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**



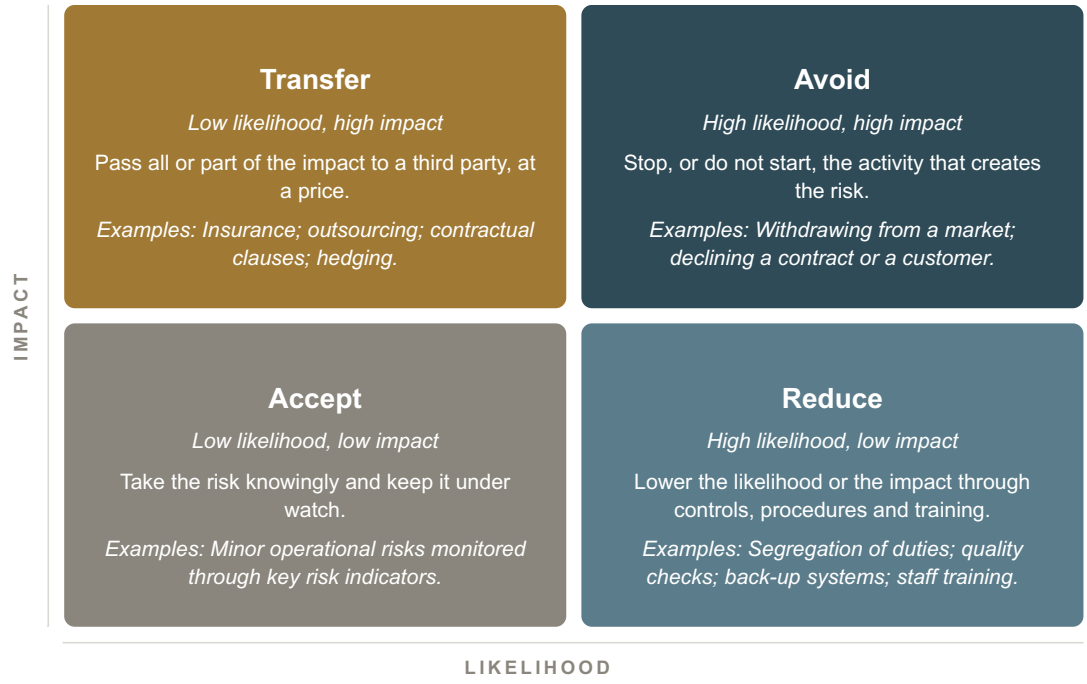
Score = likelihood (1–5) × impact (1–5). The scales, thresholds and colours should be adapted to the company's size and risk appetite.

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.

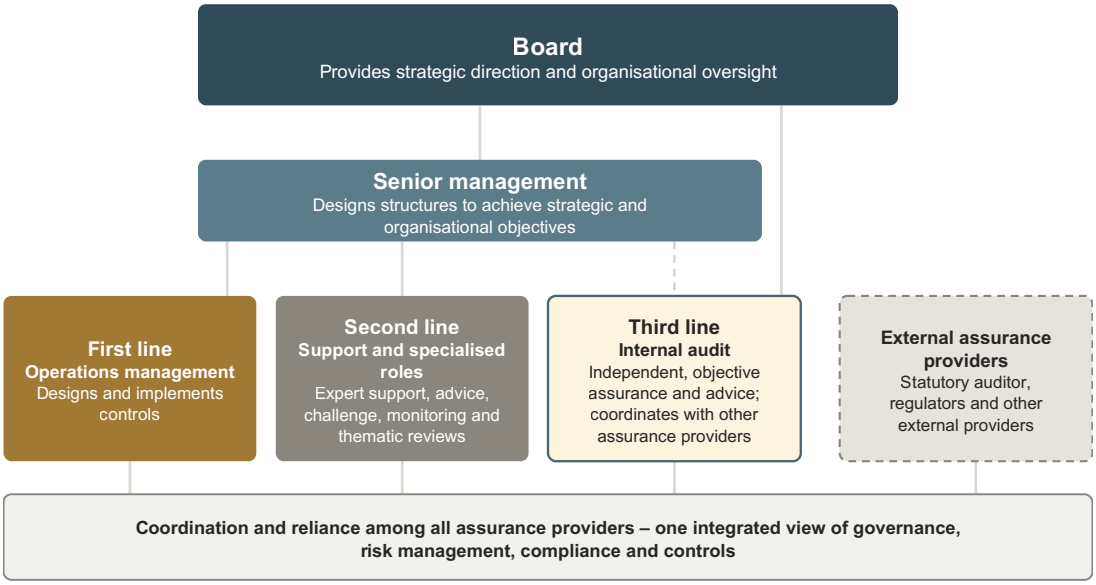
Benefits of implementing the Three Lines Model in a company:

- 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.