GOVERNANCE, COMPLIANCE & RISK

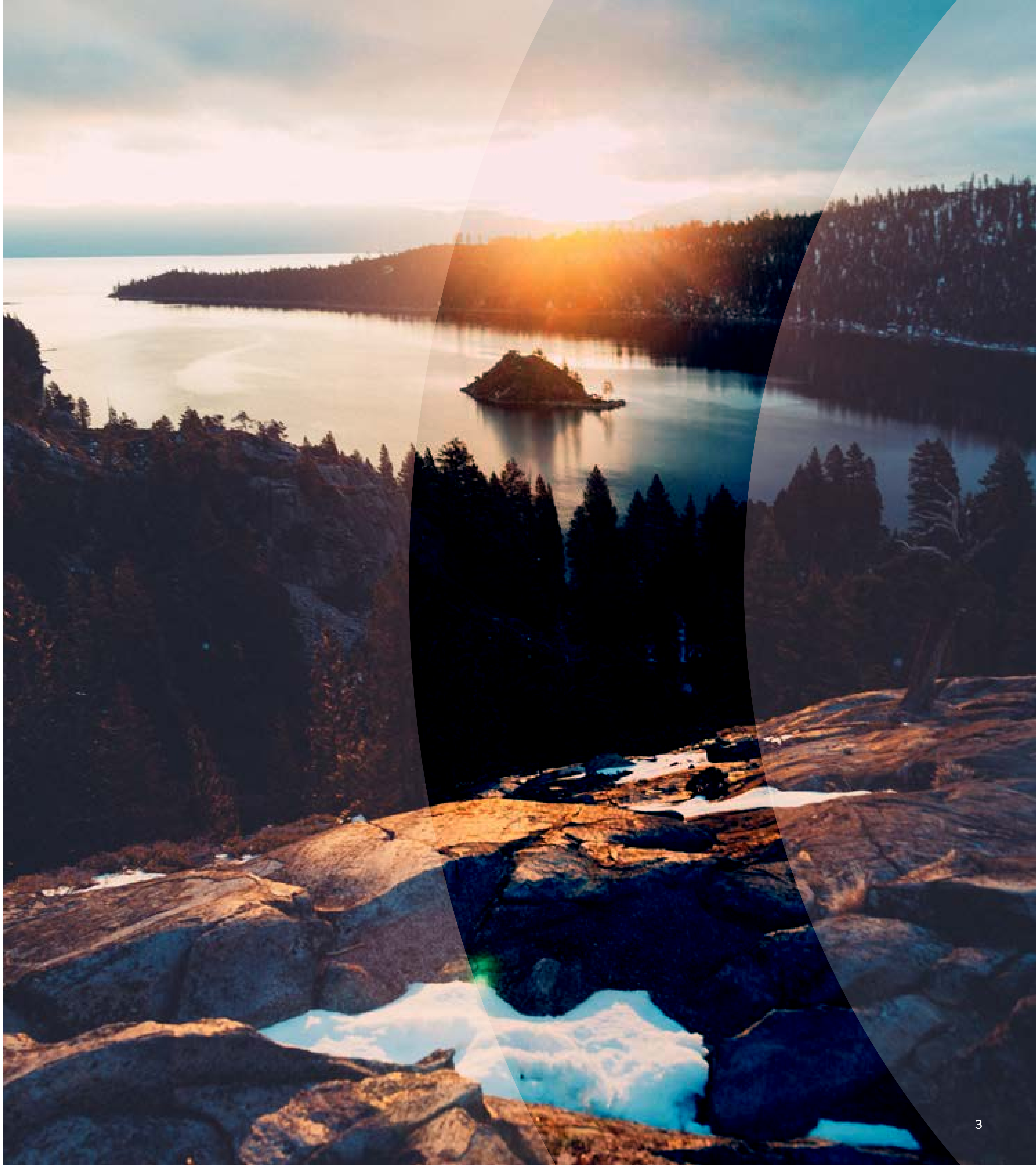
A How-To Guide From The Legal Director

Governance

Good governance is important for businesses of all sizes in all sectors. Not only are stakeholders increasingly demanding evidence of good corporate management, but poor governance and deficiencies in business controls can cause major issues and expose an organisation to significant risk.

Corporate governance supports growth delivery, helps maintain an effective management framework and engenders trust. A well-managed business increases your standing with all your stakeholders and potential investors, partners, and customers. It also improves your ability to bring in outside expertise, retain your best employees, attract funding, and ensure long-term sustainability.

In this guide, we will give you some pointers about what to focus on when establishing good governance and share some of the traits of a well-governed business. If you have any questions or would like our help in establishing best practice in your business, please contact us on 020 3053 8613 or info@thelegaldirector.co.uk.



Knowing and Understanding Your Business

Though you will undoubtedly be doing much that constitutes good governance already, as a starting point, we would recommend that all companies think carefully and systematically about the position overall, especially in the context of the purpose and aims of their business. Most companies, if they challenge themselves, will find areas that can be improved as well as areas of strength. This knowledge, based on honest assessment, provides the foundations upon which good governance is built.

Key to this is having:

- A clearly defined business purpose
- A business strategy
- A plan to deliver on the strategy
- A framework of processes that support these.

Advice: If you're looking at creating good governance in your business, The QCA Corporate Governance Guide, is worth consulting. It promotes the interests of smaller and mid-sized quoted companies and, though the guidelines are specifically designed for the AIM market, the principles are relevant for private SMEs, particularly those with growth aspirations.

The Board

Corporate governance begins with board level action, and a properly constituted and well-functioning board is essential to manage risk and implement strategy.

Board Structure

Bringing diversity and independence at board level supports robust decision making and helps a business manage risk. For SMEs, there is no 'one size fits all', and careful consideration of the individual circumstances is key in considering board structure. However, strong governance would include the following:

- Your board should be led by a Chair with strong leadership skills. The roles of CEO and Chair should not be combined.
- There should be at least two non-executive directors on the board, and with larger boards, 50% of the board should be made up of independent, non-executive directors.
- The role of the Company Secretary is to assist the Chair and have responsibility for the efficient administration and smooth functioning of the board and for ensuring that the board's decisions are implemented. The Company Secretary is often referred to as the 'conscience of the company' acting with a degree of independence as a trusted advisor to the board. For those reasons, ideally your Company Secretary should not be a director.
- A well-functioning board will have a good balance of skills and experience.

In smaller or family-run organisations, fulfilling all these criteria can be more challenging, so it is particularly important to focus on governance principles when directing the business.

The Role and Responsibilities of the Board

An effective board knows what its role is and comprises individual directors who understand their particular and collective responsibilities, all of which are led by the Chair. The roles and responsibilities of the board should be captured in a written document. It is almost inevitable that the process of writing down the finer detail of what a group of people think they know will reveal areas where there is not perfect agreement or understanding in practice.

> "A schedule detailing 'Matters Reserved for the Board' is also imperative. Management then understands when they need to gain the board's approval, and what is otherwise delegated to them."

The purpose of the board is to:

- Determine what the company's strategic goals are and plan how to implement them.
- Communicate responsibilities effectively.
- Take decisions, with each director acting in accordance with their statutory duties, including to promote the success of the company for the benefit of members as a whole, taking into account broader stakeholder interests.
- Engage with stakeholders.
- Define and promote an ethical corporate culture.
- Manage risk.

Ongoing Review

Businesses constantly evolve and the board must embed evaluation and review into its activities.
To support this:

- Carry out regular (ideally at least annual) board reviews. This gives an understanding of how the board and individual directors are performing and affords an opportunity for directors to get things off their chests, iron out niggles and allow progress and growth.
- Question the status quo and evaluate board performance against agreed and pertinent objectives.
- Leverage input from non-executive directors and other key stakeholders – their insight into your operations could be invaluable.

- Ensure that individual training and development needs are regularly assessed and addressed.
- Build a plan to address any gaps and keep review and reporting on this as an agenda item for discussion by the board.

Tip: To allow for proper discussion and effective decision-making, ensure that the board is kept informed and is given salient information in a concise and timely manner ahead of meetings and sufficient time is allocated to discussion at the meeting. Simple practical improvements can often be found that make board meetings more effective and efficient and focus precious time on the right activities.

Engage with Stakeholders

Your stakeholders include shareholders, employees, customers and suppliers. Consider how you communicate your values, plans and news with these groups and what responsibilities you have towards them.

The board is committed to providing long-term value for shareholders. To this end, seek to understand (and if necessary, manage) their expectations and requirements.

Environmental, Social and Governance ("ESG")

We are seeing increasing focus on the wider ethical credentials of businesses and the ESG agenda is gathering momentum. A business's stance on environmental and social issues impacts its reputation and relations with customers, investors, shareholders, suppliers and employees. It is important to get this right. Please do get in touch with us if you would like some advice on this.

Risk Management

A fundamental part of good governance is understanding what the key risks are for your business, and how these risks can be mitigated.

This should be a proactive, not a reactive process. It is far better to be aware of the true position of the business and be comfortable with (and prepared for) your level of risk, than to attempt to deal with an unexpected problem after a potential issue has been exposed.

You need to be able to answer these questions:

- What are the risks to our business?
- What risks are we prepared to accept?
- Why are we prepared to accept those risks?
- How can we have confidence, and demonstrate that, we are mitigating risk in the business?
- Who takes which responsibilities for managing risk: strategically, and day-to-day?
- What is the likely impact if a risk materialises?
- What is the process to follow if a risk materialises?

A written Risk Register and regular risk reviews are essential, and risk management should be an integral part of agendas for board meetings.

In appropriate cases, a dedicated committee of the board will be required to deal with risk, and related committee arrangements will need to be put in place accordingly (e.g., terms of reference, and mechanisms for engaging with the board over the activities of the committee and outcomes of its work).

Demonstrating Good Governance

It is increasingly necessary to evidence good governance. Your governance structures and processes need to be fit for purpose, and your documentation needs to be well-maintained, up-to-date, and transparent.

Not only does this engender confidence and trust internally and externally, it also aligns and empowers good decision-making at all levels of the organisation.

Compliance

The increase in regulation and legislation targeting corporate governance and corporate behaviour makes it more important than ever to develop and maintain a robust compliance programme.

Though the focus and the regulations that govern your business will vary depending on your operations and industry sector, the framework to determine and implement the necessary measures to ensure your compliance are highly transferable across different sectors and industries.

In this guide, we will demonstrate a process that can be adopted to help you to gain useful insight into the effectiveness of your business's compliance programme, how to assess the risk and how to identify and prioritise potential programme enhancements. We will also give you some insights in effective ways to manage ongoing compliance in the face of a changing regulatory environment and how to schedule regular reviews of your programme, including policies, procedures and training as well as potential implications for your relationships with your clients and vendors.

If you have any questions about compliance in your business, please contact us on 020 3503 8613 or info@thelegaldirector.co.uk. We have a great deal of experience in this area and have developed a 'Compliance Blueprint' service that is designed to give businesses an accurate view of their compliance matters and a clear plan to address any gaps.

Audit and risk assessment

The first step in establishing a practicable compliance programme is to conduct an initial risk assessment and develop a process for updating and maintaining this assessment. This will give you valuable, actionable insights - it will provide an overview of your business's current situation, help you focus on the potential impact of non-compliance and prioritise the most urgent enhancements.

Step one: Decide the scope of your assessment, considering any required risk assessments by any external agencies.

Compliance requirements focus on the external rules and the internal controls that govern how a business should operate, and they affect every area of your business. You may decide to concentrate on a particular area or areas in your assessment. Broadly speaking, they fall under:

- Corporate Governance & Oversight – Regardless of the extent of your compliance obligations it is essential you have a well-developed and documented programme demonstrating effective accountability and management oversight.
- Regulatory compliance – this refers to the legislation and regulations set down by external regulators like government agencies or industry bodies, that are relevant to your business and its operations. These requirements extend to all industries and includes areas such as bribery and corruption, modern slavery as well as economic sanctions, money laundering or any other trading rules that may apply specifically to you.
- Financial compliance – these regulations impact all businesses, not just financial services companies and include rules relating to preparation of accounts and tax compliance. In most instances professional accounting and tax advice will be necessary.
- HR compliance – this affects any policies, procedures or contracts that relate to your employees and are regulated by employment law.
- IT compliance – there is strict regulation governing how you handle data privacy and data protection and how your IT is managed.
- Health & Safety compliance –These are the rules and regulations that govern health & safety in the workplace. In many cases this can be considered a subset of either regulatory compliance or HR compliance and may be addressed under either of these areas. For certain businesses who have specific health and safety exposure, such as those operating in heavy industry, it should be considered independently.

Step two: Assess inherent exposure to risk for your business without any controls.

This is intended to assess the risk driven purely by the nature of your business, the markets you operate in, the rules and regulations that apply, and the clients/suppliers you engage with. How likely is a violation of any applicable legislation in the normal course of your business operations with no controls in place, and if a violation does occur how severe will the impact on your business be?

To calculate this, you need to assess the potential frequency of any violation and the severity of any violations should they occur. In determining this you will need to determine a scale of likelihood or frequency that is relevant to your business that can be consistently applied.

Once the likelihood and severity of any potential violation has been worked out, you can create a matrix that will give you the inherent risk.

		Frequency		
		Common	Uncommon	Rare
Severity	High	High	High	Medium
	Medium	High	Medium	Low
	Low	Medium	Low	Low

Step three: Assess the strength of the controls currently deployed.

It's important that this assessment uses objective data to determine the effectiveness of your controls. So, you will need to use a consistent scoring system for each control element or issue that can be identified. This will also provide a roadmap for identifying opportunities for enhancement should management feel the level of residual risk is undesirable.

Your control assessment may consider, amongst other elements, how comprehensive and up to date your documented policies and procedures are, what training is in place and documented violations.

Once you've assessed each control and obtained a score, convert this into a control strength rating of high, medium or low.

Tip: Consider engaging an inhouse lawyer with compliance expertise to help you devise a workable scoring system and assess your current controls. Understanding the current status of your compliance is key to developing a sound compliance programme.

Step four: Using inherent risk and assessment of control strength, determine the residual risk to the business.

Calculating your residual risk allows you to assess the risk your company is ultimately exposed to, given the nature of your business and the controls you have employed. You work this out by cross referencing the Inherent Risk to the Control Strength using the table below.

		Control Strength		
		Low	Medium	High
Inherent Risk	High	High	High	Medium
	Medium	High	Medium	Low
	Low	Medium	Low	Low

Collate and report findings

Whoever undertakes the assessment must report their findings to management.

Management will then consider:

- Are the areas covered by the risk assessment sufficient or are there any elements of the business that have not been assessed that have the potential to violate applicable regulations?
- Is the process that has been employed to assess the risks robust and comprehensive?
- Do the risks fall within risk tolerances that are acceptable to them?

Based on these considerations, management will decide if any programme enhancements are necessary. It is important that these conclusions and determinations are recorded in writing and kept in accordance with the record retention requirements.

Implement improvements

Develop a plan to enhance your compliance programme based on the opportunities identified in the assessment. Ensure you have identified accountable parties for each component of your compliance programme, that you have appropriately robust controls in place and can demonstrate and record the effective operation of each element of the programme.

This risk assessment workflow is an ongoing process. So, you need to schedule in reviews at appropriate times.

Establish a policy management framework

To support regular review and a consistent approach to ongoing compliance matters, you should develop and maintain a policy management framework.

This should set down a standard and principles for policy development, approval, implementation and review across your business. Include information about the process for assigning a senior manager with ownership of the policy, preparing or updating policy documents, engaging in stakeholder consultation and ensuring appropriate oversight and approval.

Evidently, when you have created this, you must make sure that everyone within your organisation is aware of it and understands their responsibilities.

How we can help

In this guide, we have given an overview of the steps to take to develop a robust compliance programme. We're aware, however, that the process is time consuming and complex.

We have developed a 'Compliance Blueprint' product, which puts one of our Client Legal Directors in your business to review your current compliance programme. They will work with you to develop a bespoke risk matrix that is tailored to your business and then conduct an independent review of your current programme assessing it against that matrix. You will then receive a written report comprising a summary matrix assessing the effectiveness of each element of your compliance programme covered by the review against your own risk matrix with recommendations for potential enhancements to your compliance programme. We can produce this as a discrete piece of work or alongside our customary part-time in-house legal service. We can also work with you to prepare and implement any compliance enhancements that are identified in our report.

Our Client Legal Directors are all senior lawyers with a great deal of experience in establishing compliance programmes and processes that allow businesses to operate with confidence. They are adept at prioritising the most important issues and are aware of any changes in regulations or legislation that will impact your business. They can also take ownership of your documentation, scheduling in reviews of policies and procedures.


TLD
The
Legal
Director®