.coso.org/pages/erm-integratedframework.aspx.

Figure 5.4 **COSO Enterprise Risk Management framework: five components and twenty principles**



Source: adapted from the Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management – Integrating with Strategy and Performance, 2017.

Three Lines Model

The Three Lines Model (known until 2020 as the Three Lines of Defence Model, and refreshed in July 2026) is a governance and risk management framework developed by the Institute of Internal Auditors (IIA). It provides clarity on roles and responsibilities in risk management, assurance, and oversight. Additionally, it ensures that value creation, risk-taking, and accountability are aligned across the organisation.[14]

While the COSO Framework explains and helps to design and evaluate effective internal control processes, the Three Lines Model explains who does what in governance, risk, control and assurance, and ensures clear roles and accountability.

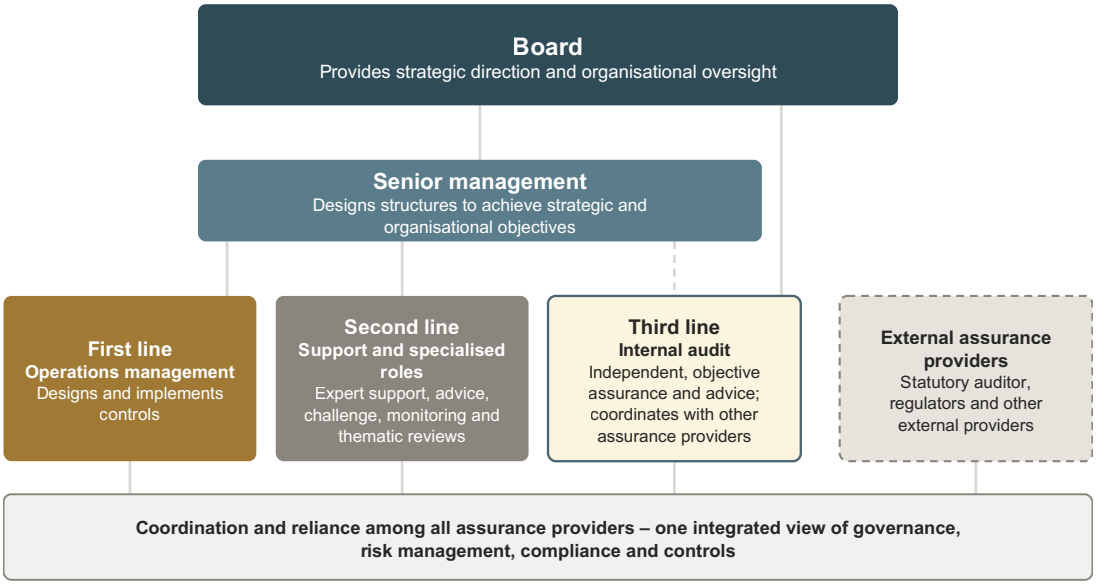
Benefits of implementing the Three Lines Model in a company:

- Clarifies roles, responsibilities and accountability – prevents gaps and overlaps in risk management.
- Strengthens governance – supports the Board's oversight role.
- Enhances resilience – enables early risk detection and effective response.
- Improves assurance – ensures that the Board receives reliable, objective information.

14 The Institute of Internal Auditors, www.theiia.org.

– Meets stakeholder expectations – regulators, investors and rating agencies increasingly expect structured governance models.

Figure 5.5 The Three Lines Model (The IIA, refreshed in July 2026)



Solid line: functional reporting and oversight Dashed line: administrative reporting Dashed border: outside the organisation

Source: adapted from The Institute of Internal Auditors, Assurance and Advice in Support of Effective Governance: Three Lines Model, Statement of Position, 2026.

Each of the three lines ***plays a distinct role*** in the company's control environment:

1. The first line (functions that own and manage risks)
   This line is formed by the managers and staff who are responsible for identifying and managing risk as part of their accountability for achieving objectives. Collectively, they should have the necessary knowledge, skills, information and authority to operate the relevant risk control policies and procedures. This requires an understanding of the company, its objectives, the environment in which it operates and the risks it faces. These are the operational teams directly involved in delivering products or services; they own and manage the risks related to their daily activities.

2. The second line (functions that oversee, or specialise in, compliance or the management of risk)

   These are the specialists in areas such as risk management, compliance, quality control or finance, who monitor and oversee the first line's risk management activities, ensure adherence to policies and regulations, and help the first line to set up the right tools and processes for managing risk.

The second line provides the policies, frameworks, tools, techniques and support that enable risk and compliance to be managed in the first line, conducts monitoring to judge how effectively this is done, and helps to ensure consistency in the definition and measurement of risk.

3. The third line (functions that provide independent assurance)
   This is provided by internal audit. Sitting outside the risk management processes of the first two lines, its main roles are to ensure that the first two lines are operating effectively and to advise how they could be improved. Tasked by, and reporting to, the Board or audit committee, it provides a risk-based evaluation of the effectiveness of governance, risk management and internal control to the organisation's governing body and senior management. It can also give assurance to sector regulators and external auditors that appropriate controls and processes are in place and operating effectively.

The structure of the **model refreshed in 2026** is unchanged, but the emphasis has shifted. **Assurance and advice are now treated as distinct but complementary**: assurance confirms whether processes are adequate and effective, and is credible only where the provider neither designs nor operates the process, while advice identifies improvements and emerging issues and allows closer collaboration with management. The **refreshed model calls for coordination and reliance among all assurance providers**, internal and external, to reduce overlap and "assurance fatigue", and **names internal audit as the integrator** that **gives the Board one system-wide view** of how governance, risk management, compliance and controls work together. **Independence is defined more precisely**, through functional reporting to the Board, autonomy over scope, unrestricted access to information, adequate resources and protection from retaliation, but "should not be interpreted as isolation". Finally, the model accepts that roles in real companies are often blended and **sets out safeguards for such cases, such as Board approval, clear separation of activities, full disclosure and periodic independent review**, while confirming that outsourcing an activity change neither its place in the model nor the Board's accountability.[15]

Recommendations for the Board

1. ***Set the tone***: endorse and actively support the use of the Three Lines Model.
2. ***Demand clarity***: request clear definitions of roles, responsibilities and accountabilities across the lines.
3. ***Monitor balance***: ensure no line becomes too dominant or too weak.

---

15 The IIA (2026), Assurance and Advice in Support of Effective Governance: Three Lines Model, Statement of Position.

4. ***Ensure the independence of internal audit***: its reporting line should go directly to the audit committee or the Board.
5. ***Promote collaboration***: encourage open communication among all three lines to prevent duplication or blind spots.
6. ***Request integrated assurance reporting***: ensure that the Board receives a consolidated view of risks, controls and assurance.
7. ***Review effectiveness regularly***: include the effectiveness of the model in governance reviews.
8. ***Stay informed***: request regular training or updates on governance, risk and assurance frameworks.

The most common mistakes in implementing the Three Lines Model:

- Lack of tone at the top from the Board.
- Treating it as a rigid checklist instead of a flexible model adapted to the organisation's needs.
- Blurred role boundaries – e.g. management expecting internal audit to design controls, or risk and compliance functions acting as internal auditors.
- Poor communication between lines – leading to duplicated or missed assurance.
- Underestimating the Board's role – some Boards assume the model is only for management, but the governance tone must come from the top.
- Overloading the third line with both advisory and assurance duties, undermining independence.

More information on this model is available on the IIA website.[16]

KEY TAKEAWAYS

A. The Board bears ultimate responsibility for the risk governance system: it sets the risk appetite and risk tolerances, approves or guides major strategic risks and sets the tone of the risk culture. A risk committee, where established, prepares this work but remains accountable to the Board.

B. Roles must be clear: the CEO is responsible for risk management at the operational level, the Chief Risk Officer coordinates and reports, employees manage the risks of their own roles, and internal audit independently evaluates the whole system and reports directly to the Board.

C. Risk management follows four steps: identify the risks, evaluate them by likelihood, impact and control effectiveness, select a response (avoid, transfer, reduce or accept) and monitor through a risk register, key risk indicators and audits.

D. Risk appetite is the amount of risk the company is willing to accept in pursuit of value; risk tolerances are the acceptable variations around objectives. Both should be set with the strategy and guide resource allocation. Risks may also present opportunities.

E. The Three Lines Model clarifies who does what: the first line owns and manages risk, the second line provides expertise, oversight and monitoring, and the third line (internal audit) provides independent assurance to the Board. Its most common failures are a lack of tone at the top, blurred role boundaries and poor communication between the lines.

QUESTIONS FOR THE BOARD

1. *Has the Board set the company's risk appetite and risk tolerances, and are they linked to the strategy and used in resource allocation?*
2. *Are the roles of the Board, its risk committee, the CEO, the risk officer, employees and internal audit in risk governance clearly defined and understood?*
3. *Do we maintain a current risk register with risk owners, key risk indicators and mitigation measures, and when did the Board last review it?*
4. *For our most significant risks, has the Board consciously chosen a response (avoid, transfer, reduce or accept) rather than accepting them by default?*
5. *Do the three lines in our company work as intended: does the first line own its risks, does the second line have the authority to challenge it, and does internal audit report directly to the Board?*
6. *Does the Board receive an integrated view of risks, controls and assurance, and is the effectiveness of the risk governance system itself reviewed regularly?*

16 The Institute of Internal Auditors, www.theiia.org.

5.2.4

RESILIENCE: CRISIS PREPAREDNESS, BUSINESS CONTINUITY AND RECOVERY

Why resilience matters

Corporate resilience is the ability of a company to anticipate, prepare for, respond to and recover from significant disruptions while protecting its people, assets, operations, reputation and long-term value. Resilience is not limited to emergency response. It includes crisis preparedness, business continuity, disaster recovery, communication with stakeholders, and the ability to learn and adapt after disruption.

The importance of resilience has increased significantly in recent years due to geopolitical instability, cyber threats, pandemics, supply chain disruption, climate-related events, energy insecurity, regulatory change and social expectations. The G20/OECD Principles of Corporate Governance expressly include a chapter on **Sustainability and resilience**, and emphasise that Boards should consider material sustainability risks and opportunities when reviewing strategy, risk management and internal control systems.

For the Board, resilience is not an operational detail to be left entirely to management. It is part of the Board's responsibility for strategic guidance, effective monitoring of management, risk oversight and accountability to the company and its shareholders.

In the European Union, resilience's importance is increasing as a legal requirement as well as good practice. The NIS2 Directive on cybersecurity, the Digital Operational Resilience Act (DORA) for the financial sector and the Critical Entities Resilience Directive, as transposed in Estonia, Latvia and Lithuania, require many companies to manage their risks, maintain business continuity and report significant incidents, and in several cases place explicit responsibility on the management body. The Board should know which of these regimes apply to the company and how compliance is assured.[17]

What corporate resilience includes

Corporate resilience should be understood as an integrated governance framework and as a legal duty of the companies and their Boards covering four connected

17 Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS2); Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA); Directive (EU) 2022/2557 on the resilience of critical entities (CER).

areas, supported by crisis communication and by learning from every incident, both of which are addressed below:

Crisis preparedness means the company's readiness to identify, assess and prepare for serious events that may threaten its operations, people, financial position, licence to operate or reputation.

Emergency response means the immediate actions taken when an incident occurs, including protection of life and health, mitigation of damage, activation of crisis teams, internal escalation and communication with relevant authorities and stakeholders.

Business continuity means the ability of the company to continue its most critical activities at an acceptable level during disruption. A business continuity plan identifies critical functions, key dependencies, minimum service levels, alternative processes, responsibilities and recovery priorities.

Disaster recovery usually refers to the restoration of critical systems, infrastructure, data and technology after a disruption. It is particularly relevant for IT, cybersecurity, data protection, operational technology and other infrastructure on which business continuity depends.

These areas should not be managed as separate documents without coordination. A company may have a crisis management plan, business continuity plan, disaster recovery plan, cyber incident response plan, communication plan and other related documents, but they should form one coherent resilience framework. The Board should be able to understand how these documents fit together, who owns them, when they are activated, and how they are tested.

The Board's role in resilience

The Board is not expected to manage an emergency on a day-to-day basis. Operational responsibility normally belongs to the CEO and management. However, the Board should ensure that the company has an appropriate resilience framework, that management is prepared for serious disruptions, and that the company can continue to protect long-term value under stress.

The Board should approve the company's overall approach to resilience, including the risk appetite, governance structure, reporting arrangements and escalation criteria. It should satisfy itself that resilience is embedded in strategy, risk management, internal control, compliance, sustainability and capital allocation.

The Board should also ensure that the company has identified its most material disruption scenarios. These may include cyberattacks, loss of key systems, loss of premises, supply chain failure, energy disruption, industrial accidents, fraud, regulatory intervention, sanctions exposure, pandemics, extreme weather events, product safety incidents, liquidity shocks, reputational crises or loss of key people.

A mature Board should not only ask whether plans exist. It should ask whether they are realistic, tested, understood by the right people, supported by adequate resources, and capable of being executed under pressure.

Responsibilities of management

Management is responsible for designing, implementing and maintaining the company's resilience arrangements. This includes preparing relevant plans, assigning roles, training employees, maintaining emergency contacts, ensuring data back-up and system recovery, engaging with critical suppliers, organising simulations and reporting material weaknesses to the Board.

Management should ensure that the company has clear procedures for incident detection, escalation, decision-making and communication. In a crisis, delays, uncertainty and unclear authority may cause as much damage as the incident itself. Therefore, the company should know in advance who has authority to activate the crisis plan, who leads the crisis team, who communicates with employees, regulators, customers, shareholders and media, and when the Board must be informed or convened.

Management should also maintain an up-to-date view of critical dependencies. These include key people, key suppliers, technology systems, outsourced service providers, premises, logistics, licences, funding arrangements, insurance cover and regulatory permissions.

Crisis management and emergency response

A crisis may develop rapidly and under conditions of uncertainty. The purpose of crisis management arrangements is to ensure that the company can make timely, coordinated and well-informed decisions when normal management processes are insufficient.

A crisis management plan should define:

AREA	KEY QUESTION
1. **Activation**	What events trigger the crisis plan?
2. **Escalation**	When must the CEO, Chair, Board or committee be informed?

AREA	KEY QUESTION
3. **Crisis team**	Who is responsible for leading the response?
4. **Decision authority**	Who can make urgent decisions?
5. **Stakeholder communication**	Who communicates with whom, and through which channels?
6. **Regulatory obligations**	Which notifications may be required?
7. **Documentation**	How are decisions and actions recorded?
8. **Recovery**	How does the company return to normal operations?
9. **Learning**	How are lessons identified and implemented?

The Board should agree in advance which events require immediate notification to the Chair, the full Board or a relevant Board committee. For example, the Board should normally be informed promptly of incidents that may have a material impact on people's safety, financial stability, legal compliance, market disclosure, reputation, business continuity, data security or licence to operate.

Business continuity plan

A business continuity plan should identify how the company will continue its essential operations during a disruption. It should be practical, proportionate and tailored to the company's size, sector, complexity and risk profile.

At a minimum, the business continuity plan should address:

AREA	MATTERS TO BE COVERED
1. **Critical functions**	Which activities must continue during disruption
2. **Recovery priorities**	Which services, processes or sites must be restored first
3. **Minimum acceptable level of service**	What level of operation is acceptable during disruption
4. **Roles and responsibilities**	Who activates and manages the plan
5. **Key dependencies**	People, systems, suppliers, premises, data and funding
6. **Alternative arrangements**	Remote work, substitute suppliers, alternative sites, manual processes
7. **Communication**	Employees, customers, regulators, shareholders, suppliers and media

AREA	MATTERS TO BE COVERED
8. **Testing**	Exercises, simulations and lessons learned
9. **Review cycle**	Regular updates and approval process

The business continuity plan should not be a formal document prepared only for compliance purposes. It should be capable of being used in real time. The Board should therefore receive assurance that the plan is up-to-date, tested and known by the relevant people.

Disaster recovery plan

A disaster recovery plan should set out how the company will restore critical systems, data, infrastructure and technology following a major disruption. For many companies, disaster recovery is closely linked to cybersecurity, data protection, digital operations, customer service and financial reporting.

The disaster recovery plan should define recovery time objectives and recovery point objectives (RTO and RPO) for critical systems. In simple terms, the company should know how quickly each critical system must be restored and how much data loss, if any, is acceptable. The plan should also address back-up arrangements, access rights, third-party service providers, cloud infrastructure, alternative communication channels and manual workarounds.

The Board does not need to review every technical detail. However, it should understand whether recovery assumptions are realistic, whether critical systems have been tested, whether there are single points of failure, and whether the company has adequate cyber and technology resilience.

Crisis communication

Communication is a central part of resilience. In a crisis, unclear or inconsistent communication can damage trust, increase legal risk and undermine the company’s reputation. The company should have prepared communication protocols for employees, customers, regulators, shareholders, creditors, suppliers, communities, media and other relevant stakeholders.

The Board should ensure that the company’s communication approach is accurate, timely, responsible and aligned with legal obligations. For listed companies, crisis communication may also involve market disclosure obligations. For regulated companies, communication with supervisory authorities may be critical. For companies providing essential services, communication with customers, municipalities, government bodies and the public may be equally important.

The company should avoid both excessive silence and premature speculation. Good crisis communication should explain what is known, what is being done, what stakeholders should do, and when further information can be expected.

The Board should ensure that the company has a written crisis communication plan that is approved at the appropriate management level and reviewed by the Board or relevant Board committee. The plan should be proportionate to the company's size, sector, ownership structure, regulatory status and risk profile.

Testing and Board assurance

Resilience cannot be assessed only by the existence of written plans. Plans should be tested through exercises, simulations, scenario discussions and post-incident reviews. Testing helps to reveal gaps in decision-making, communication, technology recovery, supplier readiness, employee awareness and Board escalation.

The Board should receive periodic assurance on resilience. This may include management reports, internal audit reviews, external assessments, cyber resilience testing, supplier resilience reviews, insurance reviews and tabletop exercises involving senior management and, where appropriate, Board members.

A useful practice is to conduct at least one annual Board-level resilience discussion. This may focus on a major scenario such as cyberattack, loss of a critical supplier, liquidity stress, geopolitical disruption, energy shortage, product safety incident or reputational crisis. The purpose is not to predict the future precisely, but to test whether the company can think and act under pressure.

Good governance practices

A company with a sound resilience framework will usually have the following features:

GOOD PRACTICE	EXPLANATION
Board-level oversight	The Board periodically reviews resilience risks, plans and test results
Clear management ownership	A senior executive is responsible for resilience coordination
Integrated plans	Crisis management, business continuity and disaster recovery plans are aligned
Defined escalation	The company knows when and how to inform the CEO, Chair and Board
Tested procedures	Plans are tested through realistic exercises

GOOD PRACTICE	EXPLANATION
Critical dependency mapping	Key systems, people, suppliers and sites are identified
Communication protocols	Internal and external communication responsibilities are clear
Supplier resilience	Critical third-party dependencies are reviewed
Cyber resilience	Technology recovery and cyber response are regularly tested
Lessons learned	Incidents and exercises lead to documented improvements
Regular reporting	The Board receives concise, decision-useful information
Proportionality	Arrangements reflect the company's size, sector and complexity

KEY TAKEAWAYS

A. Corporate resilience is the ability to anticipate, prepare for, respond to and recover from serious disruption while protecting people, assets, operations, reputation and long-term value. It is part of the Board's responsibility for strategy, risk oversight and accountability, not an operational detail.

B. Resilience is one integrated framework: crisis preparedness, emergency response, business continuity and disaster recovery, supported by crisis communication and learning from incidents. The Board should know how the plans fit together, who owns them, when they are activated and how they are tested and results assessed.

C. The Board does not manage emergencies, but it approves the overall approach and risk appetite, ensures that the most material disruption scenarios and critical dependencies have been identified, and agrees in advance which events must be escalated to the Chair, the Board or a committee.

D. For many companies' resilience is also a legal duty under EU rules such as NIS2, DORA and the Critical Entities Resilience Directive, with obligations on the management body.

E. Plans are only as good as their testing. The Board should receive periodic assurance on resilience and hold at least one Board-level resilience discussion a year around a major scenario.

F. Good crisis communication is prepared in advance for all key stakeholders, avoids both silence and speculation, and is aligned with disclosure and regulatory obligations.

QUESTIONS FOR THE BOARD

1. *What are the most serious disruption scenarios that could affect the company, and which activities, systems, people and suppliers are critical to continuing operations?*
2. *Do we have approved and tested crisis management, business continuity and disaster recovery plans, and do they form one coherent framework with clear ownership?*
3. *Who has the authority to activate the crisis plan, and when must the Chair, the Board or a Board committee be informed?*
4. *Which resilience-related legal regimes (NIS2, DORA, critical entities) apply to us, and how is compliance assured?*
5. *Have we tested crisis decision-making at senior management and Board level, and what did the last exercise, incident or near miss teach us?*
6. *Are our communication protocols clear for employees, regulators, shareholders, customers and the media, and consistent with our disclosure obligations?*
7. *Do we understand our critical third-party and outsourced dependencies, and is our insurance cover, including D&O, cyber and business interruption, adequate?*
8. *Does internal audit or another assurance provider review our resilience arrangements, and are resilience risks reflected in strategy, capital allocation and risk appetite?*
9. *In a group, are the group resilience policies suitable for each subsidiary, and could we continue critical operations if several disruptions occurred at the same time?*

5.2.5

CYBERSECURITY AND INFORMATION SECURITY OVERSIGHT

Cybersecurity oversight

With increased reliance on digital technologies, cybersecurity has become a significant concern. The Board is responsible for overseeing the company's cybersecurity measures, ensuring the protection of sensitive data and mitigating potential risks.

The key areas of its responsibility are:

1. ***Strategic oversight:*** integrate cybersecurity risks into the overall company strategy and ensure an understanding of how cyber threats could affect the business goals and financial performance of the entire organisation.
2. ***Oversight and accountability:***
    a. Be aware of and understand the key cyber risks. The Board should be informed about the most significant cyber risks the company faces and how management is addressing them.
    b. Monitor cyber resilience: oversee the company's ability to withstand and recover from cyberattacks.
3. ***Board expertise:*** the Board and its designated committee (if any) should have clear ownership of cybersecurity oversight. Board members may seek additional training, if needed, to fulfil this responsibility professionally and effectively.

By actively engaging in these areas, the Board can help the company to mitigate cyber risks and protect its critical assets, ensuring its resilience.

More on cybersecurity oversight can be found in "Cyber-Risk Oversight – Key Principles and Practical Guidance for Corporate Boards in Europe".[18]

Information security oversight

Information security is one of the core elements of corporate resilience, risk management and internal control. It covers the protection of the company's information, systems, data, networks, digital assets and critical technology infrastructure against unauthorised access, misuse, loss, disruption, manipulation or disclosure. It is directly linked to strategy, business continuity, legal compliance,

18 BICG (2020), Cyber-Risk Oversight – Key Principles and Practical Guidance for Corporate Boards in Europe, https://www.bicg.eu/wp-content/uploads/2020/09/Handbook-1.pdf.

customer trust, reputation, financial reporting, personal data protection, intellectual property and long-term value creation. It also supports operational resilience, strategic decision-making and the company's ability to maintain critical services during disruption.

The Board should ensure that the company has a clear information security policy, defined roles and responsibilities, and regular reporting to the Board and/or a relevant Board committee. Management should be able to explain which information assets and systems are critical, what the main threats are, what controls are in place, how incidents are detected and escalated, and how the company would respond to and recover from a serious cyber or information security incident.

Information security oversight should cover at least the following areas:

AREA	WHAT THE BOARD SHOULD ENSURE
Governance	Clear accountability for information security at executive level
Risk appetite	Agreed level of acceptable information security and cyber risk
Critical assets	Identification of critical data, systems, infrastructure, intellectual property, artificial intelligence systems and operational technology
Controls	Appropriate preventive, detective and corrective controls
Incident and crisis response	Tested procedures for detecting, escalating, responding to and recovering from incidents, including communication, authorities' notification and stakeholder coordination arrangements
Business continuity	Alignment between information security, business continuity and disaster recovery plans
Third parties	Oversight of information security risks from suppliers, cloud providers, outsourced services, software dependencies, supply chains and group companies
People	Employee awareness, access controls, training, insider-risk management and information security culture
Legal compliance	Compliance with data protection, cyber, sectoral and disclosure obligations
Assurance	Internal audit, external testing, penetration testing or independent reviews where appropriate
Reporting	Clear, concise and decision-useful reporting to the Board

The Board should receive regular information security reporting. Such reporting should not be limited to technical metrics. It should help the Board understand whether the company is operating within its risk appetite and whether management

is improving the company's resilience. Useful Board-level indicators may include material incidents and near misses, results of cyber exercises, status of critical remediation actions, employee training completion, phishing and social engineering test trends, vulnerability remediation, third-party risk exposure, audit findings, disaster recovery test results, insurance coverage and regulatory developments.

The Board should also ensure that the company periodically tests its information security arrangements. This may include tabletop exercises, cyber incident simulations, disaster recovery tests, penetration testing, supplier-risk reviews and crisis communication exercises. Lessons learned should be reported to the Board, with clear owners and deadlines for improvement actions.

The Board also plays an important role in setting the tone for security culture across the organisation. Information security should be treated as a shared business responsibility rather than solely a technical or IT matter.

Information security risks increasingly arise through third parties, outsourced services, software providers and interconnected supply chains. The Board should ensure that supplier risk management is proportionate to the company's critical services, dependencies and regulatory obligations, particularly where critical operations, data or technology services rely on external providers.

In company group structures, information security policies may be developed at group level. However, the Board of each subsidiary should consider whether group policies are suitable for the subsidiary's own business, systems, regulatory environment, risk profile and stakeholder interests. Group consistency is valuable, but it should not replace the subsidiary Board's responsibility to ensure that the subsidiary has adequate information security governance and resilience.

Effective Board oversight does not require technical expertise from every Board member, but it does require sufficient understanding to ask informed questions, challenge management and support informed decision-making.

The key expectation is that the Board should **oversee, challenge and assure**, not manage technical details. A robust information security framework should give the Board confidence that management understands the company's digital risks, has implemented proportionate controls, can respond effectively to incidents, manages critical dependencies and continuously improves the company's resilience and security culture.

KEY TAKEAWAYS

A. Cybersecurity and information security are strategic risk governance matters, not IT matters. The Board oversees, challenges and assures; it does not manage the technical detail, but it must understand enough to ask informed questions.

B. The Board should ensure that there is a clear information security policy, executive-level accountability, an agreed risk appetite for cyber and information risk, identified critical assets, proportionate controls and tested incident, continuity and recovery procedures.

C. Board reporting should go beyond technical metrics: material incidents and near misses, exercise results, remediation status, training and phishing test trends, third-party exposure, audit findings and regulatory developments.

D. Information security risks increasingly come through suppliers, cloud providers, software dependencies and group companies; supplier risk management must be proportionate to the company's critical dependencies.

E. In a group, each subsidiary Board remains responsible for ensuring that group policies are suitable for its own business and risk profile. The Board also sets the tone for a security culture in which information security is a shared business responsibility.

QUESTIONS FOR THE BOARD

1. *What are our most critical information assets, systems and data, and who is accountable for their security at executive level?*
2. *Is cyber and information security risk included in the company's risk appetite and risk register, and integrated into the strategy?*
3. *Which third-party, cloud and software dependencies could significantly disrupt our critical operations, and how are they overseen?*
4. *Do we understand the risks associated with emerging technologies, including artificial intelligence and automation?*
5. *How often does the Board receive information security reporting, and what were the most significant incidents, near misses or control weaknesses in the last year?*
6. *Have our incident response, business continuity and disaster recovery plans been tested, and were the lessons translated into concrete improvements?*
7. *Do we have sufficient internal expertise and independent external assurance, and are employees and managers properly trained?*
8. *Does the Board itself have sufficient understanding to challenge management on cyber risk, or should it seek training or expert support?*

5.2.6

INTERNAL AND EXTERNAL AUDIT

The Board (with the support of the audit committee) is responsible for the proper oversight of the company's control system. In this regard, the best friends of the Board and the audit committee are a well-functioning internal audit function and an independent, professional external auditor.

Responsibility for the development and operation of sound risk management and internal control systems lies with management. The Board (with the support of the audit committee) is responsible for the oversight of these processes.

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation to accomplish its objectives by bringing a systematic, disciplined approach to evaluating and improving the effectiveness of risk management, control and governance processes. The internal auditor is appointed by the Board, not by the CEO or Management Board, is not part of the management team and, unlike other employees, does not hold an operational role.

External (statutory or financial) auditing is the obligatory annual examination of a company's financial statements and records by an independent external auditor. The external auditor is approved by the shareholders on the recommendation of the Board.

Differences between the internal and external audit functions

ASPECT	INTERNAL AUDIT	EXTERNAL AUDIT
Who performs it?	Employees of the company or outsourced internal auditors	Independent third-party firm
Purpose	Improve internal operations, risk management, and controls; help the company achieve its goals	Provide an independent opinion on the fairness and accuracy of financial statements
Audience	Management and the Board and audit committee	Shareholders and other stakeholders (investors, creditors, regulators, public)
Scope	Broad; covers various aspects of the business (operations, compliance, IT, HR, cyber and other areas)	Primarily focused on financial statements and internal controls over financial reporting

ASPECT	INTERNAL AUDIT	EXTERNAL AUDIT
Reporting	Internal reports for the audit committee and the Board, with recommendations for improvement	Formal audit report, expressing an opinion on financial statements and presented to the audit committee, Board and shareholders
Independence	Organisational independence; not subordinate to the company's CEO or Management Board	Strict independence from the company being audited (no material ties, no provision of other services)
Mandatory?	Generally, not, but highly recommended for good governance	Usually legally mandatory
Frequency	Ongoing throughout the year	Typically, annual

Internal audit

Internal audit is a function within a company that is tasked with providing unbiased, independent reviews of systems and processes. That is why the internal auditor is the only non-operational function in the company. The role of internal audit is to provide the Board and top management with an objective source of information regarding the company's risks, control environment, operational effectiveness and compliance with applicable laws and regulations.

The reviews performed by Internal Audit are called internal audits. The aim of internal audits is to identify weaknesses within the organisation's processes and control environment internally so that they can be fixed as quickly as possible to prevent harm to the company or its stakeholders.[19]

Internal audit reports to the Board (and its audit committee), providing recommendations for the necessary improvements in systems and processes as well as reports on the implementation of those recommendations. It is important to emphasise that, where the Board has an audit committee, the Board should still maintain a regular relationship with the internal auditor and not delegate this important duty entirely to its audit committee, which supports the Board by examining internal audit activities in greater depth and providing opinions and suggestions for Board decisions.

It is important to emphasise that internal audit not only performs internal audits, but also advises the responsible company employees to help them achieve the set goals. Internal audit is the eyes and ears of the Board.

19 See also Linford & Co, Internal control environment, https://linfordco.com/blog/internal-control-environment/.

Internal audit should comply with the Global Internal Audit Standards of the IIA.[20]

The audit committee proposes, and the Board approves:

- the internal audit regulations;
- the strategic internal audit plan;
- the risk-based internal audit plan (three-year and annual);
- the internal audit budget (annually);
- the appointment, dismissal, evaluation and remuneration of the head of internal audit.

The head of internal audit must have functional accountability to the audit committee and the Board, and only administrative accountability to the CEO. It is the Board, not the CEO, that appoints the internal auditor, sets their remuneration and assesses their performance.

External audit

The responsibilities of the Board and its audit committee in relation to the external audit include:

1. ***Recommending the external auditor.*** The audit committee assesses potential audit firms (and the particular auditor) for independence, objectivity and expertise, and then recommends a firm (and the particular auditor) to the Board for appointment or reappointment by the shareholders.
2. ***Negotiating fees.*** The audit committee negotiates the auditor's fees to ensure that they are reasonable and will not compromise audit quality.
3. ***Reviewing the audit plan.*** The audit committee reviews and approves the external auditor's audit plan, including the scope of the work, the key risks identified and the planned resources.
4. The entire Board (including the audit committee) should ***meet the auditor twice*** during the annual audit cycle: before the audit, to share its insights into the situation in the company that could be relevant to the auditor and to learn about the audit plan, and after the audit, to discuss the findings and the auditor's report. ***In addition***, the audit committee should meet the auditor during the audit to discuss emerging findings.
5. The audit committee should ***assess the quality of the external auditor's work***.

20 The IIA (2024), Global Internal Audit Standards, https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/.

6. Ensure that the external auditor is invited to the annual general meeting of shareholders.
7. The Board, with the help of its audit committee, should ***follow up on the external auditor's recommendations***.
8. The Board should ***ensure the disclosure of the audit report*** (in the annual report and on the website).
9. Ensure that the auditor is rotated in line with the applicable rules: for public-interest entities, EU law requires rotation of the audit firm after no more than ten years and of the key audit partner after no more than seven years, unless national legislation sets other limits.
10. Pay close attention to the smoothness of the collaboration between the executives and the auditor.

KEY TAKEAWAYS

A. Management is responsible for sound risk management and internal control systems; the Board, with the support of the audit committee, is responsible for their oversight. Internal audit and the external auditor are the Board's principal sources of independent assurance.

B. Internal audit is an independent, objective assurance and consulting function that evaluates and improves risk management, control and governance. It is appointed by the Board, not the CEO, reports functionally to the Board and its audit committee, and is the only non-operational function in the company.

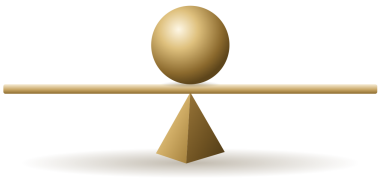
C. The audit committee proposes, and the Board approves, the internal audit regulations, the strategic and risk-based audit plans, the budget and the appointment, dismissal, evaluation and remuneration of the head of internal audit. Even with an audit committee, the full Board should maintain a direct relationship with the internal auditor.

D. External audit is the statutory annual examination of the financial statements by an independent auditor, approved by the shareholders on the Board's recommendation. The audit committee assesses the auditor's independence and quality, negotiates fees and reviews the audit plan.

E. The Board should meet the external auditor at least twice a year, follow up on the auditor's recommendations, ensure the audit report is disclosed and that rotation rules are observed, and watch the quality of the working relationship between executives and the auditor.

QUESTIONS FOR THE BOARD

1. *Does internal audit report functionally to the Board and its audit committee, and is it the Board, not the CEO, that appoints, evaluates and remunerates the head of internal audit?*
2. *Are the internal audit regulations, the strategic and annual risk-based audit plans and the budget approved by the Board, and do they cover the company's most significant risks?*
3. *How does the full Board, and not only the audit committee, engage with internal audit, and how are its recommendations followed up?*
4. *Has the audit committee assessed the external auditor's independence, expertise and quality of work, and are the fees adequate to secure a quality audit?*
5. *Did the Board meet the external auditor before and after the annual audit, and what did the auditor raise that management did not?*
6. *Are the auditor rotation requirements observed, is the auditor invited to the general meeting, and is the audit report disclosed in the annual report and on the website?*
7. *Does the relationship between executives and the auditor allow open and timely disclosure of issues, and would the Board know if it did not?*



CHAPTER

5.3

ETHICS AND INTEGRITY

How the Board sets and guards the company's ethical standard – from compliance and whistleblowing to conflicts of interest and related party transactions.

IN THIS SECTION

5.3.1	Ethics	134
5.3.2	Compliance	139
5.3.3	Whistleblowing	144
5.3.4	Conflict of interest	149
5.3.5	Related party transactions	154

5.3.1

ETHICS

Ethics is about doing what is right, not only what is required. The law and the corporate governance code set the minimum standards; ethics is the standard the company sets for itself, and the one by which its Board, management and people are judged when the rules are silent or inconvenient. Every company has an ethical standard in practice, whether or not it is written down. The question for the Board is whether that standard is chosen deliberately and upheld consistently, or left to emerge from habit and pressure.

This sub-chapter deals with the ethical standard itself and the Board's responsibility for it. Corporate culture and tone at the top are covered in sub-chapter 5.1.2; compliance, whistleblowing, conflicts of interest and related party transactions in sub-chapters 5.3.2 to 5.3.5; and the duty of loyalty of each Board member in sub-chapter 4.1.

Most corporate scandals begin not with an illegal act but with a series of lawful decisions that no one was willing to call wrong. Ethical failures destroy trust faster than financial ones. In the Baltic states, where markets are small and business and political networks overlap, the cost of an ethical lapse is high, and for state-owned and municipally owned enterprises public trust in the company is also public trust in its owner.

The role of the Board

The Board is the guardian of the company's ethical standard. It cannot delegate this role to a compliance function or a lawyer, because ethics is ultimately a matter of judgement, and the Board's judgement sets the ceiling for everyone else's. The Board's contribution has four parts. It defines the standard, by approving the code of ethics and the company's position on the dilemmas that matter in its business. It embodies the standard, by applying the same rules to itself and by the way it takes decisions. It tests the standard, by asking about the ethical dimension of what it approves and by refusing lawful but improper proposals. And it protects the standard, by ensuring that systems are in place to detect and correct breaches, and that consequences apply regardless of seniority.

Management runs the ethics programme: it drafts the code, designs training, handles day-to-day questions and investigates most incidents. The Board does not do this work, but it approves the framework, receives the evidence and holds management to account for the results. Where a Board committee exists, the audit committee or a dedicated ethics and compliance committee will usually prepare the