5.3.2

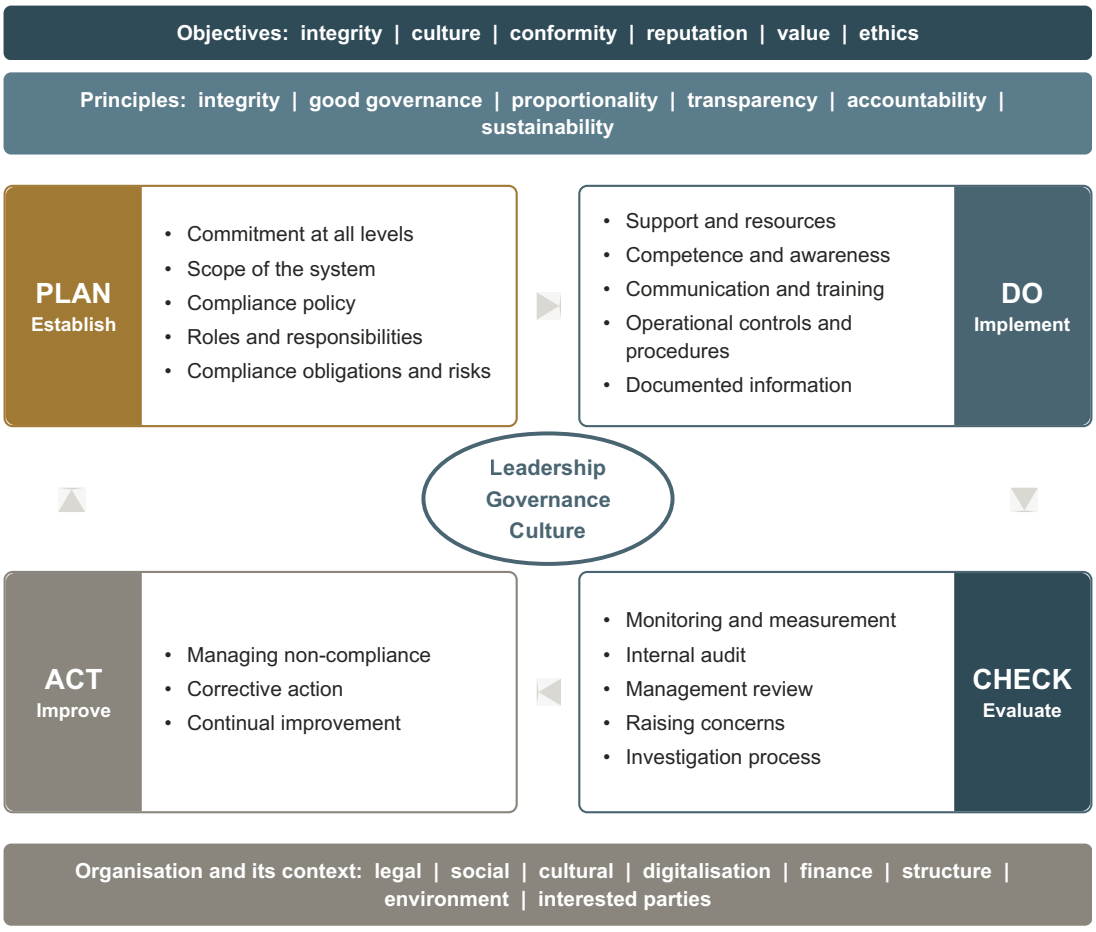
COMPLIANCE

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?*