

CHAPTER

5

KEY AREAS OF BOARD ENGAGEMENT

The six areas in which the Board's attention creates the most value: direction, control, integrity, innovation, leadership and accountability.

IN THIS CHAPTER

5.1	Direction and value creation	62
5.2	Control, risk and assurance	92
5.3	Ethics and integrity	133
5.4	Technology and innovation	157
5.5	Leadership and remuneration	166
5.6	Shareholders, stakeholders and accountability	176



CHAPTER

5.1

DIRECTION AND VALUE CREATION

How the Board sets the company's direction, oversees strategy and protects long-term value – and where its role ends and management's begins.

IN THIS SECTION

5.1.1	Company's purpose, vision, mission and values	63
5.1.2	Corporate culture and tone at the top	68
5.1.3	The strategy cycle: building, updating, implementing	71
5.1.4	Integrating sustainability into company strategy, its oversight, sustainability reporting	77
5.1.5	Capital structure and dividend policy	82
5.1.6	Mergers, acquisitions and major transactions	86
5.1.7	Budget and KPIs for the company and CEO, performance monitoring and evaluation	90

5.1.1

COMPANY'S PURPOSE, VISION, MISSION AND VALUES

Before building the strategy, the Board should discuss with the shareholders what the purpose of the company is, and then set the vision, mission and values to provide clarity and direction for its employees, customers, stakeholders and the broader community. These elements serve as a foundation for the organisation's identity and guide its actions and decisions. There are numerous benefits for companies that have a well-established purpose, vision, mission and values, in particular:

- Clarity and focus: define and concentrate on long-term objectives.
- Guidance: support decision-making and strategy.
- Encourage purpose-driven business development.
- Inspire and motivate employees and attract top talent.
- Alignment: encourage collaboration and consistency.
- Competitive advantage: set the company apart from the competition.
- Improve branding and public relations through effective communication.
- Business sustainability: promote long-term growth.
- Resilience: navigate challenges based on purpose and values.
- Build public trust and reputation.
- Enable the company to have a broader and more meaningful impact on the world, beyond profit generation.

Purpose statement sets out the reason or reasons why an organisation exists. It defines the core reason for being and the positive impact the organisation wants to have on the world. The definition of the purpose leads to strategic choices and builds on cultural strengths to drive impact.

What is our purpose as an organisation, and how does it link with our "superpower", our capacity to make a distinctive contribution to the world?

Ask whether your purpose is:

1. Meaningful. In other words, does it make a real difference in people's lives? Does it have the potential to make a meaningful difference for all stakeholders?
2. Authentic. Does it match what people in the organisation care deeply about? Does it resonate with the company's values?

3. Credible. Does it draw on the organisation's unique abilities or assets? Can the company deliver in a way that makes a significant difference? Does it make business sense? Can it be translated into concrete actions?
4. Powerful. Are the needs the organisation addresses important and sizeable? How much good comes from addressing these needs?
5. Compelling. Is it clear, specific and aspirational enough to inspire and mobilise people both within and outside the organisation?

Examples of purpose statements:

- Telecommunication company: Inspire human progress through the power of communication and entertainment.
- Investment company: To help more and more people experience financial well-being.
- Beverage producer: Refresh the world. Make a difference.
- E-commerce company: To empower people and create economic opportunity for all.
- Automobile producer: To drive human progress through freedom of movement.
- Technology company: To create world-changing technology that enriches the lives of every person on earth.

Vision statement describes what the organisation will look like in the future: a big picture of what you want to achieve.

As you develop and review your vision statement, check for the following things:

1. Is it ambitious enough? The statement should feel aspirational, not like a finite goal to be accomplished.
2. Is it realistic enough? Make sure you strike a balance between the aspirational and the realistic.
3. Does it accurately reflect your organisation? Run the statement past internal stakeholders who were not involved in creating it, and ask for their feedback on what may be missing, which parts may be unnecessary, or how certain ideas may be phrased more effectively.
4. Does it make sense? Ask people outside the company to read the statement, to confirm that it makes sense to the average reader.

Examples of vision statements:

- Online technology company: To be Earth's most customer-centric company, where customers can find and discover anything they might want to buy online, and which endeavours to offer its customers the lowest possible prices.

- Financial services company: To become essential to our customers by providing differentiated products and services to help them achieve their aspirations.
- Computing technology company: To make the best products on earth and to leave the world better than we found it.
- Web technology company: To bring the metaverse to life and help people connect, find communities and grow businesses.
- Entertainment streaming company: Becoming the best global entertainment distribution service.

Mission statement describes what an organisation does and for whom, and how the vision will be achieved. The organisation's function, target audience and value proposition are elements often mentioned in a mission statement. The mission is an action statement that usually begins with the word "to".
It is important for:

- motivating employees;
- inspiring customers;
- strategic planning;
- setting values.

Examples of mission statements:

- Seller of furniture and home products: To offer a wide range of well-designed, functional home furnishing products at prices so low that as many people as possible will be able to afford them.
- Mass media and entertainment company: To entertain, inform and inspire people around the globe through the power of unparalleled storytelling.
- Business social media platform: To connect the world's professionals to make them more productive and successful.
- Athletic footwear and apparel producer: To bring inspiration and innovation to every athlete in the world.
- Construction toy production company: To inspire and develop the builders of tomorrow.

Double-check the uniqueness of your statements. They should not be too general and should not fit too many organisations.

Values are very important because they serve as guiding principles that help to shape the culture and behaviour of the company. Values also provide a shared

understanding of what is important for the company and help to align employees' actions with the company's mission and goals. They provide a framework for decision-making: when employees understand the company's values, they can use them as a reference point when making choices and solving problems, which leads to better outcomes and a more predictable corporate culture. Clearly defined values can also attract and retain employees who share them.

When defining the company's values, take into consideration the following aspects:

- Involve employees at all levels of the organisation in the process
- Ensure that your company values align with your purpose, mission and vision
- Keep them simple and easy to remember and apply
- Make them actionable: it should be clear how employees can demonstrate these values in their daily work
- Lead by example: senior management should set a good example and embrace the company's values.

A company's values are not just a statement of what the organisation believes in; they are a strategic tool for shaping culture, behaviour and decision-making. Values play a vital role in creating a positive and effective work environment and are a key component of an organisation's overall identity and success.

These statements are one of the primary starting points for the development of the strategy. They should be reviewed at the beginning of each strategy revision and amended if needed.

KEY TAKEAWAYS

A. Purpose, vision, mission and values are the foundation of strategy and of the company's identity. The Board should agree the purpose with the shareholders and then set the vision, mission and values before the strategy is built.

B. A purpose statement explains why the company exists; it should be meaningful, authentic, credible, powerful and compelling. A vision describes what the company will look like in the future; a mission describes what it does, for whom and how the vision will be achieved.

C. Values are a strategic tool, not a poster: they guide decisions and behaviour, shape culture and attract people who share them. They work only if they are simple, actionable, developed with employees and visibly practised by senior management.

D. The statements must be specific to the company; if they would fit any organisation, they are not doing their job. They should be reviewed at the start of every strategy revision and amended where needed.

QUESTIONS FOR THE BOARD

1. *Have we, together with the shareholders, agreed a purpose that explains why the company exists, and do our vision, mission and values follow from it?*
2. *Would our purpose, vision and mission statements fit almost any company, or do they clearly describe ours?*
3. *Were employees involved in defining the values, and can they say how the values apply to their daily work?*
4. *Does senior management visibly live the values, and does the Board see evidence of this in decisions, not only in communications?*
5. *When did we last review these statements against the strategy, and what changed as a result?*

5.1.2

CORPORATE CULTURE AND TONE AT THE TOP

Corporate culture is the pattern of behaviours that people in the organisation actually follow when no one is watching – how decisions are made, how bad news travels, how rules are applied when they are inconvenient. Tone at the top is the signal the Board and executive management send about which behaviours are rewarded, tolerated or punished. The two are inseparable: culture rarely rises above the standard that its leaders visibly practise. Policies, codes of conduct and training matter, but employees watch what leaders do far more closely than what they publish. A single decision – a sales target met by cutting corners and celebrated anyway, a senior manager whose misconduct is quietly overlooked – can undo years of compliance messaging.

Culture is not a soft topic to be delegated to the human resources function. It is a governance matter, because most corporate failures – fraud, safety incidents, mis-selling, sanctions breaches – are cultural failures first and control failures second. The controls existed; people chose to work around them, and leadership signalled, deliberately or not, that this was acceptable.

What the Board should do

Board actions:

1. Define, together with management, a small number of core values and expected behaviours, and approve the code of conduct that expresses them. Keep the language concrete: “we escalate bad news within 24 hours” is more useful than “we act with integrity”.
2. Model the behaviour personally. Arrive at Board meetings prepared, declare conflicts of interest without being prompted, challenge the CEO respectfully but openly, and observe the same rules that apply to employees – including expense discipline and training requirements.
3. Make culture a standing item, not a crisis item. Review cultural indicators at least annually: employee engagement and exit survey results, whistleblowing report volumes and outcomes, staff turnover in control functions, audit findings on behavioural root causes, and disciplinary statistics broken down by seniority.
4. Test consistency between incentives and values. Ask whether the remuneration system rewards the behaviours the code of conduct describes – or quietly rewards their opposite. Ensure that how targets are met carries real weight in performance evaluation, not only whether they are met.

5. Insist on consequence management at all levels. Verify that misconduct by senior or high-performing individuals is investigated and sanctioned with the same rigour as misconduct by junior staff. Nothing corrodes culture faster than visible double standards.
6. Get beyond the boardroom. Visit sites, meet middle managers and employees without executives present, and hear directly from the heads of internal audit, compliance and risk in closed sessions.

Warning signs

- Consistently positive reporting – no bad news, no near-misses, no dissent recorded in minutes.
- A dominant CEO whom no one, including directors, visibly challenges.
- High turnover in the finance, compliance, internal audit or legal functions.
- Whistleblowing channels that receive almost no reports – silence usually signals fear, not virtue.
- “Star performer” exceptions: targets, rules or investigations applied selectively to protect key revenue generators.
- Values posters on the walls that employees quote with irony rather than conviction.

Common pitfalls and drawbacks

Boards most often fail on culture in one of three ways. The first is delegation by declaration: approving a values statement and assuming the work is done. Culture is shaped by thousands of daily decisions, not by a document. The second is measurement theatre: tracking engagement scores as an end in themselves, which invites gaming and tells the Board little about how people behave under pressure. Indicators are prompts for inquiry, not proof of health. The third is inconsistency at the top itself: a Board that tolerates its own late papers, undeclared conflicts or dominant personalities has no credibility demanding better from management. Board members should also be alert to the opposite risk – a culture programme so heavy with surveys, campaigns and slogans that it breeds cynicism. Fewer, more honest signals outperform elaborate programmes.

KEY TAKEAWAYS

A. Culture is what people actually do when no one is watching; tone at the top is the signal the Board and management send about which behaviours are rewarded, tolerated or punished. Culture rarely rises above the standard its leaders visibly practise.

B. Culture is a governance matter, because most corporate failures are cultural failures first and control failures second. It should be a standing Board item, reviewed through concrete indicators, not a crisis item.

C. The Board shapes culture by defining a few concrete values and behaviours, modelling them personally, testing that incentives reward the right behaviours and insisting on consequence management at every level, including senior and high-performing individuals.

D. Governance professionals translate tone into practice: the company secretary keeps culture on the agenda, compliance makes the code and whistleblowing channels usable, internal audit reports cultural root causes, and HR aligns recruitment, promotion and pay with the stated values.

QUESTIONS FOR THE BOARD

1. *Do our stated values translate into a short, concrete code of conduct that employees can actually apply?*
2. *Does the Board itself observe the standards it expects of management, in preparation, conflicts of interest and open challenge?*
3. *Which cultural indicators do we review each year, and what did the last review tell us about the gap between stated values and daily practice?*
4. *Does our remuneration system reward how targets are met, not only whether they are met?*
5. *Is misconduct by senior or high-performing individuals investigated and sanctioned with the same rigour as misconduct by junior staff?*
6. *When did Board members last meet employees and middle managers without executives present, or hear from the heads of internal audit, compliance and risk in a closed session?*
7. *If an employee saw a Board member or the CEO breaching our code of conduct, would they dare to report it, and to whom?*
8. *When did we last decline a profitable opportunity on values grounds, and did we communicate that decision internally?*
9. *How quickly does bad news reach the Board, and does anyone soften it on the way?*

5.1.3

THE STRATEGY CYCLE: BUILDING, UPDATING, IMPLEMENTING

Strategy is the way in which the company uses its mission to achieve its vision, based on its values and on a clear understanding of the company's purpose and the expectations of the shareholders. The Board has to ensure that all the steps of the process listed below are implemented. Management develops and proposes the strategy and implements it once approved; the Board sets the direction, challenges the proposals, approves the strategy and oversees its implementation. The process below sets out the steps in three phases: development, approval and cascade, and implementation oversight.

Phase A – Strategy development or updating

1. **Agree the process and the roles.** Before any analysis begins, the Board and management should agree who does what, the strategy horizon (typically five to ten years), the timetable and the working format (for example, dedicated strategy sessions or an off-site meeting).
2. **Confirm purpose, mission, vision and values.** The strategy must flow from what the company exists to do and what it aspires to become. If these foundations are outdated or unclear, revisit them first – otherwise the strategy will lack an anchor and discussions will not be consistent.
3. **Map and understand the stakeholders.** Identify the company's key stakeholders and assess their relative power, interest and expectations and agree how conflicting expectations will be reconciled over time. Understanding the stakeholder map is the basis of effective strategy, and a strategy that lacks the buy-in of key stakeholders is unlikely to succeed.
4. **Conduct a thorough strategic analysis.** Analyse the company and its environment from the inside out, using recognised tools such as SWOT, PESTEL, VRIO, Ansoff Matrix, value chain analysis, Porter's five forces and gap analysis, and others that may be relevant for the company. Invite external experts where the in-house perspective is too narrow. Weak analysis at this stage is the most common root cause of later implementation failure.
5. **Identify and assess risks, and set the risk appetite.** Every strategic initiative carries risks, and these change over time. The Board should ensure that key risks are identified, assessed and matched with mitigation measures, and should define the risk appetite within which the strategy must fit. Without this, the result is a "fair-weather strategy" that works only until the first storm. The

Board should also distinguish the company's risk appetite from its risk capacity – the ability to absorb shocks – and pay particular attention to high-impact, low-probability risks, which are often neglected precisely because they seem unlikely to materialise.

6. **Evaluate industry trends, innovation and disruption.** The Board should consider the latest industry developments, technological change, research and development, and actual or potential disruptions to the business model – both as threats and as sources of opportunity.
7. **Integrate sustainability and ESG matters.** Sustainability-related risks and opportunities – including those identified through the double materiality assessment under CSRD/ESRS, where applicable – should be embedded in the company strategy itself, not treated as a separate strategy document. Further guidance on ESG topics is given in the BICG ESG Guidelines for Baltic Boards and the ecoDa ESG Governance Toolkit.[6]
8. **Develop and debate strategic options.** Crystallise realistic strategic opportunities and alternatives, and test them through scenario planning and stress-testing. Each option rests on certain assumptions. It is the Board's duty to challenge assumptions wisely, because assumptions presented by management carry built-in bias. Challenge contributes to the improvement of the strategy. A strategy adopted without genuine alternatives on the table has not been chosen – it has been assumed.
9. **Make the strategic choice.** Decide which alternatives will be embedded in the company strategy, using explicit criteria: value creation, fit with the risk appetite, available resources and competences. Record which options were rejected and why – this discipline will be valuable when the strategy is next reviewed.
10. **Translate the strategy into goals, objectives and action plans.** Ensure a clear hierarchy:
    - **Goals** – what needs to be accomplished to implement the strategy;
    - **Objectives** – specific, measurable milestones with a timeline for achieving each goal (the SMART criteria apply);
    - **Action plans** – how the company will achieve each objective, with named owners, resources and deadlines.
11. **Align resources and incentives with the strategy.** Verify that the budget, capital allocation, financing and people actually support the strategic priorities,

6 BICG (2022), ESG Guidelines for Baltic Boards – What, Why and How, https://www.bicg.eu/wp-content/uploads/2022/09/ESG-Guidelines-for-Baltic-Boards.pdf; ecoDa (2019), ESG Governance Toolkit for Boards, https://ecoda.eu/wp-content/uploads/2019/08/ESG-Governance-toolkit-for-boards_FINAL.pdf.

and link executive remuneration and key performance indicators (KPIs) to the strategic objectives.

Phase B – Approval and cascade

1. **Approve the strategy at Board level.** The Board formally approves the strategy together with its strategic goals, the implementation roadmap and the reporting schedule. Approval should follow genuine challenge and debate, not a single presentation.
2. **Ensure each unit's contribution is defined.** Cascade the strategy so that every business unit has its own sub-strategy (functional strategy) and knows its specific contribution to implementation, reflected in unit-level plans and individual objectives. Cascading does not mean that the creation of strategy is top-down: engagement is an iterative process, and each unit should be given the opportunity to work out what the strategy means for its own work that contributes to the company's objectives – this builds ownership as well as alignment.
3. **Communicate the strategy thoroughly.** Communicate the strategy and its rationale consistently within the company and, where appropriate, its essential parts to external stakeholders. People cannot implement what they do not understand. Boards routinely underestimate how much communication is needed – as a rule of thumb, double what seems sufficient, and then double it again. A concise "strategy on a page", built around a small number of clear strategic themes, is often far more effective than a lengthy strategy document.

Phase C – Oversight of implementation

1. **Assess the company's capability to implement.** A well-implemented average strategy will outperform a perfectly designed strategy that is poorly executed. The Board should periodically assess the organisation's implementation capability across dimensions such as people, organisational structure and resources, understanding of the business case, communication, measures, culture and processes.
2. **Monitor implementation through efficient reporting.** Management reports regularly against the approved KPIs and milestones; the Board reviews progress at an agreed cadence using a concise dashboard that includes leading indicators, not only financial results. Strategy should have a standing place on the Board agenda (2–4 times a year), not appear once a year.
3. **Take corrective action and review the strategy regularly.** Where implementation deviates from plan, the Board ensures that management analyses the causes and adjusts the actions – or, where the environment has

shifted, that the strategy itself is revised. A full strategy review should take place at least annually, and immediately after any material change in the business environment.

Strategy-setting process: Board and management roles

Often it is not clear to companies what the roles of the Board and management are in strategy development. One common failure is when the Board “rubber-stamps” the strategy: management prepares a 150-page strategy document, the Board discusses it for a few hours, and approves it. Another common failure is the “management Board”, where the Board engages itself in designing products, selecting markets, and developing implementation initiatives – effectively doing the job of executives.

There should be a clear division of responsibilities in strategy development: the Board owns the strategic direction, choices, desired outcomes and risk appetite, while management owns the analysis, development of strategic options, resource and capability planning, and execution of the chosen strategy.

The five stages below put this division into practice, alternating lead responsibility between the Board and the executives, so that strategy is set through structured dialogue rather than by either party alone.

STAGE	PRIMARY ROLE	WHAT HAPPENS
1. Strategic framing	**Board**	Board discusses and (re)approves purpose, vision, mission and values, clarifies the expectations of owners, shareholders and other key stakeholders, and sets the ambition, key strategic issues, risk appetite and the questions the strategy must answer. Where a strategy committee exists, it prepares this discussion for the full Board.
2. Analysis & options	**Executives**	Management conducts internal and external analysis (market, competitive, financial and risk) and develops credible strategic alternatives, including underlying, financial implications, risks, trade-offs and how each option addresses the Board's strategic questions. Where useful, scenario planning is used to stress-test alternatives against plausible future conditions.
3. Strategic choice	**Board**	Management presents the strategic alternatives. The Board challenges assumptions, tests trade-offs and, after a thorough discussion, selects the preferred strategic direction(s). The Board's rationale and any conditions attached to the decision are recorded in the minutes to provide a clear mandate for the next stage.
4. Strategy development	**Executives**	Management converts the chosen direction into an integrated strategy: objectives, key performance indicators, initiatives, resource allocation, capabilities, financial plans, risk mitigation measures and an implementation roadmap with clear ownership and milestones.

STAGE	PRIMARY ROLE	WHAT HAPPENS
5. Approval & oversight	**Board**	Board assesses whether the resulting strategy reflects the agreed choices and risk appetite, formally approves it, and thereafter oversees execution through periodic progress reviews against the agreed KPIs and milestones. Material deviations, changing conditions or emerging risks are escalated to the Board, which revisits Stage 1 as needed – making strategy-setting a continuous cycle rather than a one-off event.

Warning signs

- The Board is presented with only one strategic proposal, rather than alternative strategic options and their trade-offs.
- Strategy papers are always approved without challenge or amendment – silence is being mistaken for consent, a classic symptom of groupthink.
- The strategy appears on the Board agenda only once a year, at approval time.
- Unit managers cannot explain their unit's contribution to the strategy.
- Reporting on implementation consists of financial results only, with no leading indicators.
- Sustainability is handled in a separate document that never intersects with the company strategy.
- The assumptions behind the strategy are never revisited once it has been approved.
- No one can say in advance what would cause the Board to reopen the strategy.

KEY TAKEAWAYS

A. Strategy is set through structured dialogue between the Board and management: the Board frames the direction, ambition, risk appetite and questions; management analyses and develops credible options; the Board challenges assumptions and chooses between genuine alternatives; management develops the detailed strategy; the Board approves it and oversees implementation.

B. Strategy development rests on confirmed purpose, mission, vision and values, a clear stakeholder map, thorough analysis, a defined risk appetite (distinguished from risk capacity), attention to trends and disruption, and sustainability embedded in the strategy itself.

C. A strategy adopted without genuine alternatives on the table has not been chosen but assumed. Options should be tested through scenario planning and stress-testing, and rejected options recorded with the reasons.

D. Approval is not the end: the strategy must be translated into goals, objectives and action plans, aligned with budget, resources and incentives, cascaded to every unit and communicated far more than seems necessary.

E. Implementation should be monitored two to four times a year through a concise dashboard with leading indicators, with corrective action where needed and a full review at least annually or after any material change in the environment.

QUESTIONS FOR THE BOARD

1. *Have the Board and management agreed who does what in strategy-setting, the strategy horizon, the timetable and the working format?*
2. *Does the Board set the direction and risk appetite before management develops options, or does it react to a finished document?*
3. *Were genuine alternatives presented, and did we test the assumptions behind the option we chose?*
4. *Is the strategy translated into goals, objectives and action plans with named owners, and are budget and incentives aligned with it?*
5. *Can every unit manager explain their unit's contribution to the strategy?*
6. *How often does strategy appear on our agenda, what does our implementation dashboard show beyond financial results, and when did we last revise the strategy in response to a change in the environment?*
7. *Do we know which risks could break this strategy, and how they will be mitigated?*
8. *Which stakeholders must support this strategy for it to succeed, and how do we know that they do?*
9. *How quickly would we learn that implementation is going off track?*

5.1.4

INTEGRATING SUSTAINABILITY INTO COMPANY STRATEGY, ITS OVERSIGHT, SUSTAINABILITY REPORTING

Sustainability has moved from a peripheral corporate-responsibility function to a core input into strategy. Climate-related risk, resource dependency, workforce and supply-chain resilience, and stakeholder expectations now bear directly on a company's competitive position, cost of capital and even existence. For Boards, this means sustainability cannot be delegated to a sustainability officer, treated as an annual reporting exercise, or managed through a separate sustainability strategy: it must be part of the company's core strategy, set, approved and overseen through the same governance processes.

This holds regardless of whether a company falls within the scope of mandatory EU sustainability regulation. Lenders, investors, customers and supply-chain partners increasingly apply their own expectations, and the underlying business drivers – energy prices, physical climate risks, access to capital and talent – affect every company. The Board's task is not to maximise sustainability ratings, but to ensure that material sustainability factors are properly weighed in strategic decisions.

The role of the Board

Sustainability considerations belong at the stage of strategy development and annual revision, not bolted on after strategic choices have already been made or reduced to a year-end reporting exercise.

Integration of sustainability-related matters into company strategy, revision of business models, and oversight of these activities is getting more attention in boardrooms – and these topics have become even more important as new EU-level regulation, including CSRD, ESRS and CSDDD, has raised the stakes, even though the 2026 Omnibus I amendments narrowed mandatory reporting and due diligence to the largest companies. The Board should take leadership in re-evaluating risks, identifying new sustainability-related risks and opportunities, and reshaping strategy where needed, rather than waiting for management or auditors to surface them.

Sustainability-related issues do not only create obligations to comply with EU regulation and generate risk; they also open access to opportunities that might otherwise go uncaptured, including:

- New business models

- New products and offerings
- Access to green capital on more favourable terms
- Improved competitive advantage
- Reduced energy use, lowering dependence on energy markets and price volatility
- A stronger company brand

The Board's ongoing task is to challenge, approve and monitor: ensuring sustainability-related risks and opportunities are identified through a rigorous double materiality assessment, embedded in the chosen strategy, properly resourced, and reported accurately to the market. Its oversight does not stop at risk and opportunity either – the Board is also expected to act when sustainability management within the company reasonably deviates from the company's stated values.

What the Board should do

1. **Set the sustainability risk appetite** at the strategic framing stage, alongside financial and operational risk appetite, so it shapes strategic choice rather than following it.
2. **Require and challenge a double materiality assessment** – impact materiality (the company's effect on people and environment) and financial materiality (sustainability factors' effect on the company) – refreshed at least annually rather than treated as a one-off compliance exercise.
3. **Assign clear oversight,** either to the full Board or to a dedicated committee (audit, risk, or a standalone sustainability committee), with a defined mandate, reporting line and competence requirement.
4. **Approve measurable targets and KPIs** linked to the strategy – not generic commitments – and track them with the same rigour as financial KPIs in periodic Board reporting.
5. **Oversee the reporting process itself,** including data quality, internal controls and external assurance, for CSRD/ESRS-aligned disclosures where in scope, or proportionate voluntary reporting were not.
6. **Link executive remuneration,** where appropriate, to sustainability KPIs so management incentives align with the approved strategy.
7. **Build Board competence** through training, briefings or committee expertise, so Board members can test management's assumptions rather than defer to them.

8. **Extend oversight into the value chain,** given that suppliers, customers and lenders increasingly request sustainability data and due diligence regardless of a company's own regulatory scope.

Warning signs

- Sustainability strategy, targets or reporting owned entirely by one function, with no Board-level sponsor or committee.
- Public claims or reported KPIs that management – or the Board – cannot trace back to underlying data.
- A materiality assessment that has not changed in substance year on year, or was outsourced entirely with no internal ownership.
- Sustainability reporting produced after the strategy is finalised, rather than informing it.
- No independent assurance over reported sustainability data, or assurance scope quietly narrowing over time.
- Board papers that treat sustainability as a once-a-year agenda item rather than a recurring line in strategy and risk reporting.

Common pitfalls and drawbacks

- **Treating reporting as the objective.** Compliance with CSRD/ESRS, or a voluntary framework, is necessary but not sufficient – a well-reported strategy that does not reduce risk or build resilience has still failed its purpose.
- **Starting too late and under-resourcing the work,** compressing materiality and data-collection into a year-end scramble that degrades quality and invites audit findings.
- **Greenwashing through selective disclosure –** publicising favourable metrics while omitting less favourable ones – which exposes the company and its Board members to reputational and, increasingly, legal risk.
- **Passive Board oversight:** receiving sustainability updates without challenging data quality or the gap between stated ambition and actual resourcing.
- **Treating scope thresholds as the only test.** Following the EU's 2026 Omnibus simplification, direct CSRD scope has narrowed materially (broadly, large undertakings above 1,000 employees and €450 million net turnover); companies below that threshold can still face equivalent demands indirectly, as larger customers, lenders and investors request comparable data down the value chain.[7]

7 Thresholds under Directive (EU) 2022/2464 (CSRD) as amended by the EU "Omnibus I" simplification package adopted in 2025–2026.

- **Underinvesting in Board and management competence,** leaving oversight dependent on external advisers who cannot be held accountable in the way directors can.
- **Waiting for the rules to settle.** National transposition of CSRD is still evolving across Estonia, Latvia and Lithuania, which tempts companies to delay rather than build durable internal processes – a strategy built for the direction of travel, not just the current rules, tends to age better.

Practical, step-by-step guidance and the specific tasks for Boards related to ESG and sustainability can be found in the BICG ESG Guidelines for Baltic Boards, in ESG Governance: questions Boards should ask to lead the sustainability transition, and in A Practical Guide for Boards and Leadership Teams on Sustainability.[8]

KEY TAKEAWAYS

A. Sustainability is a core input to strategy, not a separate reporting exercise. It bears on competitive position, cost of capital and resilience, and it must be integrated into the company's strategy through the same governance processes as any other strategic matter.

B. The Board's role is oversight, starting at strategy development: setting the sustainability risk appetite, requiring and challenging a double materiality assessment, assigning clear oversight, and approving measurable targets and KPIs linked to the strategy.

C. Sustainability creates opportunities as well as obligations: new business models and products, access to green capital, competitive advantage, lower energy dependence and a stronger brand.

D. The Board oversees the reporting process itself, including data quality, internal controls and external assurance, and should be alert to greenwashing through selective disclosure.

E. Companies outside the direct scope of CSRD can still face equivalent demands through customers, lenders and investors, so processes should be built for the direction of travel, not only the current rules.

8 BICG (2022), ESG Guidelines for Baltic Boards – What, Why and How, https://www.bicg.eu/wp-content/uploads/2022/09/ESG-Guidelines-for-Baltic-Boards.pdf; ESG Governance: questions Boards should ask to lead the sustainability transition; BICG (2022), A Practical Guide for Boards and Leadership Teams on Sustainability, https://www.bicg.eu/wp-content/uploads/2022/01/A-practical-guide-for-boards-leadership-teams-on-sustainability-11.pdf.

QUESTIONS FOR THE BOARD

1. *Where in our strategy process do sustainability risks and opportunities enter, and is that before or after the main strategic choices are made?*
2. *Who owns our double materiality assessment, when was it last refreshed, and which external stakeholders were consulted?*
3. *Do we have measurable sustainability targets and KPIs linked to the strategy, and are they tracked with the same rigour as financial KPIs?*
4. *Which of our reported sustainability metrics are independently assured, and can we trace every public claim to underlying data?*
5. *Does the Board have the competence to test management's assumptions on sustainability, or do we defer to external advisers?*
6. *How exposed are we, directly or through our value chain, to CSRD, taxonomy or due-diligence requirements, and how is that changing?*
7. *What are our two or three most material sustainability-related risks and opportunities, and how do they change our strategy, not just our reporting?*
8. *Are our public sustainability commitments and targets consistent with what management is actually resourcing and delivering?*
9. *Does management's remuneration reward the sustainability outcomes we say we want, and what escalation path exists if a target is missed or a material risk emerges mid-cycle?*

5.1.5

CAPITAL STRUCTURE AND DIVIDEND POLICY

How a company finances itself – the mix of debt and equity it carries – and how it returns capital to shareholders are not routine treasury matters. Together they determine a company's resilience under stress, its capacity to fund strategy and growth, its cost of capital, and the confidence lenders, investors and rating agencies place in it. Capital structure and dividend policy sit directly within the Board's fiduciary oversight: decisions here are strategic choices with legal consequences, not calculations to be left entirely to the finance function.

The role of the Board

The Board's task is to set the framework within which capital structure and distribution decisions are made, and to test management's proposals against it – not to draft them. In practice, this means approving a target capital structure and a dividend policy consistent with the company's strategy and risk appetite.

Usually, the final decision to distribute profit rests with the general meeting of shareholders, acting on the approved annual accounts and the proposal of the Board. That does not reduce the Board's role to a formality. The Board reviews and approves the management's dividend proposal before it reaches shareholders. Either way, the Board's job is to confirm that a proposed distribution is lawful, that it does not compromise the company's solvency or its ability to fund strategy, and that it is consistent with a policy the Board has itself endorsed – rather than an ad hoc figure produced late in the reporting cycle.

What the Board should do

1. **Set and periodically review a target capital structure** – an acceptable range for leverage and the debt/equity mix – aligned with the company's risk appetite and strategy, not simply the lowest available cost of capital or short-term tax optimisation.
2. **Approve a clear, published dividend policy** (a payout ratio range and a stated priority between reinvestment, deleveraging and shareholder returns) so that distributions follow a discipline the Board has set, rather than being decided year to year. The dividend policy also plays an additional role: it explains transparently to the shareholders and all relevant stakeholders how dividends are set. This is particularly important where some shareholders demand high dividends without regard to the financial health of the company.

3. **Verify the statutory distribution tests** before recommending any dividend to shareholders. Estonian law requires that equity remain at least half of share capital and that a distribution not endanger solvency; Latvian law prohibits distribution if own funds would fall below share capital; Lithuanian law restricts distribution that would reduce equity below authorised capital or mandatory reserves. These are Board-level checks, not back-office formalities.[9]
4. **Stress-test the capital structure** against adverse scenarios – a revenue shock, a rise in interest rates, tighter refinancing terms, or a market unwilling to roll over debt – rather than relying solely on the base case.
5. **Assess covenant headroom and refinancing risk** before approving new borrowing or a distribution that would reduce that headroom, and monitor both on an ongoing basis, not only at renewal.
6. **Maintain a predictable, well-communicated policy,** particularly for companies listed on Nasdaq Baltic, where unexplained deviation from stated dividend guidance affects market credibility and share price.
7. **Record the rationale** for capital structure and dividend decisions in Board and shareholder minutes, including the basis for the distributable-profit calculation – closing the same accountability gap this Handbook flags for strategic decisions generally.

Warning signs

- A dividend maintained or increased despite weakening cash flow, rising leverage or narrowing covenant headroom.
- No clearly articulated capital structure or dividend policy – distributions and financing decided ad hoc, year to year, with little Board discussion.
- Distributions approved without documented confirmation that statutory solvency and net-asset tests were met.
- Growing reliance on short-term or refinancing debt to fund distributions or ongoing investment.
- Capital structure decisions driven primarily by tax optimisation, with limited regard to underlying business risk.
- Little or no Board challenge to management's proposed leverage, payout ratio or financing structure.

9 See the provisions on the distribution of profit and the protection of capital in the Estonian Commercial Code, the Latvian Commercial Law and the Lithuanian Law on Companies.

Common pitfalls and drawbacks

- **Treating dividend policy as a technical finance decision,** delegated entirely to the CFO and rubber-stamped by the Board rather than scrutinised as a strategic choice.
- **Protecting a stable or progressive dividend at the expense of strategic investment,** including transition or resilience-related capital expenditure, weakening the company's longer-term position to preserve a short-term signal to the market.
- **Carrying leverage inconsistent with the business's actual risk profile,** either too conservative to fund growth or too aggressive relative to the volatility of the underlying business.
- **Overlooking the statutory distribution tests,** which in each Baltic jurisdiction can expose Board members to personal liability for an unlawful distribution – this is a compliance matter, not only a financial one.
- **An inconsistent or opportunistic dividend policy** that damages market credibility and, for listed companies, raises the cost of capital by increasing perceived uncertainty.
- **Ignoring the tax asymmetry across the Baltic states** when structuring group financing and dividend flows – moving cash between an Estonian or Latvian entity, where reinvested profit is untaxed, and a Lithuanian parent taxed annually, without coordinated group tax planning.
- **Failing to document the Board's reasoning,** leaving no audit trail for why a particular capital structure or distribution was approved – a gap that becomes costly precisely when a decision is later questioned.

As elsewhere in this Handbook, the mechanism of approval differs by structure – the Supervisory Board or Council in the two-tier structures common across Estonia, Latvia and Lithuania, or the non-executive members of a one-tier Board – but the standard does not: a disciplined, documented policy, tested against the law and the company's own risk appetite, before it ever reaches the shareholders who make the final call.

KEY TAKEAWAYS

A. Capital structure and dividend policy are strategic choices with legal consequences, not routine treasury matters. They determine the company's resilience, its capacity to fund strategy and its cost of capital.

B. The Board sets the framework, a target capital structure and a published dividend policy aligned with strategy and risk appetite, and tests management's proposals against it. The final decision on distributions usually rests with the shareholders, acting on the Board's proposal.

C. Before recommending any distribution, the Board must verify the statutory tests in the relevant Baltic jurisdiction; an unlawful distribution can expose directors to personal liability.

D. The different tax treatment of retained and distributed profit in Estonia, Latvia and Lithuania should inform where cash is held and how intra-group distributions are structured.

E. The capital structure should be stress-tested against adverse scenarios, covenant headroom and refinancing risk monitored continuously, and the rationale for every decision recorded in the minutes.

QUESTIONS FOR THE BOARD

1. *Do we have an approved target capital structure and a published dividend policy, and when were they last reviewed against the strategy and risk appetite?*
2. *Is the current dividend proposal consistent with that policy, and if it deviates, has the Board recorded why?*
3. *Who verified that the statutory solvency and minimum-equity tests are met for this distribution, and is that verification documented?*
4. *How would our leverage and liquidity hold up under a revenue shock, higher interest rates or a tighter refinancing market?*
5. *Are we retaining enough capital to fund the strategy without becoming dependent on external financing?*
6. *Does our group financing and distribution structure take account of the differing tax treatment of profit across the Baltic states?*
7. *What is our target leverage range, and why is it the right one for our strategy and risk appetite, not simply the cheapest available financing?*
8. *What covenant headroom do we have today, and how does this financing or distribution decision change it?*
9. *If a lender or rating agency reviewed our capital structure today, what would concern them most?*

5.1.6

MERGERS, ACQUISITIONS AND MAJOR TRANSACTIONS

Few decisions test a Board as severely as a merger, an acquisition, a disposal of a core business or another transformational transaction. The amounts at stake are large, the information is asymmetric, the timetable is compressed, and the atmosphere is often charged with ambition. Research consistently shows that a substantial share of acquisitions destroy value for the buyer – not because the idea was bad, but because the price was too high, the risks were underestimated or the integration failed. The Board's role is therefore not to run the deal, but to ensure that the company enters it for the right reasons, at a defensible price, with open eyes and with a credible plan for what happens after signing.

Major transactions also concentrate governance risks that are diffuse in ordinary business: conflicts of interest, related party transactions, insider information, disclosure obligations and shareholder rights all converge on a single decision. In smaller markets, where the counterparty may well be connected to a shareholder or a director, this convergence deserves particular attention.

The role of the Board

The Board owns three things in any major transaction: the strategic rationale, the approval decision and the oversight of execution. Management identifies opportunities, negotiates and integrates; advisers value, structure and document. The Board's distinct contribution is disciplined judgement – whether the transaction serves the company's strategy or merely someone's ambition, whether the price rests on realistic assumptions, and whether the organisation can absorb what it is buying. The Board must also safeguard process integrity: conflicts of interest, inside information, equal treatment of shareholders, and disclosure and merger control requirements.

What the Board should do

Board actions:

1. Anchor every transaction in strategy before discussing price. Require management to show how the deal fits the approved strategy and what the realistic alternatives are – including organic growth, partnership or doing nothing.
2. Establish the process at the outset: a clear mandate for management, approval thresholds, a timetable for Board involvement, and rules for confidentiality and

insider lists. For significant deals, consider a transaction committee of unconflicted Board members with relevant experience.

3. Identify and manage conflicts of interest immediately. Require every Board member and senior executive to declare any connection to the counterparty, its owners or its advisers. Conflicted Board members must be excluded from deliberation and decision, and related party transaction procedures must be applied where the law or the company's corporate governance code requires.
4. Commission genuinely independent advice. Ensure that financial, legal and tax due diligence is proportionate to the deal, and consider an independent fairness opinion on valuation – especially where a shareholder, a director or management has an interest in the outcome.
5. Interrogate the assumptions, not only the model. Ask which synergies are proven, which are hoped for, and what the deal looks like if revenue synergies are removed entirely. Require a downside case and a walk-away price, and hold the Board to it when negotiation pressure mounts.
6. Approve the integration plan together with the deal, not after it. Require named accountability for integration, a budget for one-off costs, retention plans for key people of the target, and milestones the Board will track.
7. Review the outcome. Twelve to twenty-four months after closing, compare actual performance against the investment case presented at approval, and record the lessons for the next transaction.

Warning signs

- Deal momentum: the transaction accelerates while scrutiny weakens, and the question shifts from "should we" to "how fast can we".
- A CEO personally invested in the deal as a legacy project, with the Board hearing only supporting evidence.
- Due diligence findings dismissed as "deal points" without analysis of their long-term cost.
- Advisers remunerated only on completion, with no one in the room paid to say no.
- Undeclared connections between the counterparty and shareholders, Board members or executives.
- No integration plan, budget or named owner at the moment of approval.

Common pitfalls and drawbacks

The most expensive pitfall is overpayment driven by momentum and optimism: once time, money and reputation have been invested in a deal, walking away feels

like failure, and Boards approve prices they would have rejected at the outset. The second is treating approval as the finish line – most value is won or lost in integration, which begins the day after closing and typically takes years. The third is process failure: a conflicted Board member who participated in the decision, a missed disclosure, a breach of insider rules or an overlooked merger control filing can invalidate the transaction and expose Board members to personal liability. Boards should also recognise the drawbacks of excessive caution: a Board that demands certainty on every point will lose good opportunities to faster competitors. The aim is disciplined speed – a well-designed process that allows the Board to decide quickly without skipping the questions that matter.

Guidance for other governance professionals

Company secretaries, general counsel, chief financial officers and internal auditors carry much of the practical burden of a clean transaction. The company secretary should design the decision trail: properly convened meetings, complete papers, minutes recording the alternatives considered and the reasons for the decision, declarations of interest, and insider lists maintained from the first confidential discussion. General counsel should map the approval requirements early – shareholder approvals, related party transaction procedures, merger control filings, disclosure obligations – and build them into the timetable. The chief financial officer should present the investment case with its assumptions visible and testable, including a downside scenario, and resist pressure to tune the model to a predetermined answer. Internal audit should review the process after closing. The guiding principle for all of these roles: the file should show that the Board decided carefully, on complete information and free of conflicts.

KEY TAKEAWAYS

A. Major transactions test a Board more severely than any other decision: large amounts, asymmetric information, compressed timetables and charged ambition. A substantial share of acquisitions destroy value because the price was too high, the risks underestimated or the integration failed.

B. The Board owns the strategic rationale, the approval decision and the oversight of execution. Management negotiates and integrates; advisers value and document. The Board's contribution is disciplined judgement and process integrity.

C. Every transaction should be anchored in strategy before price is discussed, run under a clear process with approval thresholds and insider rules, and protected against conflicts of interest through declarations and exclusion of conflicted Board members.

D. Independent advice, interrogated assumptions, a downside case and a walk-away price protect against deal momentum. The integration plan, with named accountability and a budget, is approved with the deal, not after it.

E. Outcomes should be reviewed twelve to twenty-four months after closing against the investment case, and the lessons recorded.

QUESTIONS FOR THE BOARD

1. *Do we have a defined process for major transactions: mandate for management, approval thresholds, Board timetable, confidentiality and insider lists?*
2. *Has every Board member and senior executive declared any connection to the counterparty, its owners or its advisers, and have conflicted Board members been excluded?*
3. *Is our due diligence and valuation advice genuinely independent, and have we seen a downside case and set a walk-away price?*
4. *Is there a named owner, a budget and milestones for integration at the moment of approval?*
5. *Are our advisers paid in a way that gives someone an incentive to say no?*
6. *When did we last compare a completed transaction against its investment case, and what did we learn?*
7. *Why this target, why now, and what happens to our strategy if we do not proceed?*
8. *What did due diligence find that we are choosing to accept, and why?*
9. *If this transaction appeared on the front page tomorrow, could we explain the process and the price with confidence?*

5.1.7

BUDGET AND KPIS FOR THE COMPANY AND CEO, PERFORMANCE MONITORING AND EVALUATION

When targets are defined, the Board must set specific KPIs or other agreed performance measures for the company and for the CEO, monitor regularly (at least quarterly) how management is performing against the set KPIs, and take the necessary measures if performance is not satisfactory. The more often the Board monitors performance, the more opportunities it will have during the year to take the measures needed to adjust operations and drive the company to better results.

KPIs should be both financial and non-financial (e.g. related to ESG and sustainability). It is not obligatory to set the same KPIs for the CEO as for the company. The CEO could have additional (e.g. “soft”) KPIs related to organisational culture and the well-being and satisfaction of employees.

It is good practice not to set too many KPIs. With more than 10 KPIs, the weight of a single KPI will be less than 10 per cent, and the motivation to achieve it may be weak.

KPIs should be defined very clearly and understandably, in order to avoid discussions after the year end about whether or not they have been achieved.

It is good practice to use the SMART concept when setting KPIs. Some companies use the SMARTER concept (specific, meaningful, achievable, relevant, time-bound, evaluate and readjust).

A budget sets out the income and expenses planned for the company. The budget should be challenging enough on both the income and the expense side. This gives management a sense of urgency, makes them continually search for the best and most innovative solutions and the most efficient way of operating, and keeps the company highly competitive. All these measures help to ensure that the value created is maximised.

KEY TAKEAWAYS

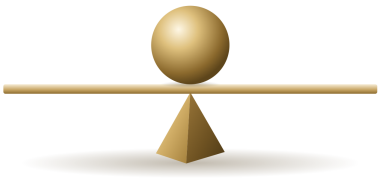
A. Once targets are set, the Board defines specific KPIs for the company and the CEO, monitors performance against them at least quarterly and takes corrective measures where performance falls short.

B. KPIs should be both financial and non-financial, few enough for each to matter (more than ten dilutes their weight), defined clearly enough to avoid year-end disputes, and SMART. The CEO's KPIs need not be identical to the company's and may include softer measures such as culture and employee well-being.

C. The budget should be challenging on both the income and the expense side, giving management a sense of urgency and keeping the company competitive and focused on value creation.

QUESTIONS FOR THE BOARD

1. *Do the company and the CEO have a short set of clearly defined, SMART KPIs, financial and non-financial, aligned with the strategy?*
2. *Is any KPI so weakly weighted that it no longer motivates, and are the definitions precise enough to leave no room for dispute at year end?*
3. *How often does the Board review performance against the KPIs, and what happened the last time performance fell short?*
4. *Is the budget challenging enough on both the income and the expense side, and how do we know?*
5. *Are the CEO's KPIs and remuneration consistent with the company's KPIs and with the behaviours we expect?*



CHAPTER

5.2

CONTROL, RISK AND ASSURANCE

How the Board makes sure that controls work, risks are understood and managed, and the company can withstand and recover from disruption.

IN THIS SECTION

5.2.1	Control environment	93
5.2.2	Internal control framework	98
5.2.3	Risk governance, Three Lines Model	104
5.2.4	Resilience: crisis preparedness, business continuity and recovery	116
5.2.5	Cybersecurity and information security oversight	124
5.2.6	Internal and external audit	128

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."

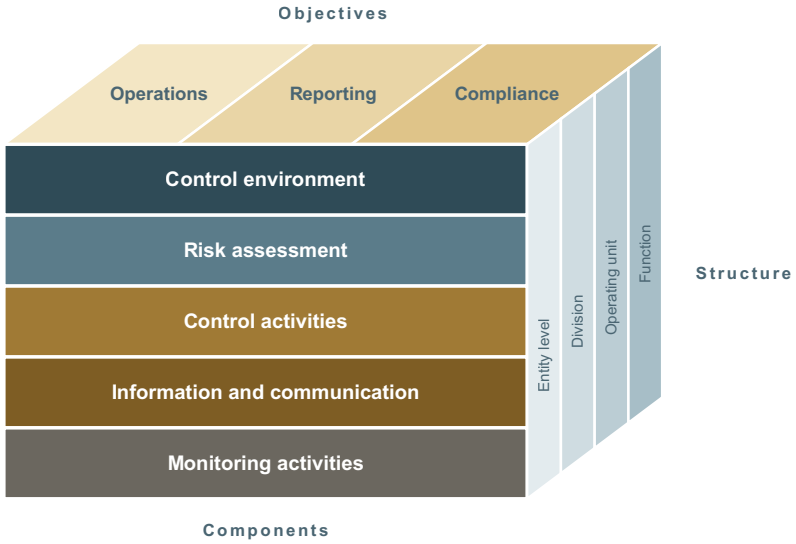
10 Committee of Sponsoring Organizations of the Treadway Commission (COSO), https://www.coso.org/.

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**



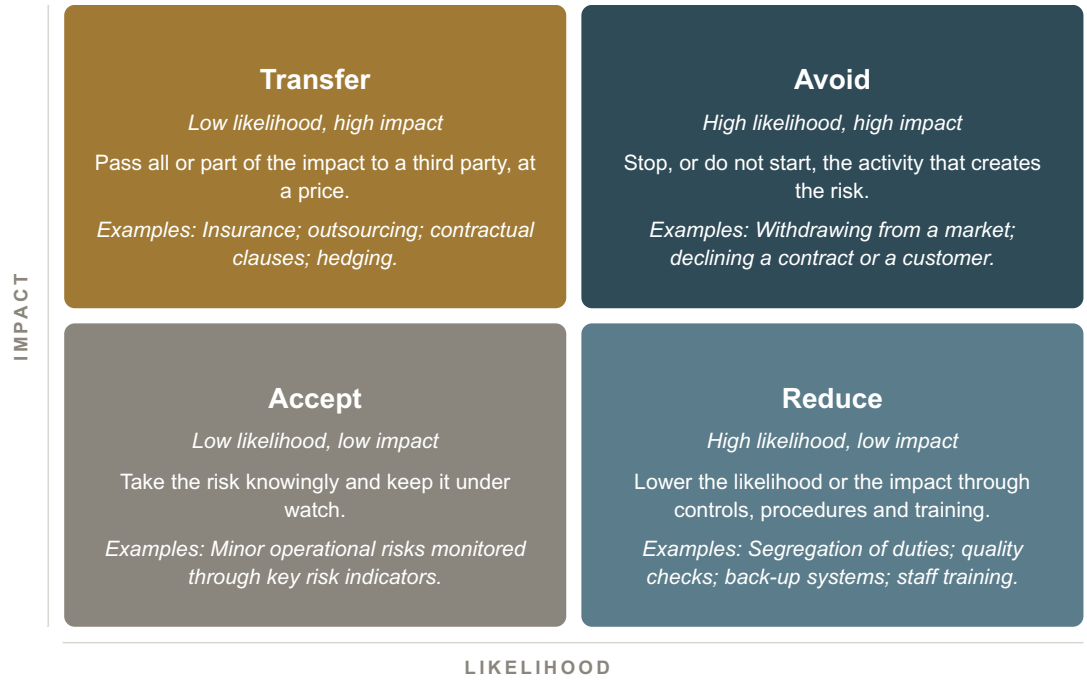
Score = likelihood (1–5) × impact (1–5). The scales, thresholds and colours should be adapted to the company's size and risk appetite.

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.

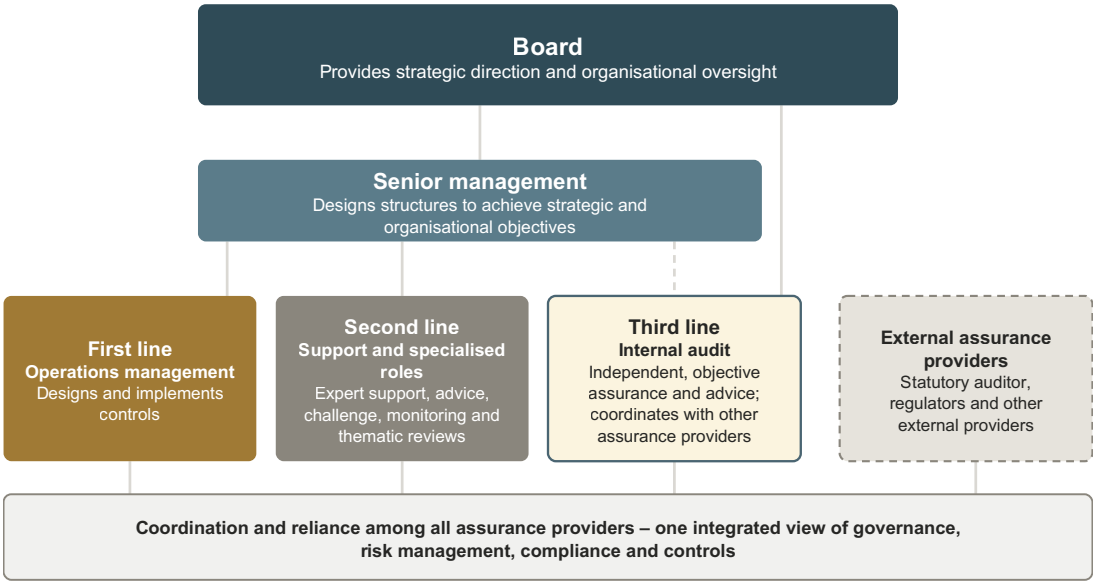
Benefits of implementing the Three Lines Model in a company:

- 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.

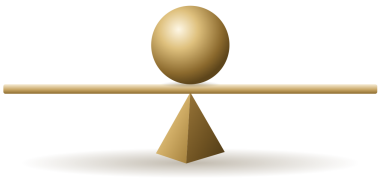
C. The audit committee proposes, and the Board approves, the internal audit regulations, the strategic and risk-based audit plans, the budget and the appointment, dismissal, evaluation and remuneration of the head of internal audit. Even with an audit committee, the full Board should maintain a direct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

materials and proposals for the Board; the responsibility, however, remains with the full Board.

What the Board should do

1. **Own the ethical standard.** Approve a code of ethics (or code of conduct) that expresses the company's values in concrete terms, states what is expected of everyone from the Board down, and explains how to raise concerns. Keep it short and specific to the company; review it at least every three years and whenever the business changes materially.
2. **Apply the standard to the Board first.** Adopt Board-level rules on gifts and hospitality, outside interests, use of company information and dealings with shareholders, and record in the minutes that they are observed. A Board that exempts itself from the code cannot demand that management follows it.
3. **Make ethics a criterion in decisions, not an afterthought.** Require that major proposals to the Board (transactions, market entries, restructurings, incentive schemes and similar) address the ethical and reputational dimension explicitly: who is affected, what could go wrong, and how the decision would look if made public. Where a decision is lawful but questionable, the Board should be prepared to say no.
4. **Assign clear ownership.** Designate who is responsible for the ethics programme (an ethics or compliance officer, the company secretary or a committee) with direct access to the Board or its audit committee, adequate resources and the authority to investigate. In smaller companies the role can be combined with another function, provided the reporting line to the Board is preserved.
5. **Insist on training that is practical.** Ensure that all employees, and the Board itself, receive training built around real dilemmas the company faces, in the languages people actually speak, rather than a generic annual e-learning module. Ask to see the dilemmas used, not only the completion rates.
6. **Review ethical performance at least annually.** Receive a report covering incidents and how they were handled, questions raised with the ethics function, results of employee surveys on trust and pressure, and the disciplinary consequences applied at all levels. Treat this review with the same seriousness as the review of financial results.
7. **Verify consistency across the company, its group and the value chain.** Ensure that subsidiaries, agents, distributors and major suppliers are bound by equivalent standards, particularly where the company operates in markets or sectors with a higher risk of corruption, sanctions breaches or human rights violations.

Warning signs

- The code of ethics has not been revised for years and nobody on the Board can recall its main provisions.
- Ethical questions are referred to the legal department, and the answer is always “it is legal”.
- Board papers on major transactions or incentive schemes contain no reference to reputational or ethical risk.
- Reported incidents are few and always minor, while the company operates in a high-risk sector or market.
- Senior managers accept invitations, gifts or side engagements that would not be tolerated at lower levels.
- Employees describe the values as “what we say to customers” rather than “how we work”.
- Pressure from a shareholder, including a public owner, to take a decision the Board considers improper is accepted without a recorded discussion.

Common pitfalls and drawbacks

The first pitfall is confusing ethics with compliance: assuming that because the lawyers have cleared a decision, the ethical question has been answered. It has not; the law is the floor, and many of the decisions that later prove most damaging were perfectly lawful. The second is the aspirational code: a document full of fine words that gives no guidance on the three or four dilemmas that actually arise in the company’s business, such as gifts from suppliers, pressure from a large customer or shareholder, or cutting corners to meet a deadline. The third is the exception for the important: tolerating behaviour from a founder, a star salesperson or a politically connected manager that would end the career of a junior employee. Nothing tells the organisation more clearly what the real standard is. The fourth is treating ethics as a reporting line rather than a Board responsibility, so that the Board hears about it once a year in a slide on training completion. Boards should also be aware of the opposite risk: an ethics programme so heavy with policies, declarations and campaigns that people stop reading and start ticking boxes. A short code, honest examples and visible consequences work better than volume.

Guidance for other governance professionals

The company secretary should ensure that the code of ethics is formally approved and periodically reviewed by the Board, that ethics appears on the Board’s annual calendar, that Board members’ own declarations are collected and minuted, and that new directors are inducted into the company’s ethical standards and the

dilemmas specific to its business. The ethics or compliance officer should keep the code short and usable, build training around real cases, maintain a record of the questions and incidents raised, and report to the Board on patterns and root causes rather than on activity. Internal audit should test whether the standard is applied in practice, for example by reviewing gifts and hospitality registers, procurement decisions and the handling of past incidents, and should state in its findings where a control was bypassed for reasons of culture rather than capability. Human resources should ensure that ethical conduct is assessed in performance reviews and promotion decisions, and that disciplinary outcomes are consistent across levels. General counsel should advise on what the law requires, but should also be willing to tell the Board when a lawful course of action is nonetheless unwise.

KEY TAKEAWAYS

A. Ethics is about doing what is right beyond what the law requires. Compliance sets the floor; ethics sets the standard by which the company, its Board and its people are judged.

B. The Board is the guardian of the ethical standard. It approves and reviews the code of ethics, applies the code to itself first, and treats ethical and reputational considerations as a criterion in every major decision.

C. An ethical standard needs an infrastructure: clear ownership with a reporting line to the Board, practical training built on the company's real dilemmas, a safe channel for raising concerns (sub-chapter 5.3.3), and consistent consequences at all levels.

D. Ethics must be reviewed at least annually on the basis of evidence – incidents, questions raised, survey results and disciplinary outcomes – with the same rigour as financial performance

E. In the Baltic context, small markets, close personal networks and, in SOEs and MOEs, political pressure create specific ethical risks. The Board should name them openly and set rules for them, rather than assume goodwill.

F. Ethics extends beyond the company's own staff to subsidiaries, agents, distributors and suppliers, particularly in higher-risk markets and sectors.

QUESTIONS FOR THE BOARD

1. *Do we have a code of ethics that is specific to our company, approved and reviewed by the Board, and would it tell a new employee what to do in the three situations most likely to arise in our business?*
2. *Does the Board apply to itself the rules on gifts, hospitality, outside interests and confidential information that it expects management to follow, and have we, as directors, declared our own?*
3. *Is ethical and reputational risk assessed explicitly in the papers for major decisions, and which decision in the last year did we take, or refuse, mainly on ethical grounds?*
4. *Who owns the ethics programme, do they have the resources and authority to investigate, and do they report directly to the Board or its audit committee?*
5. *Who in this company would tell the Board that management has crossed an ethical line, and would they feel safe doing so?*
6. *Do our remuneration and promotion decisions reward the way results are achieved, or only the results, and are consequences for misconduct applied consistently regardless of seniority or performance?*
7. *What evidence did the Board review in the last year on ethical performance – incidents, questions raised, survey results, disciplinary outcomes – and what did it decide as a result?*
8. *What do our subsidiaries, agents, distributors and key suppliers know about our ethical standards, and how would we find out if they breached them?*
9. *For SOEs and MOEs: how does the Board handle requests from the owner that it considers improper, and is that handling recorded?*

5.3.2

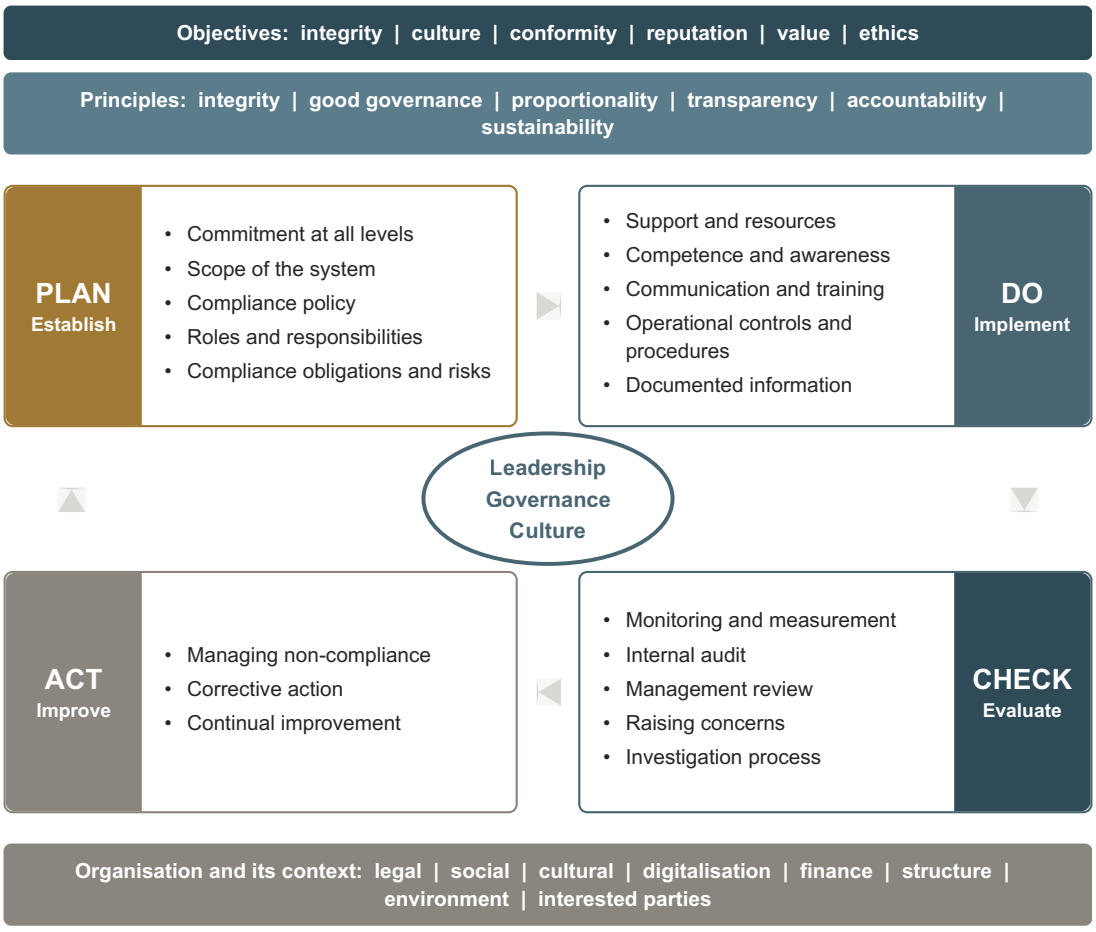
COMPLIANCE

With ever-evolving regulatory requirements, compliance risk is one of the key risks that every company, irrespective of its type, size or other characteristics, faces daily. Compliance risk is the risk of legal or regulatory sanctions, material financial loss or loss of reputation that a company may suffer as a result of its failure to comply with laws, regulations, rules, self-regulatory standards and codes of conduct.

To manage compliance risk, every company should maintain an effective compliance management system. For the system to be effective, it should not only implement policies and procedures to prevent and detect violations of the law, but also promote an organisational culture that encourages ethical conduct and a commitment to compliance with applicable laws, good governance and ethical standards.

The diagram below shows the main elements of a compliance management system as set out in the ISO 37301:2021 standard.

Figure 5.6 **Main elements of a compliance management system**



Source: BICG, based on the structure of ISO 37301:2021, Compliance management systems – Requirements with guidance for use.

A **compliance management system follows the plan - do - check - act cycle**. The company:

1. **plans the system** by securing commitment at all levels, defining its scope, adopting a compliance policy, allocating roles and responsibilities and identifying its obligations and compliance risks;
2. **puts the system into operation** through support, competence, communication, training, controls, procedures and documentation;
3. **checks the system** through monitoring and measurement, internal audit, management review, channels for raising concerns and an investigation process; and
4. **acts on the results** by managing non-compliance and improving continually. Leadership, governance and culture sit at the centre of the cycle, and the whole system is shaped by the company's objectives, its principles and its context.

Compliance is the outcome of a company meeting its obligations. Policies and procedures to achieve compliance should be integrated into all aspects of how the company operates. Compliance should not be treated as a stand-alone activity: it should be aligned with the company's overall strategic objectives and, while maintaining its independence, integrated with the company's financial, risk, quality, environmental and health and safety management systems and its operational procedures.

A company's approach to compliance should be shaped by its leadership, applying the company's core values and generally accepted governance, ethical and community standards.

In essence, compliance is a threefold duty covering:

1. the personal duty of Board members and employees to behave in accordance with the law and the company's rules;
2. the organisational duty of the governing bodies to set up and maintain a system that ensures that the company and its employees act in accordance with the law and the company's principles, and that breaches are discovered in a timely and efficient manner;
3. the duty of the members of the corporate bodies to pre-empt breaches and to avoid the resulting damage to the company's value.

A practical first step is to identify and map the compliance areas most relevant to the company and to establish, and keep up to date, a register of the external legal requirements and internal rules with which the company must comply.

The role of the Board

The Board approves the compliance policy and the appointment of a compliance officer or function with the independence, resources and authority to do the job, and with a direct reporting line to the Board or its audit committee. It sets risk-based priorities, receives regular reports on compliance risks, breaches, contacts with regulators and remediation, and ensures that the compliance function is integrated with risk management and internal audit under the Three Lines Model and operates effectively. In smaller companies the role may be combined with another function, provided that its independence and access to the Board are preserved.[AJ1.1]

Board roles and responsibilities

The Board is ultimately accountable for the company's compliance with law and ethical standards. This cannot be fully delegated - management implements, but the Board oversees and is responsible.

The Board's specific responsibilities include:

(i) Set the tone - demonstrate commitment to ethical behavior and compliance, including zero tolerance for corruption and misconduct.

(ii) Approve key policies - Code of Ethics, Anti-Corruption Policy, and Whistleblower Policy should be board-approved documents.

(iii) Engage in compliance risk oversight - understand the company's material compliance risks, satisfy themselves that appropriate mitigation measures are in place, and challenge management where controls appear inadequate.

(iv) Oversee compliance performance - receive and critically review periodic compliance reports and risk assessments; ask probing questions; and escalate concerns where red flags are not adequately addressed.

(v) Foster a compliance culture - actively promote company's culture in which ethical conduct is expected, reported concerns are taken seriously, and non-retaliation is guaranteed.

(vi) Ensure adequate resources - satisfy themselves that a competent, sufficiently independent compliance function (or Compliance Officer) exists with an adequate budget and clear reporting lines to the board.

(vii) Personal conduct - each board member must comply with conflict of interest obligations, insider trading rules (if applicable), confidentiality duties, and all other duties to which they are subject in their capacity as board members, including expected conduct under the Code of Ethics.

(viii) Incident oversight - serious compliance incidents and material whistleblower cases must be reported to the board, which should oversee investigation and remediation.

(ix) Board-level liability - directors may incur personal criminal or administrative liability for compliance failures. Ignorance of compliance obligations is not a defence — board members are expected to be and remain informed.

KEY TAKEAWAYS

A. Compliance risk is the risk of sanctions, financial loss or reputational damage from failing to comply with laws, regulations, self-regulatory standards and codes of conduct. Every company faces it daily, whatever its size or sector.

B. An effective compliance management system combines policies and procedures to prevent and detect breaches with a culture that encourages ethical conduct. ISO 37301:2021 provides a recognised reference model.

C. Compliance is a threefold duty: the personal duty of every Board member and employee to comply, the organisational duty of the governing bodies to set up a system that ensures compliance and detects breaches, and the duty to pre-empt breaches and avoid damage to the company.

D. Compliance is integrated into the way the company operates, aligned with its strategy and linked to its risk, quality, environmental and health and safety systems, while keeping the independence of the compliance function.

E. The Board approves the compliance policy, ensures that the compliance function has independence, resources and a direct line to the Board or its committee, and receives regular reporting on compliance risks, breaches and remediation.

QUESTIONS FOR THE BOARD

1. *Which laws, regulations and internal rules matter most for our business, and do we maintain an up-to-date register of them with named owners?*
2. *Has the Board approved regularly reviews a compliance policy and appointed a compliance officer with adequate resources, independence and direct access to the Board or its audit committee?*
3. *Does the compliance system prevent and detect breaches in practice, and what were the most significant compliance incidents, regulatory contacts and remediation actions in the last year?*
4. *Is compliance risk part of the risk register and risk appetite, and how does the Board satisfy itself that the compliance function is effective and not only documented?*
5. *Do Board members and management set the example in complying with the company's rules, and how does the company keep track of regulatory change?*

5.3.3

WHISTLEBLOWING

A whistleblowing mechanism is the structured, formal system that a company puts in place to allow employees, customers, suppliers, contractors and other stakeholders to report misconduct, illegal activities or unethical behaviour safely.

Whistleblowing addresses matters that affect the public interest or the integrity of the company. To distinguish whistleblowing from personal employment grievances, a whistleblowing framework applies to actions that threaten the company's integrity or the public interest, such as:

- Fraud, corruption, bribery or money laundering.
- Financial malpractice or deliberate breach of accounting controls.
- Breaches of environmental, health and safety regulations.
- Cover-ups or destruction of evidence related to any of the above.

The core goals of a whistleblowing mechanism are:

- Early detection. To act as an early-warning system that uncovers fraud, bribery and compliance breaches before they grow into corporate crises.
- Psychological safety. To create a "speak-up" culture where employees feel safe to voice concerns without fear of workplace bullying, demotion, or dismissal.
- Stakeholder trust. To build mutual trust by giving external stakeholders a transparent mechanism for identifying systemic risks, preventing ethical breaches and safeguarding the interests of investors, partners and the community.
- Accountability. To bypass traditional hierarchies so that misconduct at the executive or management level cannot be concealed.

The strategic benefits for the company are:

- Financial protection. Research consistently shows that occupational fraud is most frequently detected through tips. Early detection greatly reduces financial losses and helps to avoid regulatory fines.
- Reputational safeguarding. Handling issues internally and correcting them proactively reduces the risk of damaging leaks to the media or regulators.
- Improved culture. An active, trusted whistleblowing system signals to employees that management values integrity, boosting morale, trust and talent retention.

– Competitive advantage. Institutional investors increasingly treat robust environmental, social and governance (ESG) frameworks, including whistleblowing mechanisms, as a criterion in allocating capital.

The role of the Board and Management

The roles and responsibilities of the Board in whistleblowing:

1. Setting the tone at the top. The Board should publicly champion the whistleblowing system, making it clear that raising concerns is an act of loyalty to the company.
2. Whistleblowing policy. The Board approves and regularly reviews a whistleblowing policy establishing a formal infrastructure: secure reporting channels (hotlines, web platforms), independent investigators (where appropriate, external service providers) and strict non-retaliation rules.
3. Ensuring independent reporting lines. The Board (typically through its audit committee) should ensure that the whistleblowing process is functionally independent of executive management, to prevent conflicts of interest.
4. Direct escalation route. The policy should provide fast-track reporting for high-risk cases: a report concerning senior management goes directly to the Chair of the Board or the audit committee, so that the subjects of an investigation can never oversee it.
5. System monitoring and key indicators. The Board (with the help of its audit committee) regularly reviews anonymised metrics on the reporting system (number of reports, categories of misconduct, investigation closure rates). A complete absence of reports should be challenged by the Board as a possible sign of a culture of fear.
6. Protecting the whistleblower. The Board safeguards the speak-up culture by holding management responsible for the well-being of those who report, and verifies that protection measures are effective and that any retaliation is met with immediate corrective action.

The roles and responsibilities of management in whistleblowing:

1. Establishing accessible channels. Management provides secure, accessible and easy-to-use channels (such as external 24/7 hotlines or encrypted web platforms) that allow anonymous or strictly confidential reporting.
2. Drafting and enforcing procedures. Management creates clear, transparent written procedures detailing how reports are received, how investigations are conducted and how feedback is given to the reporter.

3. Appointing competent case handlers. Management designates and empowers impartial, trained individuals or functions (such as compliance) to handle incoming reports objectively. It is recommended to appoint an independent third-party provider to host the intake hotline or digital platform; this significantly increases employee trust and ensures that reporting data cannot be traced by the internal IT department and that reports are investigated independently.
4. Awareness and training. Management is responsible for continuously training staff on how to use the system and for educating managers on how to react appropriately when an employee raises a concern.
5. Taking corrective action. When an investigation confirms wrongdoing, management takes appropriate disciplinary action and updates internal controls to prevent recurrence.
6. Reporting to the Board and its audit committee. Management provides regular anonymised reports that allow the Board to fulfil its oversight duty.

The core conditions for whistleblowing to succeed are:

- Confidentiality and anonymity. The identity of the whistleblower must remain strictly confidential and be shared only on a need-to-know basis with those conducting the investigation. Anonymous reporting must be fully supported.
- Impartiality. Every report must be assessed objectively by a trained professional who has no personal or professional conflict of interest with the subject of the report.
- Timely feedback. The system must acknowledge receipt of reports promptly and provide the reporter with status updates within a reasonable, predefined timeframe.
- Actionable outcomes. Whistleblowing must yield tangible results; management must follow through with concrete disciplinary actions when wrongdoing is proven.
- Transparency. The whistleblowing policy and the reporting channel or form should be freely available on the company's external website (reachable from its home page). This demonstrates transparency to all stakeholders and ensures that external parties and former employees can easily access the channels.
- Tone in the middle. While the Board sets the tone at the top, management must ensure that middle managers and supervisors support the policy, translating ethical values into daily operational behaviour so that employees feel safe raising issues at departmental level.

Compliance with EU rules

When establishing or improving a whistleblowing framework, companies must ensure that it complies with the EU Whistleblowing Directive, as transposed in Estonia, Latvia and Lithuania, and with the GDPR, so that reports are handled lawfully and personal data are protected. The Directive requires companies with 50 or more employees to establish internal reporting channels and procedures.[21]

KEY TAKEAWAYS

A. A whistleblowing mechanism is a formal system that allows employees and external stakeholders to report misconduct, illegal activity or unethical behaviour safely. Its purpose is early detection, a speak-up culture, stakeholder trust and accountability that bypasses hierarchy.

B. The Board sets the tone, approves the whistleblowing policy, ensures the process is independent of executive management, provides a direct escalation route to the Chair or the audit committee for cases involving senior management, reviews anonymised metrics and protects those who report.

C. Management provides accessible and secure channels, clear procedures, impartial and trained case handlers (preferably with an independent external provider for intake), training, corrective action and regular reporting to the Board.

D. Whistleblowing succeeds only with confidentiality and anonymity, impartiality, timely feedback, actionable outcomes, transparency of the policy and channels, and support from middle management.

E. In the EU, the framework must comply with the Whistleblowing Directive, as transposed nationally, and with the GDPR; companies with 50 or more employees must have internal reporting channels.

21 Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law (the Whistleblowing Directive).

QUESTIONS FOR THE BOARD

1. *Do we have a Board-approved whistleblowing policy and secure channels that are known to employees and accessible to external stakeholders, including through our website?*
2. *Is the process independent of executive management, and would a report concerning the CEO or a Board member reach the Chair or the audit committee directly?*
3. *What did the last year's anonymised metrics show (number of reports, categories, closure times), and if there were no reports, why?*
4. *How do we know that whistleblowers are protected from retaliation, and what happened in the last case where someone raised a concern?*
5. *Do our channels and procedures comply with the national law transposing the EU Whistleblowing Directive and with the GDPR, and when were they last reviewed?*
6. *Does management, including middle management, treat raising concerns as an act of loyalty, and how does the Board know?*

5.3.4

CONFLICT OF INTEREST

A conflict of interest (***COI***) is a situation in which two or more parties have competing interests which may, actually or potentially, improperly influence a decision-making process and make it difficult for those involved to fulfil their duties fairly. In general terms, a COI exists where the interests of two parties collide, so that satisfying one is at the expense of the other.

In the context of Board work, a COI is a situation in which a Board member's personal, financial or other interests interfere, or could interfere, with their duty to act in the best interests of the company, thus compromising, or appearing to compromise, their ability to make impartial decisions on the company's behalf.

A conflict of interest typically arises when personal interests are placed above those of the company, and it usually materialises in the decision-making process. It may involve one party being able to take a decision affecting another, or holding or having access to information about another, where the decision or the information can benefit or harm the deciding or receiving party or a person related to it, and generally carries a risk of violating the rights of the other party.

Conflicts of interest are not in themselves illegal or prohibited. To ensure that they do not lead to corrupt practices, which may be subject to investigation and prosecution with serious legal, financial and reputational consequences, they must be disclosed, prevented, mitigated or managed.

Types of conflict of interest

A COI can be (i) actual, (ii) potential or (iii) perceived, and can arise in a wide variety of ways:

Actual COI: the person is influenced by a conflict of interest

An actual COI is a situation in which the circumstances clearly constitute a conflict: a Board member or another person related to the company faces a real and existing conflict of interest. For instance, the following situations constitute an actual COI:

- Serving on the Board of the company while also serving on the Board of a competitor or of a service provider of the company;
- The company entering into a transaction with a Board member or their related party;
- Hiring or supervising a relative, spouse, cohabitee or close friend;

- Using company assets for private benefit;
- Close personal relationships influencing decisions taken as part of the Board role;
- Using confidential information obtained in the role for one's own benefit.

Potential COI: the person could be influenced by a conflict of interest

A potential COI is a situation that does not yet constitute a conflict but where there is a reasonable possibility of an actual or apparent conflict arising. For instance:

- A person serves on the Boards of two companies that have no business relationship; a COI may arise if the two companies plan to do business together;
- Serving on several Boards, within or outside the group, which takes up a significant amount of time and raises the question whether the person can fulfil all of their duties and, if not, which will be prioritised;
- A Board member is a former official of a public authority; a COI could arise if the company becomes subject to an investigation by that authority;
- A Board member of company A also serves on the Board of company B, a client of company A; a COI could arise if company B were to file a complaint against company A.

Perceived COI: the person could appear to be influenced by a conflict of interest

A perceived conflict is a situation in which a person appears to have a COI even though this is not the case. For instance, the company hires a new employee who has the same surname as the CEO although they are not related.

Managing conflicts of interest

In performing their duties, Board members must act fairly and reasonably and be loyal to the company, without preference for the interests of any shareholder or group of shareholders, even if the Board member was nominated and appointed by that shareholder or group.

Proper management of conflicts of interest involves at least the following:

1. **Effective COI policy and processes.** The Board is responsible for ensuring that the company has effective procedures to identify, evaluate, prevent and mitigate conflicts of interest. The Board should approve the COI policy, regularly revise it and oversee its implementation. The policy should be reviewed at least every three years and whenever it becomes apparent that the processes it establishes are not effective.

2. **Training.** The company should organise initial training (on induction) and regular refresher training on conflicts of interest for the Board and employees, so that everyone is reminded of their obligation to identify and manage them and new recruits are informed in a timely manner.
3. **Declaration of interests.** Board members, senior management and key personnel must (i) declare their related parties (close family members and entities in which they or their close family members have a material holding, votes or influence), other positions and employments held currently or during the last three to five years, and any other material interests and affiliations that could influence their independence of mind in performing their duties; and (ii) update this information regularly (quarterly or annually) and whenever changes occur.
4. **Declaration of a COI.** Where a COI may arise in a specific situation (for example, the company intends to sign a contract with an entity controlled by a Board member), the Board member must declare the existence and nature of the potential conflict to the Chair and the Board without delay upon becoming aware of it. Best practice is to declare it as soon as the member learns that the matter is on the Board's agenda and before the Board materials on the matter are distributed.
5. **Checking for a COI.** Management preparing an agenda item, and the corporate secretary checking the materials before the Board pack is distributed, should check against the declarations of interests whether a COI may exist and, if so, advise the Chair accordingly. At the beginning of each meeting the Chair asks whether any member may have a COI in respect of any agenda item.
6. **Decision on the existence of a COI.** Upon declaration or identification of a possible COI, the Board evaluates the nature and circumstances of the situation and the interests disclosed and decides whether a COI exists. If it does, the Board evaluates its materiality and decides on the measures to prevent, mitigate or manage it.
7. **Recusal.** A Board member who has a COI must recuse themselves from the consideration of, and voting on, the agenda item concerned. Recusal means that the information and Board materials on the matter are not shared with the member, that the member does not take part in its consideration (including leaving the meeting while it is discussed), so that the non-conflicted members can discuss it freely and without bias, and that the member does not vote on it.
8. **No influence on the decision.** The Board member must not seek to influence in any other way the decision on the matter in which they have a COI.
9. **Documentation.** The declaration, identification and evaluation of a COI, the decision on its existence and the measures taken to prevent, mitigate or

manage it should be documented. It is also recommended to draw up separate minutes recording the discussion and decision on a matter in which a Board member has a potential COI. Such minutes are reviewed, approved and signed by, and available to, the non-conflicted members; the conflicted member is informed of the decision and has access only to the resolution part of the separate minutes.

10. **COI register.** The company should keep an up-to-date register of conflicts of interest and the measures taken to manage them.
11. **Continuing COI.** *A* COI of a continuing rather than one-off nature, and the measures taken to manage it, should be regularly revisited, re-evaluated and, if necessary, adjusted to ensure that they remain sufficient and effective. A continuing COI may arise, for example, from a long-term service contract between the company and an entity controlled by a Board member's spouse. Where a continuing COI would require the member to recuse themselves from most of the matters discussed by the Board (for example, advising or serving on the Board of a competing business), this should be assessed before the appointment, and the person should not be appointed, since constant recusal would prevent them from performing their duties.

KEY TAKEAWAYS

A. A conflict of interest arises when a Board member's personal, financial or other interests interfere, or could interfere, with their duty to act in the best interests of the company. Conflicts may be actual, potential or perceived, and are not illegal in themselves, but must be disclosed and managed.

B. Board members act loyally to the company and without preference for any shareholder, including the one that nominated them.

C. Managing conflicts requires a Board-approved policy, training, declarations of interests by Board members and key personnel, prompt declaration of a conflict when it arises, checks by management and the corporate secretary before each meeting, and a Board decision on whether a conflict exists and how to manage it.

D. A conflicted member recuses themselves from the materials, discussion and vote and does not seek to influence the decision in any other way; the process and decision are documented, with separate minutes where appropriate, and recorded in a COI register.

E. Continuing conflicts are revisited regularly; a conflict that would require constant recusal should rule out the appointment in the first place.

QUESTIONS FOR THE BOARD

1. *Do we have a Board-approved conflict of interest policy, when was it last reviewed, and are Board members and key personnel trained on it?*
2. *Have all Board members and senior managers submitted declarations of interests, and are they updated regularly and when circumstances change?*
3. *How is each Board agenda checked for potential conflicts before the materials are distributed, and does the Chair ask about conflicts at the start of every meeting?*
4. *When a conflict was last declared, did the member recuse themselves fully, and was the decision documented and recorded in the COI register?*
5. *Do any Board members have continuing conflicts, and are the measures taken to manage them still sufficient?*
6. *Does any Board member act, or appear to act, in the interest of the shareholder that nominated them rather than of the company?*

5.3.5

RELATED PARTY TRANSACTIONS

Related party transactions (RPTs) are one of the situations in which a COI is inherent. RPTs are usually legitimate transactions between the company and a related party. A problem arises where such a transaction allows the related party to extract more value from the company than it would otherwise be entitled to (for example, a majority shareholder being paid above the market price for goods it sells to the company).

The Board should approve the related party transaction policy, regularly revise it and oversee its implementation.

Related party

Although the definitions in national regulations differ in detail, for the purposes of RPT governance the concept of a related party usually includes at least the following persons:

1. a direct or indirect controlling shareholder of the company, or any other person that, through shareholding or otherwise, has sole or joint control or significant influence over the company;
2. a member of the Board or of the key management personnel of the company or its affiliated entities;
3. close relatives of the persons listed in (1) and (2);
4. the holding, subsidiary and other affiliated entities of the company and of the persons listed in (1) to (3).

Related party transaction

A related party transaction is any arrangement involving a transfer of value (resources, services, rights or obligations) between the company and a related party, irrespective of whether a price is charged.

RPT governance

RPT governance aims to distinguish, and prevent, RPTs that are unfair to the company, to its shareholders generally or to minority shareholders from transactions that benefit the company and enhance its value. Although national regulations differ,

good corporate governance requires at least the following standards in respect of RPTs:

1. **Sufficient information.** Management provides the approving body with sufficient information on the terms and conditions of the proposed transaction.
2. **Audit committee opinion.** The opinion of the Board's audit committee (if the company has one) on the proposed RPT is obtained before the Board approves it. Committee members with a potential COI in respect of the RPT recuse themselves from its consideration and the vote, and follow the other principles of COI management.
3. **Board approval.** The RPT is approved by the Board in accordance with the RPT policy. Board members with a potential COI in respect of the RPT recuse themselves in the same way.
4. **Approval conditions.** When considering and approving an RPT, the audit committee and the Board must ensure that:
    i. the transaction is at *arm's length*; if it is not, the approving body must evaluate and justify that the RPT is *in the best interests* of the company and is *not unfair* to the shareholders unrelated to it. Before approving the RPT, the audit committee or the Board may obtain an independent qualified third-party opinion on the fairness of the transaction (a *"fairness opinion"*);
    ii. **the same internal procedures** have been followed for the evaluation, approval and monitoring of the RPT as for any other third-party transaction;
    iii. continuing RPTs (for example, the provision of services over a period of time, as opposed to one-off purchases) are regularly revisited, including:

    – regular reporting on and monitoring of the performance of the RPT;

    – regular re-evaluation and re-approval of the transaction, to ensure that it continues to be at arm's length, fair and in the best interests of the company; and

    – a change of its terms, or its termination, where it can no longer be justified as fair or as serving the interests of the company.

5. **Disclosure.** RPTs are disclosed in the company's financial statements and annual report.

Transactions with related parties entered into in the ordinary course of business and on market terms, and non-material transactions, are usually excluded from prior evaluation and approval. The permitted exclusions should be defined in the RPT policy and comply with national regulatory requirements, and summary information

on such transactions should be reported regularly to the Board (for example, in the regular compliance reports).

KEY TAKEAWAYS

A. Related party transactions are transfers of value between the company and a related party: a controlling shareholder, a member of the Board or key management, their close relatives, or affiliated entities. They are usually legitimate but carry an inherent conflict of interest.

B. The Board approves an RPT policy, revises it regularly and oversees its implementation. Its purpose is to prevent transactions that are unfair to the company, its shareholders generally or minority shareholders.

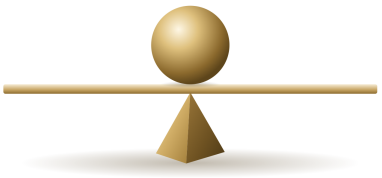
C. Before approval, management provides sufficient information, the audit committee gives its opinion, conflicted members recuse themselves, and the Board satisfies itself that the transaction is at arm's length or otherwise justified as being in the company's best interests, if necessary, with an independent fairness opinion.

D. RPTs follow the same procedures as any third-party transaction, continuing RPTs are re-evaluated and re-approved regularly, and RPTs are disclosed in the financial statements and annual report.

E. Ordinary-course, market-terms and non-material transactions may be excluded from prior approval if the policy so provides and the law allows, but summary information on them is still reported to the Board.

QUESTIONS FOR THE BOARD

1. *Do we have a Board-approved related party transaction policy that defines related parties, approval thresholds and permitted exclusions in line with national law?*
2. *Which related party transactions did the Board approve in the last year, and for each, how did it satisfy itself that the terms were at arm's length or otherwise in the company's best interests?*
3. *Did the audit committee give its opinion before approval, and did all conflicted members recuse themselves from the materials, discussion and vote?*
4. *Which continuing related party arrangements exist, when were they last re-evaluated, and are they still fair to the company?*
5. *Are related party transactions fully disclosed in the financial statements and annual report, and does the Board receive summary reporting on the transactions excluded from prior approval?*



CHAPTER

5.4

TECHNOLOGY AND INNOVATION

How the Board oversees digital transformation, the use of AI and the company's capacity to innovate.

IN THIS SECTION

5.4.1	Digital transformation and AI	158
5.4.2	R&D and innovation	162

5.4.1

DIGITAL TRANSFORMATION AND AI

Companies have recognised the importance of digital transformation for staying competitive, improving efficiency and meeting customer expectations. Today every company is involved in digitalisation to some extent, and the role of the Board is to lead and oversee the digital transformation of the company and to ensure that:

- digital transformation is aligned with the company's long-term vision and strategic objectives;
- digital initiatives are integrated into the overall business strategy;
- resources are used efficiently;
- it strengthens the company's competitive advantages and creates long-term value.

The Board plays a key role in setting the strategic direction of digital transformation, overseeing the process and ensuring that the transformation is aligned with the overall goals and interests of the company.

It is important to emphasise that the Board itself must ensure that it possesses the competencies required for digital transformation. If needed, additional Board members should be recruited to bring the essential competencies, experience and know-how to the Board.

The Board's role in digital transformation and its oversight has several aspects:

1. ***Setting the strategic direction of digital transformation.*** The Board defines the company's overall strategy, including its approach to digital transformation. This requires a clear view of the potential impact of digitalisation on the company's industry, and guidance to the company in implementing a digitalisation strategy that improves operations and enhances competitiveness.
2. ***Risk governance.*** Digital transformation usually involves significant change, the introduction of new technologies and adaptation to an evolving business environment. The Board must ensure that the related risks are identified, assessed and properly managed, and that the company's digital initiatives are aligned with its risk appetite and compliance requirements.
3. ***Resource allocation and ensuring the required capacity.*** The Board approves the budgets and resources for digital transformation initiatives and needs to ensure that the necessary financial, human and technological resources are available to support successful implementation.

4. ***Talent and leadership development.*** The Board should pay attention to the development and recruitment of leaders with digital expertise. This includes hiring executives who understand digital technologies and can drive the transformation agenda. The organisational structure should also be reviewed and adjusted where necessary. The Board may also encourage a culture of continuous learning, to ensure that the Board itself and the existing leadership are well equipped for the digital age.
5. ***Monitoring progress. The*** Board must set clear goals and establish key performance indicators (KPIs) to measure the progress of digital initiatives and assess the success of the transformation. It should receive regular updates and reports on the status of digital transformation projects, allowing it to assess how effectively the digitalisation strategy is being implemented and to make informed decisions.

Digital transformation initiatives are complex and require new competencies, many changes and substantial resources. It is no surprise that many of them fail. Common reasons for failure include:

- Lack of a clear strategy and vision, and of their communication to employees and stakeholders.
- Resistance to change and to the adoption of new technologies and processes.
- Insufficient skills at Board and management level.
- Poor integration of new technologies with existing systems.
- Poor data quality and governance, leading to inaccurate insights and decisions, and the lack of a data-centric culture and of an understanding of the value of data.
- Inadequate cybersecurity measures and protocols, leading to vulnerabilities and a failure to address the security risks associated with new technologies and data storage.
- Budget overruns, poor financial planning and underestimation of the costs of digital transformation projects.
- Lack of a customer-centric approach: focusing on technology rather than on understanding and meeting customer needs and expectations.
- Poor project management practices, including inadequate planning and monitoring.
- Failure to set realistic timelines and milestones.
- Difficulties in managing relationships with technology vendors and service providers, and over-reliance on external partners without ensuring alignment with the company's goals.

- Failure to establish key performance indicators (KPIs) and metrics for evaluating the success of digital transformation.
- Inability to measure and demonstrate the return on investment (ROI).

The Board needs to ensure that the digital transformation adheres to legal and ethical standards. Compliance with regulations on data protection, security, artificial intelligence and other relevant areas must be a priority.

Artificial intelligence

Artificial intelligence has become a matter for the Board, not only for management. The Board's role is oversight and strategic alignment, while management is responsible for the day-to-day execution of AI projects. In practice this means five things: approving an AI policy that sets the company's principles for the responsible use of AI (purpose and scope, governance and accountability, risk management, ethical standards such as fairness, transparency and human oversight, data governance and regulatory compliance) and aligning AI initiatives with the business strategy; approving the budgets and resources for AI and ensuring that the company has the infrastructure and the talent to deliver; ensuring that AI-related risks, including bias, privacy, security and legal liability, are assessed and managed within the company's overall risk management framework and that the requirements of the EU Artificial Intelligence Act are met; setting clear KPIs to evaluate the return on AI investments and reviewing progress regularly; and overseeing the impact on employees, the organisational culture and other stakeholders, including the training of the Board itself.

A useful distinction for the Board is that between automation, which follows fixed rules and mainly requires monitoring of efficiency and reliability, and AI, which learns from data and therefore calls for a more demanding governance framework. BICG's Guidelines for Integrating Artificial Intelligence into the Board Agenda provide a fuller treatment, including a Board-level AI governance checklist, an opportunities and risks matrix and an implementation roadmap.[22]

In summary, the Board plays a pivotal role in guiding and overseeing the digital transformation, ensuring that it is aligned with the company’s strategic objectives, managing risks, allocating resources and fostering a culture that supports innovation and adaptability in the digital era.

22 Baltic Institute of Corporate Governance, Guidelines for Integrating Artificial Intelligence (AI) into the Board Agenda, BICG Policy Group Lithuania, [2026], available at www.bicg.eu.

KEY TAKEAWAYS

A. Every company is digitalising to some extent. The Board leads and oversees the digital transformation and ensures that it is aligned with the long-term vision and strategy, integrated into the business strategy, resourced efficiently and focused on competitive advantage and long-term value.

B. The Board must have, or acquire, the competencies to do this: through the recruitment of Board members with digital expertise and through continuous learning.

C. The Board's role has five aspects: setting the strategic direction, risk governance, resource allocation, talent and leadership development, and monitoring progress through clear goals, KPIs and regular reporting.

D. Many digital initiatives fail for predictable reasons: unclear strategy, resistance to change, insufficient skills, poor integration and data quality, weak cybersecurity, budget overruns, a technology-first rather than customer-first approach, poor project management and over-reliance on vendors.

E. Digital transformation must comply with legal and ethical standards, including data protection, security and the emerging rules on artificial intelligence.

F. Artificial intelligence is a Board matter: the Board approves an AI policy, ensures that AI risks are managed within the risk management framework and that the EU AI Act is complied with, sets KPIs for AI investments and oversees the impact on people and culture.

QUESTIONS FOR THE BOARD

1. *Is our digital strategy part of the company strategy, and can the Board explain how digitali transformation changes our industry and our competitive position?*
2. *Does the Board have sufficient digital competence to challenge management, and if not, how will we close the gap?*
3. *Which digital transformation projects are under way, what are their goals and KPIs, and how do they perform against budget and timeline?*
4. *Are the risks of digital transformation, including cybersecurity, data quality and dependence on vendors, in the risk register and within our risk appetite?*
5. *Do we have the leadership, skills and organisational structure to deliver the transformation, and is the culture supporting rather than resisting it?*
6. *Where does the company use or plan to use artificial intelligence, and how do we ensure that its risks are managed and legal requirements met?*

5.4.2

R&D AND INNOVATION

Research and development (R&D) and innovation are two crucial activities that contribute strongly to a company's competitive advantage, market differentiation, revenue growth, cost efficiency, customer experience, brand, risk mitigation and overall success.

The Board plays a vital role in guiding and overseeing the company's R&D and innovation activities. Its responsibilities include:

1. Setting the strategic direction. The Board aligns R&D and innovation efforts with the company's long-term objectives, including the goals and priorities for R&D and innovation.
2. Approving budgets. The Board approves the budgets for R&D and innovation activities in line with the company's goals.
3. Providing support and resources. The Board supports R&D efforts by ensuring access to the necessary resources, such as talent (internal and external) and infrastructure. The Board should approve strategic partnerships that contribute to the achievement of the company's innovation goals.
4. Oversight and risk management. The Board oversees R&D and innovation activities to ensure that they are conducted in a manner consistent with legal, business and ethical standards. This includes managing the risks associated with R&D and innovation investments and projects, and ensuring that appropriate controls are in place.
5. Monitoring performance. The Board monitors the performance of R&D and innovation initiatives, assessing progress towards strategic objectives and evaluating the return on investment. This may involve reviewing key performance indicators, milestones achieved and financial metrics related to R&D and innovation.
6. Fostering a culture of innovation. The Board should ensure that top management fosters a culture of innovation within the company, encouraging creativity, experimentation and knowledge sharing among employees.
7. Identifying emerging technologies and trends. The Board should stay informed about emerging technologies, market trends and competitive dynamics that may affect the company's R&D and innovation strategy, and may provide guidance on adapting to changing market conditions and seizing new opportunities.

8. Holding top management accountable. The Board should hold top management accountable for the company's R&D and innovation performance, ensuring that resources are managed effectively and strategic objectives achieved. Effective communication between the Board and the top management team is essential for this oversight.

Three questions come up repeatedly in Board discussions of R&D and innovation and deserve a closer look.

Balancing incremental and disruptive innovation. Most of a company's innovation effort goes into incremental improvements to existing products, processes and services: these are lower in risk, closer to customers and easier to measure. Disruptive innovation, which creates new business models or markets, is rarer, riskier and slower to pay back, but it is what protects the company from being overtaken. The Board's task is not to choose between the two but to make sure that the portfolio is deliberately balanced. A practical approach is to ask management to present R&D and innovation projects as a portfolio, sorted by time horizon (short, medium and long term) and by level of risk, and to agree what share of resources should go to each category given the company's strategy, its position in the industry and the pace of change around it. A company whose portfolio contains only incremental projects is usually under-investing in its future; one with only ambitious projects is usually over-estimating its ability to deliver them. The Board should revisit the balance at least once a year and whenever the strategy changes.

Protecting intellectual property. The results of R&D are worth little if they can be freely copied. The Board should satisfy itself that the company has an intellectual property strategy that fits its business: what should be patented, what is better kept as a trade secret, which trademarks and designs should be registered and in which markets, and how software, data and know-how are protected. Equally important are the contracts through which intellectual property flows: employment and contractor agreements should assign to the company the rights in what is developed for it, and agreements with partners, universities and suppliers should state clearly who owns the results of joint work. The Board should also ensure that the company respects the rights of others, since infringement claims can be as damaging as the loss of the company's own rights, and it should receive a periodic overview of the intellectual property portfolio, its value and any disputes.

Comparing R&D spending with peers. There is no correct level of R&D spending; the right amount depends on the sector, the strategy and the stage of the company. What the Board can and should do is compare. Useful benchmarks are R&D expenditure as a share of revenue, the split between research and development,

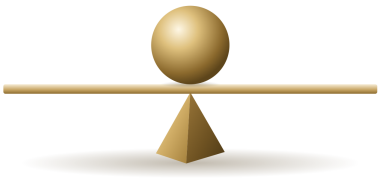
the proportion spent on incremental as opposed to new products, and the share of revenue that comes from products introduced in the last three to five years, each compared with listed competitors, sector averages and the company's own history. Public sources are often sufficient: the annual reports of listed peers, sector studies and the EU Industrial R&D Investment Scoreboard. The purpose of the comparison is not to match the peers but to explain the difference: a company that spends well below its sector should be able to say why that is consistent with its strategy, and one that spends well above should be able to show the results.

KEY TAKEAWAYS

- **A.** R&D and innovation are crucial to competitive advantage, market differentiation, growth, efficiency, customer experience and brand, and also to risk mitigation.
- **B.** The Board sets the strategic direction for R&D and innovation, approves the budgets, ensures the resources and strategic partnerships needed, and oversees that activities meet legal, business and ethical standards with appropriate controls.
- **C.** The Board monitors performance through key performance indicators, milestones and return on investment, and holds top management accountable for results.
- **D.** The Board should ensure that management fosters a culture of innovation, encouraging creativity, experimentation and knowledge sharing.
- **E.** The Board should stay informed about emerging technologies, market trends and competitive dynamics, so that it can guide the company in adapting and seizing opportunities.
- **F.** The Board judges the innovation portfolio as a whole, balancing incremental and disruptive projects by time horizon and risk; it ensures that the company's intellectual property is protected and the rights of others respected; and it compares R&D spending and results with peers to test whether the level of investment fits the strategy.

QUESTIONS FOR THE BOARD

1. *What are our innovation goals and priorities, and how are they linked to the company's long-term strategy?*
2. *How much do we invest in R&D and innovation compared with our competitors, and what has that investment delivered in the last three years?*
3. *Which KPIs and milestones does the Board use to monitor R&D and innovation, and when did it last review them?*
4. *Do we have the talent, partnerships and infrastructure needed for our innovation goals, and is our intellectual property protected?*
5. *Does the company culture encourage experimentation and tolerate well-managed failure, and how does the Board know?*
6. *Which emerging technologies or market trends could disrupt our business, and what is management doing about them?*
7. *Is our innovation portfolio deliberately balanced between incremental improvements and more ambitious projects, and when did the Board last review that balance?*



CHAPTER

5.5

LEADERSHIP AND REMUNERATION

How the Board selects, motivates, evaluates and plans the succession of the CEO, and how it oversees remuneration across the company.

IN THIS SECTION

5.5.1	The CEO: selection, motivation, evaluation and succession	167
5.5.2	Remuneration of the CEO, management and employees	172

5.5.1

THE CEO: SELECTION, MOTIVATION, EVALUATION AND SUCCESSION

One of the main functions of the Board is to select and appoint the most suitable CEO, to make sure that the CEO is properly motivated, evaluated and remunerated, and to replace the CEO if the results are unsatisfactory, the CEO retires or other circumstances, such as illness or death, make a change necessary.

Selection and appointment process

The nomination and appointment process is key to strong company performance and effective accountability. In a well-run company, the selection of candidates for the CEO position is therefore best conducted through the Board's nomination committee, where one exists, or by the Board itself. The task of the committee is to carry out the selection process for the appointment and re-appointment of the CEO (and other senior managers) and to make recommendations to the Board.

The CEO must be selected on the basis of the company's stage of development, future plans and ambitions. The profile will differ considerably depending on whether the company is in a start-up, growth, mature, turnaround or distress phase. The requirements for the CEO should be based on the company's current and expected needs.

When preparing the search for a new CEO, the Board or its nomination committee must weigh the merits of an internal candidate against those of an external one. Selecting an **internal candidate** may bring continuity and stability, better alignment with the long-term goals, familiarity with the company's culture and internal processes and stronger internal networks. An **external candidate** may bring a fresh perspective, an objective assessment of the company's challenges, the ability to drive change, wider business networks, and specialised expertise and experience that the company needs at that particular time. In each case the Board has to consider the long-term goals of the company, its stage of development and the qualities the new CEO will need.

There are several important aspects to consider when onboarding a newly appointed CEO:

- Onboarding process – a structured introduction is one of the most critical factors in helping a new CEO to work at full speed as soon as possible.
- Regular feedback – make sure that the new CEO receives the right information early; do not wait until things have gone too far before raising an issue.

- Tolerance of mistakes – no one is immune to mistakes, least of all a person who has just joined the company.
- Respecting roles – avoid the temptation to micro-manage or to solve problems that are the CEO's responsibility.
- Dealing with negative information and rumours – there will naturally be some displeased subordinates, and some of them may even try to undermine the new CEO by providing false, distorted or tendentious information.

Main employment terms and motivation

The main terms of the CEO's employment agreement for the Board to consider are:

- Non-compete – the main function of a non-compete clause is to provide the company with greater assurance that its intellectual property, information on clients, confidential resources and proprietary information will not be made available to or used by a competitor.
- Non-solicitation – this clause assists the company in retaining valuable employees and reduces the risk of their being recruited by a former CEO who would use their knowledge for competitive advantage.
- Confidentiality – a clause that goes hand in hand with the non-compete clause and prohibits the former CEO from sharing the company's confidential information, trade secrets and know-how with any third party, in particular a competitor, after the end of employment.
- Notice period – a clause setting the period of notice to be given by the CEO to the company, or by the company to the CEO, before termination takes effect. If no notice period is agreed, the statutory period applies, which may not suit the company's needs.

Once the CEO is selected, the Board should make sure that the CEO is motivated and appropriately remunerated in line with market and industry practice, using well-established means such as performance bonuses, share options and fringe benefits (company car, health care, life insurance and similar). The motivation system aims to ensure the achievement of the company's long-term goals.

Evaluation of performance

Evaluating the performance of the CEO is the responsibility of the Board, which often asks its relevant committee for assistance. The CEO is the link between the Board and the management team in the governance of the company, and the Board has an interest in the CEO being effective. As the Board and the CEO share responsibility for ensuring that the company meets its goals and objectives, the

following aspects of preparing and running the evaluation of the CEO's performance should be considered:

- the criteria against which the review is undertaken, agreed in advance;
- the use of common methods and tools for such reviews (360° feedback, company performance, stakeholder relations);
- a process run by the Board (its Chair) or a Board committee;
- an agenda for the review and the key issues to be discussed;
- sufficient time to prepare;
- an open and transparent manner (constructive criticism, areas for improvement, acknowledgement of achievements).

The purpose and benefits of evaluating the CEO's performance include:

- aligning the CEO's capabilities with the strategic direction of the company;
- spotting any potential management problems early on;
- setting appropriate goals for future growth;
- giving the Board greater objectivity about the CEO's remuneration;
- promoting collaboration between the CEO and the Board.

The success of the CEO's evaluation depends largely on setting the right KPIs at the outset and tracking the CEO's performance against them. KPIs may be "hard", based on specific metrics and therefore easily measurable (such as adherence to budget, financial performance or employee turnover), or "soft" and more difficult to measure (such as communication and personal qualities). The most widely used KPIs are SMART: specific, measurable, achievable, relevant and time-bound. Such KPIs enable the Board to make data-driven decisions, identify areas where the CEO or the company is falling short and take swift action to improve. Companies may choose other frameworks for setting the CEO's goals and objectives, such as OKRs (objectives and key results), FAST (frequently discussed, ambitious, specific, transparent) or CLEAR (collaborative, limited, emotional, appreciable, refinable).

The CEO's performance should be monitored and constructive feedback given on an ongoing basis (quarterly or at least twice a year). This alerts the Board to emerging issues and gives the Board and the CEO the opportunity to address them before they escalate.

Succession planning

Succession planning is critical to the continuity of the business and is increasingly recognised as a significant aspect of good corporate governance. It is the process of identifying and developing new leaders and key employees who can replace

existing ones when they leave or retire. Failure to focus on succession planning may result in a weak, ineffective and insufficiently diverse senior management team, which in turn creates a risk to the company's long-term success.

The aims and advantages of good succession planning include:

- ensuring that the senior management team consists of people with the right diversity of skills and talent needed to achieve the company's business objectives and promote its long-term success;
- having a procedure for identifying and developing possible successors to the CEO and other key employees, which includes determining the experience, professional capabilities and personal characteristics needed for each senior management role and assessing candidates in the light of the company's strategy and culture; and
- selecting the optimal candidates to replace the CEO and other key employees following their departure, whether planned or unexpected.

There is no one-size-fits-all way of approaching these issues, nor is there one specific succession planning procedure that would suit every company. The Board must therefore take into account the company's particular situation when formulating and implementing its succession planning policy.

To maintain continuous and efficient operations and a seamless transition of leadership, the succession planning process should be properly defined and implemented. A written succession plan is therefore highly recommended. It should at least include:

- the key (critical) management positions in the company;
- potential successors, their development plans and development opportunities;
- a step-by-step plan for emergency succession;
- alignment with the company's strategy;
- legal and financial considerations;
- regular review and updating.

The succession plan and its execution should be reviewed by the Board at least annually.

KEY TAKEAWAYS

A. Selecting, motivating, evaluating and, when necessary, replacing the CEO is one of the Board's most important functions. The selection is best run by the nomination committee, where one exists, and the profile must match the company's stage of development and expected needs.

B. Internal and external candidates each have advantages; the Board weighs continuity and cultural fit against fresh perspective and change capability in the light of the company's long-term goals.

C. A new CEO needs structured onboarding, early and regular feedback, tolerance of initial mistakes and a Board that respects the boundary between oversight and management.

D. The CEO's contract should address non-competition, non-solicitation, confidentiality and the notice period, and the remuneration should motivate the achievement of long-term goals.

E. The Board evaluates the CEO against criteria and KPIs agreed in advance, in an open and transparent process, with feedback at least twice a year.

F. Succession planning for the CEO and other key positions, including an emergency plan, is part of good governance; the plan should be written and reviewed by the Board at least annually.

QUESTIONS FOR THE BOARD

1. *Does the Board have an agreed profile for the CEO that reflects the company's stage of development and strategy, and a defined process, led by the nomination committee or the Board, for selection and re-appointment?*
2. *How did the Board support the current CEO in the first months, and does it respect the line between oversight and management?*
3. *Does the CEO's contract contain adequate non-compete, non-solicitation, confidentiality and notice provisions, and when were they last reviewed?*
4. *Against which KPIs and criteria is the CEO evaluated, were they agreed at the start of the year, and when did the Board last give the CEO structured feedback?*
5. *Do we have a written succession plan for the CEO and other critical positions, including emergency succession, and when did the Board last review it?*
6. *Who would run the company tomorrow if the CEO were unexpectedly unavailable, and does that person know it?*

5.5.2

REMUNERATION OF THE CEO, MANAGEMENT AND EMPLOYEES

Remuneration policy

The Board is responsible for establishing the remuneration policy for the CEO, Management Board members, other managers and employees of the company and for ensuring its effectiveness. To assist the Board in this responsibility, a remuneration committee may be established; larger companies and public-interest entities usually establish one, to comply with the more stringent regulatory requirements that apply to them and with good corporate governance practice.

In relation to remuneration, the main functions of the Board are to:

1. adopt the remuneration policy and ensure its regular review;
2. oversee the implementation of the remuneration policy and practices, to make sure that the policy operates as intended and continues to comply with applicable laws;
3. ensure that the remuneration of the CEO and management, both the elements of the package and the actual amounts awarded, achieves the objectives of the remuneration policy;
4. provide sufficient information to shareholders and other stakeholders to ensure external transparency of the remuneration policy and of management remuneration packages.

For listed companies, the EU Shareholder Rights Directive II, as transposed in Estonia, Latvia and Lithuania, requires the remuneration policy to be submitted to the general meeting of shareholders for a vote and an annual remuneration report to be published and put to the general meeting. State-owned and municipally owned enterprises are subject to additional statutory rules and limits on management remuneration. The Board should know which of these requirements apply to the company.[23]

The remuneration policy, and the practices used to determine remuneration, should be clear, documented and transparent. The remuneration policy should:

1. state its objectives, which should generally be to ensure that the company:
    a. provides strong incentives for management to perform in a way that is aligned with the company's long-term goals and increases long-term value

for its shareholders and other stakeholders, taking into account the company's sustainability (ESG) goals;

   b. attracts and retains the talent necessary for its successful operation;

2. be aligned with the company's purpose, vision, mission, strategy, long-term objectives and values;
3. be objective and fair, based on rewarding performance and results aligned with the long-term goals of the company;
4. be gender-neutral, non-discriminatory and inclusive;
5. provide an effective framework for performance measurement and a clear link between reward and performance aligned with the company's long-term goals;
6. include the following:
   a. a description of the structure of the remuneration package, listing all components of fixed and variable remuneration, including all bonuses and other benefits in whatever form that may be awarded to management, and their relative proportions;
   b. a link between the variable part of remuneration and the financial and non-financial performance of the company and of the individual manager;
   c. where the company awards share-based remuneration, the vesting and delivery periods and, where applicable, the rules for retaining shares after delivery;
   d. the possibility of, and conditions for, adjusting variable remuneration before it is awarded (malus) and reclaiming it after payment (claw-back), in the event of failure to achieve the performance targets, payment based on misstated data or serious misconduct by the manager concerned;
   e. the deferral of part of the cash or share-based variable remuneration;
7. be reviewed regularly, preferably at least once a year and whenever the need arises (for example, changes in the company's strategy or in labour market trends).

Management remuneration package

The management remuneration package is the total amount a manager earns for their performance and for achieving the objectives set by the Board. It may consist of various elements and usually includes:

– ***Fixed remuneration*** *(fixed monthly salary)* is non-discretionary: it cannot be unilaterally adjusted by the company or the Board and does not depend on the

23 Directive (EU) 2017/828 amending Directive 2007/36/EC as regards the encouragement of long-term shareholder engagement (Shareholder Rights Directive II), Articles 9a and 9b.

manager's performance. Its amount may vary greatly according to the business sector, the manager's experience and track record and other considerations.

– ***Performance-based variable remuneration*** depends on the performance of the company and of the manager, that is, on the achievement of company and individual goals. It is good practice to ensure that such remuneration is at all times aligned with the achievement of the company's long-term goals and the shareholders' interests.

It is common to provide variable remuneration as an ***annual*** cash bonus (***short-term incentive***, ***STI***), which usually ranges from one to six months of the manager's fixed salary. Good practice, however, is for the major part of variable remuneration to be tied to the achievement of ***long-term*** goals (long-term incentive, ***LTI***). An LTI programme usually (a) runs for three to five years, (b) is larger than the STI, (c) preferably consists of shares as well as cash, (d) includes the deferral of part of the cash element, the delivery of awarded shares at the end of the programme and a requirement to retain part of the delivered shares for a certain period, and (e) allows the awarded cash or shares to be adjusted or reclaimed in the event of misconduct or a subsequent restatement of the company's financial results. The Board may also award ***a one-off*** cash bonus for extraordinary performance, significantly above the goals set or in extraordinary situations that were not taken into account when the goals were set.

– ***Other cash and in-kind benefits*** provided by the company, such as health insurance, life insurance, a car or travel allowance, pension plans, sports and wellness programmes, family leave, compensation of relocation costs and discounts on company products or services.
– ***Severance pay*** is a payment for early termination of the contract (before the end of the term for fixed-term contracts, or before retirement for indefinite contracts), which may amount to 6 to 18 months of fixed monthly salary. Such conditions could be a subject to national law.

When defining and reviewing the management remuneration package, the Board should take into account the latest market data and trends in salaries, to ensure that its decision fits the market and motivates management.

KEY TAKEAWAYS

A. The Board establishes the remuneration policy for the CEO, management and employees and ensures its effectiveness, usually with the support of a remuneration committee in larger companies and public-interest entities.

B. The policy should be clear, documented and transparent, aligned with the company's purpose, strategy and values, objective, fair and inclusive, and built on a clear link between reward and performance against the long-term goals, including sustainability goals.

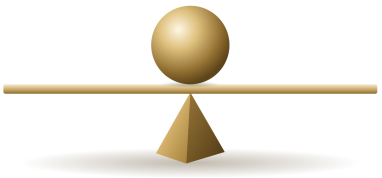
C. The policy should describe all components of fixed and variable remuneration and their proportions, link variable pay to financial and non-financial performance, and provide for deferral, share retention, malus and claw-back.

D. A remuneration package typically consists of fixed salary, short-term and long-term variable remuneration, other benefits and severance terms; good practice ties the larger part of variable pay to long-term goals through an LTI programme of three to five years.

E. For listed companies the remuneration policy and report are put to the shareholders under SRD II, and state-owned enterprises face statutory limits; the Board sets pay with reference to current market data.

QUESTIONS FOR THE BOARD

1. *Has the Board approved a remuneration policy covering the CEO, management and employees, and when was it last reviewed?*
2. *Is the variable remuneration of the CEO and management clearly linked to the company's long-term goals, including sustainability goals, and is the larger part of it long-term?*
3. *Does the policy provide for deferral, share retention, malus and claw-back, and have these provisions ever been applied?*
4. *How does management remuneration compare with the market and with the pay of the wider workforce, and can the Board justify the differences?*
5. *Are the legal requirements on shareholder approval and disclosure of remuneration (SRD II, rules for state-owned enterprises) met, and is the remuneration report clear to shareholders?*
6. *Are the amounts of severance pay in management contracts reasonable, and are they known to the Board before a termination decision is taken?*



CHAPTER

5.6

SHAREHOLDERS, STAKEHOLDERS AND ACCOUNTABILITY

How the Board protects shareholder rights, builds relationships with stakeholders and accounts for its decisions through disclosure and communication.

IN THIS SECTION

5.6.1	Rights and equitable treatment of shareholders	177
5.6.2	Stakeholder relationship governance	180
5.6.3	Board accountability, disclosure and communication	185

5.6.1

RIGHTS AND EQUITABLE TREATMENT OF SHAREHOLDERS

The **protection** of shareholder rights and the **equitable treatment** of shareholders are **core elements of a sound corporate governance framework**. They are especially important in the Baltic states, where companies may have concentrated ownership structures, controlling shareholders, family owners, state or municipal owners, and, in listed companies, minority investors. Good governance requires that all shareholders are treated fairly, that their rights are respected in practice, and that control is exercised responsibly.

Shareholders **should have secure and effective rights** to participate in fundamental corporate decisions. These include the right to vote at general meetings, elect and remove Board members, approve major changes to the company's statutes or share capital, receive dividends when declared, and obtain relevant information on the company. Shareholders should also have the right to receive timely notice of general meetings, review meeting materials in advance, ask questions, submit proposals where permitted by law, and vote in person, by proxy or through electronic means where available. These rights should not exist only formally; companies should organise shareholder engagement in a way that enables informed and meaningful participation.

Equitable treatment means that shareholders of the same class should be treated equally. Minority shareholders should be protected from abusive actions by controlling shareholders, management or the Board. This is particularly relevant in companies with a dominant shareholder, family-controlled companies, state-owned enterprises, municipal companies and group structures. Transactions with related parties, changes in control, share issuances, dividend decisions, asset transfers and intra-group arrangements should be handled transparently and on fair terms. The Board should ensure that such matters are properly reviewed, conflicts of interest are managed, and decisions are taken in the interests of the company as a whole.

The Board has a **central responsibility** in protecting the integrity of shareholder governance. Board members should not see themselves as representatives of the shareholder who nominated them, but as fiduciaries of the company. Once elected, they must exercise independent judgement, act with due care and loyalty, and consider the long-term interests of the company. This is particularly important where Board members are nominated by controlling shareholders, the state, a

municipality, private equity investors or family owners. The Board should create conditions for constructive shareholder dialogue, while preserving the clear division between ownership, Board oversight and executive management.

Transparent communication is essential for shareholder confidence. Listed companies should provide accurate, timely and balanced disclosure to the market, ensuring that all investors receive material information at the same time. Private companies should also establish appropriate information flows between the company, the Board and shareholders, especially where not all shareholders are involved in management. In family businesses and closely held companies, clear reporting practices can reduce mistrust and prevent conflicts. In state-owned and municipal companies, transparency supports public accountability and helps protect the company from political or informal influence.

Shareholder engagement should be encouraged, but it should be structured and responsible: **shareholders should not bypass the Board** by giving informal instructions to management or individual Board members. The company should have clear procedures for shareholder communication, including how shareholder proposals, questions and concerns are addressed.

Equitable shareholder treatment also requires effective management of conflicts of interest. Board members, executives and controlling shareholders should disclose personal, financial or related-party interests that may affect their judgement. The company should have **clear procedures** for approving related-party transactions, including review by independent Board members or a relevant Board committee where appropriate. Material related-party transactions should be disclosed in accordance with law and good practice.

In practice, good shareholder governance depends not only on legal rights, but also on culture. **Owners should exercise their rights responsibly**; Boards should **protect the interests of the company** as a whole; and management should operate within clear authority delegated by the Board. The objective is not to weaken ownership influence, but to ensure that ownership is exercised transparently, fairly and in a manner that supports sustainable success, investor confidence and long-term value creation.

KEY TAKEAWAYS

A. The protection of shareholder rights and the equitable treatment of shareholders are core elements of governance, and especially important in the Baltic states, where ownership is often concentrated in controlling, family, state or municipal hands alongside minority investors.

B. Shareholders should have effective rights to participate in fundamental decisions: to be notified of and vote at general meetings, elect and remove Board members, approve changes to the statutes and capital, receive dividends and obtain information, in person, by proxy or electronically.

C. Shareholders of the same class are treated equally, and minority shareholders are protected from abuse in related party transactions, changes of control, share issues, dividends, asset transfers and intra-group arrangements.

D. Board members are fiduciaries of the company, not representatives of the shareholder who nominated them; they exercise independent judgement and act in the long-term interests of the company as a whole.

E. Transparent communication, structured shareholder engagement that does not bypass the Board, and the management of conflicts of interest sustain shareholder confidence; ultimately, good shareholder governance depends on culture as much as on legal rights.

QUESTIONS FOR THE BOARD

1. *Are our shareholders, including minority shareholders, able to exercise their rights effectively: timely notice, access to materials, questions, proposals and voting by proxy or electronic means?*
2. *How does the Board ensure that related party transactions, capital changes, dividends and intra-group arrangements are reviewed independently and concluded on fair terms?*
3. *Do Board members nominated by a controlling shareholder, the state or a municipality act as fiduciaries of the company, and how would the Board respond to informal instructions from an owner?*
4. *Do all shareholders receive material information at the same time, and do we have clear procedures for handling shareholder questions, proposals and concerns?*
5. *How does the Board maintain a constructive dialogue with the owners while preserving the division between ownership, Board oversight and executive management?*

5.6.2

STAKEHOLDER RELATIONSHIP GOVERNANCE

Stakeholders are individuals, groups or organisations that have a stake in the company, through interest, influence or both, each with their own needs and expectations. They range from shareholders, employees and Board members to lenders, customers, suppliers, government and local communities.

According to the G20/OECD Principles of Corporate Governance, "The corporate governance framework should consider the rights, roles and interests of stakeholders and encourage active co-operation between companies, shareholders and stakeholders in creating value, quality jobs, and sustainable and resilient companies."[24]

There are many benefits to building and maintaining positive stakeholder relationships, including:

- lower operational and project risk;
- a stronger reputation;
- buy-in for the company's plans;
- compliance with regulatory requirements;
- competitive advantage.

Identification of stakeholders

The first step is to identify the key stakeholders: to determine the stakeholder groups and understand their needs and the roles they play. Some simply need to be kept informed, while others directly influence the company's operations or the outcome of particular projects.

Mapping the stakeholders

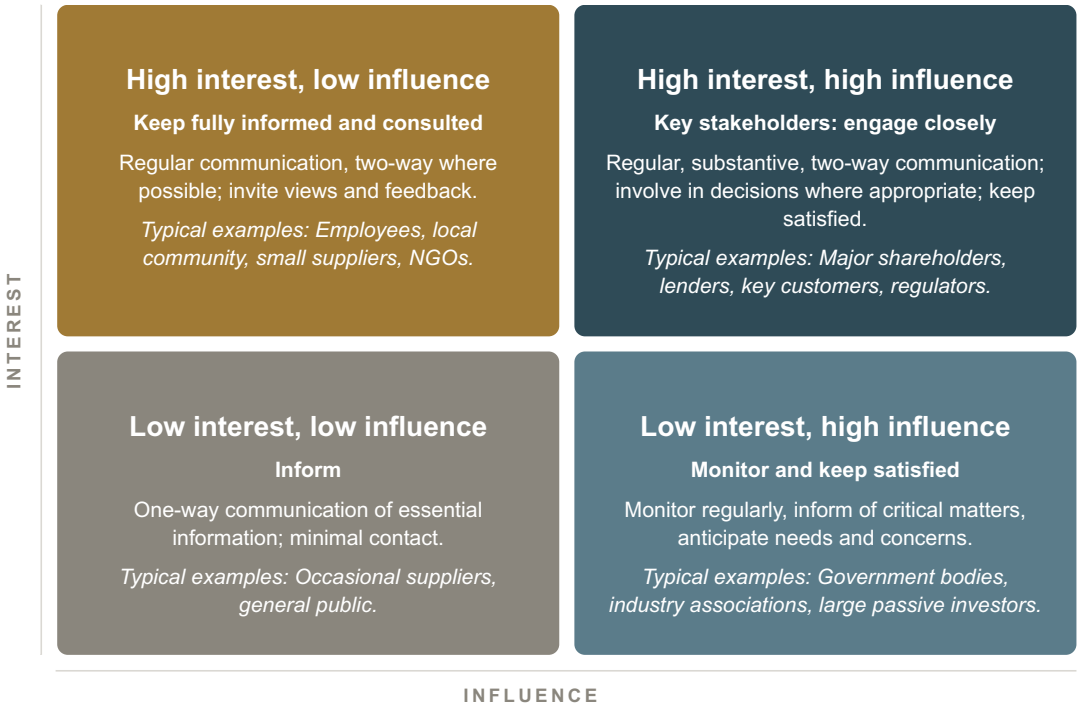
By mapping its stakeholder groups, the company can develop a plan to engage with each group in the way that works best for it. This makes the best use of resources: groups that need less attention are not over-communicated with, while the groups with high interest and high influence are engaged in greater depth.

When mapping stakeholders, place them in one of the four categories shown in the figure below.

24 OECD (2023), G20/OECD Principles of Corporate Governance, OECD Publishing, Paris, Chapter IV, The role of stakeholders in corporate governance.

Figure 5.7 **Stakeholder mapping by interest and influence**

Figure 5.7 **Stakeholder mapping by interest and influence**



Stakeholder mapping places each stakeholder group according to its interest in the company and its influence over it, so that the company can engage with each group in the way that suits it and make the best use of its resources. The key stakeholders, with high interest and high influence, are engaged closely and may be involved in decisions; highly interested groups with less influence are kept fully informed and consulted; influential groups with little day-to-day interest are monitored and their needs anticipated; and groups with low interest and low influence receive essential information only. The map should be reviewed regularly, since interest and influence change with circumstances.

It is very important to share information with stakeholders clearly and in good time, using the channels each stakeholder group prefers. Trust is established and maintained by being transparent about the status and plans of the company's activities and projects. Good communication is essential to share the company's vision with its stakeholder groups: provide the big picture, with timelines and key milestones where needed.

Another part of communication with stakeholders is active listening, one of the most important stakeholder communication skills. Listen to their feedback and make sure that their perspectives, suggestions and concerns are understood. It is good practice to convene stakeholder forums and invite key stakeholder representatives. Stakeholders who feel heard are far more likely to trust the company.

To embed stakeholder engagement in the company's operations, the Board should:

1. define stakeholder engagement as a core value;
2. identify, discuss and prioritise the key risks associated with changing societal expectations;
3. determine the Board's financial and non-financial information needs for decision-making, management oversight and the monitoring of key stakeholder relationships;
4. discuss and approve key performance indicators for social, environmental and financial performance;
5. approve a policy for external reporting;
6. integrate stakeholder issues into the annual general meeting of shareholders;
7. discuss the risks and impacts of projects and operations and provide transparent disclosure to shareholders and other key stakeholder groups;
8. convene stakeholder forums and invite key stakeholder representatives to address Board meetings;
9. consider establishing a stakeholder relations committee.

Balancing the interests of the stakeholder groups

Different stakeholder groups may have different and sometimes opposing interests. For instance, employees want higher pay while customers want lower prices, and one part of a community wants well-paid jobs while another does not want a factory built nearby.

The Board should consider the interests of the relevant stakeholder groups and find the most suitable way to balance them, taking into account the interests and long-term goals of the company.

Addressing conflicting interests requires careful consideration, compromise and effective communication by the Board, to find solutions that balance the needs of stakeholders while maintaining the sustainable development of the company and observing ethical standards. The key activities and considerations are:

1. Stakeholder identification. The Board should ensure that the company identifies its stakeholder groups and their interests (see stakeholder mapping above).
2. Stakeholder communication. The Board should ensure that the company establishes clear and consistent communication channels and delivers relevant and timely information about its activities and plans and their impact. The company should also actively seek stakeholders' feedback: communication should flow in both directions.

3. Balancing interests. Not all stakeholder groups have the same interests, so compromises are needed. The company should balance the different interests and seek solutions that benefit all sides, cooperating with key stakeholders and involving them in decision-making where appropriate. Engaging them builds a sense of mutual benefit and loyalty. The costs, benefits and risks of each alternative should be considered, together with the short- and long-term implications for the company and its stakeholders. Such an approach benefits the company's competitiveness and image.
4. Monitoring and assessment. It is important to monitor and regularly assess the results of business decisions against the interests and opinions of the stakeholder groups, for example by evaluating stakeholders' reactions and satisfaction. In this way the Board and the company understand the real consequences of their decisions and can make the necessary adjustments and improve their decision-making.

KEY TAKEAWAYS

A. Stakeholders are all those with a stake in the company through interest, influence or both; the G20/OECD Principles call for their rights, roles and interests to be recognised and for active cooperation in creating value.

B. Good stakeholder relationships lower risk, strengthen reputation, secure buy-in, support compliance and create competitive advantage.

C. Stakeholders are identified and mapped by interest and influence; the key stakeholders, with high interest and high influence, receive regular, substantive, two-way communication, while other groups are informed or monitored proportionately.

D. Communication with stakeholders is clear, timely and delivered through the channels each group prefers, and it includes active listening, for example through stakeholder forums.

E. The Board embeds stakeholder engagement in the company's operations, sets KPIs for social, environmental and financial performance, approves the external reporting policy and, where interests conflict, balances them in the long-term interest of the company and monitors the results.

QUESTIONS FOR THE BOARD

1. *Who are our key stakeholders, when did we last map them by interest and influence, and does the map reflect changes in our business and environment?*
2. *Does each key stakeholder group receive the communication it needs, through the channels it prefers, and how do we listen to what they tell us?*
3. *Which stakeholder interests conflict with each other or with the company's plans, and how has the Board balanced them in recent decisions?*
4. *Has the Board approved KPIs for social, environmental and financial performance and a policy for external reporting, and does it review them?*
5. *Do we monitor stakeholders' reactions to our decisions and adjust where necessary, and would the Board know if a key relationship were deteriorating?*

5.6.3

BOARD ACCOUNTABILITY, DISCLOSURE AND COMMUNICATION

The G20/OECD Principles of Corporate Governance state that "The corporate governance framework should ensure that timely and accurate disclosure is made on all material matters regarding the corporation, including the financial situation, performance, sustainability, ownership, and governance of the company."[25]

Timely and proper accountability strengthens the company's transparency, which improves its relationships with stakeholders and increases trust.

The Board is responsible for overseeing the company's performance, ensuring effective control of operations and being accountable to shareholders and other stakeholders for the company's activities, disclosing a true, timely and understandable picture of the company's position and prospects.

The annual report is the primary document for which the Board is accountable; it is described in the section "Disclosure and communication" below.

To give the Board, shareholders and other stakeholders external and objective assurance that the financial statements present fairly, in all material respects, the financial position and performance of the company, the financial statements must be audited by an independent, competent and qualified auditor in accordance with high-quality international auditing standards (see sub-chapter 5.2.6).

The G20/OECD Principles of Corporate Governance stipulate that the following information should be disclosed:[26]

1. The financial and operating results of the company
2. Company objectives and non-financial sustainability information
3. Capital structures, group structures and their control arrangements
4. Major share ownership, including beneficial owners, and voting rights
5. Remuneration of members of the Board and key executives
6. Information about Board members, including their qualifications, the selection process, their composition, other company directorships and whether they are regarded as independent by the Board
7. Related party transactions

25 OECD (2023), G20/OECD Principles of Corporate Governance, Chapter V, Disclosure and transparency.
26 OECD (2023), G20/OECD Principles of Corporate Governance, Principle V.A.

8. Foreseeable risk factors
9. Governance structures and policies, including the extent of compliance with the applicable corporate governance code and how it is implemented
10. Debt contracts, including the risk of non-compliance with covenants

To improve the quality of corporate disclosures, companies should move away from generic, declaratory statements in favour of **concise, company-specific reporting** that explicitly links initiatives to the company's purpose, strategy and values. This is best achieved by highlighting **measurable outcomes and impacts** rather than merely describing policies, while ensuring that all reporting on stakeholder engagement demonstrates how external views have directly influenced Board decisions. Furthermore, disclosures must provide transparency into **governance practices**, specifically detailing how the Board reviews the effectiveness of risk management systems and how executive remuneration is aligned with long-term cultural and strategic goals.

As the risk profile of the business changes constantly, accountability needs to be ingrained in the culture of the company and subject to regular review. A strong sense of accountability and the application of best practice help to safeguard the reputation of the company and of its Board members. Stakeholders scrutinise companies and their Boards ever more closely, and accountability procedures should be an important part of the Board's duties.

All relevant regulations and EU directives, in particular the Corporate Sustainability Reporting Directive (CSRD) and the accounting and transparency rules, should be taken into account when setting up the framework for the company's disclosures and reporting.[27]

The Board must ensure that all material information is disclosed in a timely manner and through the channels most suitable for the company's stakeholders.

Disclosure and communication

The significance of a company's disclosure and communication cannot be overstated: transparency fosters trust and is a crucial component of sound business practice.

Each stakeholder group has distinct interests in the company. For instance:

– shareholders and investors are interested in the company's performance, prospects, governance practices and Board composition;

27 Directive (EU) 2022/2464 on corporate sustainability reporting (CSRD); its scope and timetable were amended by the EU "Omnibus" simplification package adopted in 2025–2026.

- regulators and authorities are concerned with the company's compliance with laws and regulations;
- customers focus on the safety and sustainability of products and on warranties;
- employees are interested in the company's performance, remuneration practices and workplace safety.

Further details on stakeholder groups and their interests can be found in sub-chapter 5.6.2.

The Board should ensure that the **communication strategy** is grounded in stakeholder mapping and prioritisation. In this way the Board helps the company to build robust relationships with its stakeholders, manage risks more effectively and achieve its objectives, with better outcomes for all parties.

The Board should formulate and approve a **disclosure and communication policy** that sets out how the company communicates and discloses information and how the Board oversees this. All other internal documents on the subject should be developed on the basis of this policy and approved by the CEO. The information disseminated by the company should be timely, accurate and relevant.

The primary sources of disclosure and communication are the following.

The **company's annual** report is a fundamental document of its accountability, and the Board should be actively involved in its preparation. A well-crafted annual report should be comprehensible to a broad audience, not only to experts. Besides information about the company's past performance and current position, it should include the latest developments and a view of the future. The annual report should contain the following key sections:

- letters from the Chair of the Board and the CEO;
- the company's purpose, vision, mission and values;
- brief highlights of the strategy (the full strategy document should remain confidential);
- the major risks that could prevent the company from achieving its objectives, how they are managed and how risk management is organised;
- analysis of external factors and trends and of the internal situation of the company;
- a description of the company's operations, its business model and how value is created;
- the governance of the company, including the Board and its committees, their performance and remuneration, governance practices and policies and performance against them;

– the company's financial and non-financial (including sustainability) performance against the targets set.

The Board should lead the preparation of the annual report, with management preparing the information. It is good practice to divide the preparation into steps:

1. discussion and agreement of the topics (the table of contents);
2. preparation by management, and review by the Board, of the first draft of the non-financial part;
3. final review of the full document, including the financial information;
4. endorsement of the annual report and its submission for approval by the general meeting of shareholders. The annual report should be communicated both internally and externally and be accessible on the company's website.

In recent decades companies have adopted a broader form of accountability, integrated **reporting**: a process that results in communication by the company, most visibly a periodic integrated report, about how it creates value over time. The Integrated Reporting Framework is now maintained by the IFRS Foundation.[28]

The Board should be aware of recent and forthcoming **EU rules** on corporate reporting, in particular the CSRD, the European Sustainability Reporting Standards (ESRS) and the Corporate Sustainability Due Diligence Directive (CSDDD), and ensure that the company complies with them.

The **company's website** is another vital, easily accessible and widely used source of information. It should be user-friendly, allowing easy navigation and access to up-to-date and relevant information, and offer interactive communication.

The website should contain comprehensive information about the major owners, the Board, management and the internal auditor. All relevant documents, such as the articles of association, the charters of the Board and its committees, policies, codes and annual reports, should be readily accessible.

If the company operates beyond its country of registration, it should provide information in other languages, ensuring that the scope of information is consistent across all languages. A whistleblowing section (see sub-chapter 5.3.3) should be prominently placed on the home page for easy access. Given the risk of hacking, robust security measures and regular back-ups of the website are essential.

To ensure effective corporate communication, the Board must take a proactive approach to overseeing communication practices, processes and monitoring mechanisms. This helps to safeguard and enhance the company's reputation, foster

28 IFRS Foundation, Integrated Reporting Framework (2021), available at www.integratedreporting.ifrs.org.

stakeholder trust and promote the company's success. To this end, the Board should:

1. approve a comprehensive communication strategy;
2. formulate and approve a disclosure and communication policy;
3. ensure that a dedicated person, such as a communication manager, is responsible for corporate communication;
4. regularly assess the CEO's communication;
5. regularly review and approve key communication materials, such as the financial statements and the annual report;
6. ensure that a crisis communication plan is in place, regularly reviewed and updated and supported by training (see sub-chapter 5.2.4);
7. ensure effective internal communication.

The primary communicator should be the CEO, with the Chair or other Board members stepping in only when the CEO is unable to communicate, for instance because of misconduct or absence.

The Board must remember that it is the ultimate guardian of the company's reputation.

Reputation management

In creating and maintaining reputation, the Board's role is to ensure that all the factors contributing to the company's reputation are coordinated, including the reward and incentive systems. If these systems reward individual action, communication about teamwork will be ineffective, since people behave in line with how they are measured rather than with what they are told.

With **social networks**, customer service has become part of public communication, since customers often express their dissatisfaction on these platforms. The Board must therefore ensure that customer service systems and standards are aligned with the communication strategy and that practical solutions are implemented when issues become public.