Risk control

Time for a check up?

Risk Management Partners
rmpartners.co.uk

25 YEARS OF DEDICATION IN ACTION

Time for a check up?

Background

In the last two decades of the previous millennium there was a series of high profile corporate failures and disasters which resulted in profound adverse effects being visited upon various stakeholder groups of the effected organisations including shareholders, employees, industries, communities and in some instances, the wider economy. These events included large scale corporate financial failures, major safety and environmental disasters, prolonged interruptions to business continuity and serious damage to organisational reputations. The emergence of risk management as the formal business discipline we know today is considered by many to be a direct consequence of these events as their occurrence emphasised a real need for a more holistic and effective approach to the subject.

Due to the profound nature of these particular events and the sometimes dire consequences, questions were raised about existing standards of corporate governance and its role in risk prevention and mitigation. Questioning focused upon, among other things, the roles and responsibilities and compositions of boards of directors, how risks were being identified, assessed and controlled, the transparency and validity of information and how information was reported to various stakeholder groups.

Various codes of corporate governance were developed, some of which were mandated by regulatory requirements or listings rules of the major stock exchanges. A commonality shared among these codes was the recognition of the importance placed on organisations to maintain robust systems of internal control as part of an approach to more effective organisational governance.

Corporate Governance and Internal Control in the 21st Century

An example of the modern approach to corporate governance and internal control is that presented within the 'Delivering Good Governance in Local Government' framework published by the Chartered Institute of Public Finance and Accountancy and the Society of Local Authority Chief Executives in 2016 (ref. 1). This framework recognises that governing bodies need to ensure that their organisations have implemented robust and effective performance management systems that facilitate the effective and efficient delivery of services.

Furthermore, it recognises that due to the internal and external pressures placed upon organisations, risk management and internal control are integral to an effective performance management system, and are crucial to the achievement of an organisation's objectives and development of a risk aware, not risk adverse, culture.

Basing the foundations of effective corporate governance on integrity, strong ethical values, the respect for the rule of law, openness, and comprehensive stakeholder engagement, the framework identifies 'managing risks and performance through robust internal control and strong public financial management' as one of five essential practices to achieving good organisational governance standards.

Furthermore, it acknowledges that good governance can only be achieved if risk management is embedded into organisational culture and becomes an integral part of activities. Recommendations given to achieve effective internal control within a good governance framework include factors such as:

— Adoption and implementation of a risk management framework and strategy

— Integration of risk management into all aspects of the organisation

— Undertaking regular risk and control reviews

— Engaging employees in the risk management process

— Monitoring and reviewing the risk management framework

Who is Responsible?

The Three Lines of Defence model presented within 'Governance of risk: Three lines of defence' as published by the Chartered Institute of Internal Auditors in 2015 (ref. 2) clarifies the essential roles and duties required for effective internal control.

In the model presented, the three components of the three lines of defence are:

First line of defence

Management and ownership: Operational managers maintain direct ownership, responsibility and accountability for risk assessment and control.

Second line of defence

Oversight: These are internal governance activities which differ in nature from one organisation to another, but typically include compliance, risk management, finance, quality, IT and other functions. This line of defence facilitates and supports the implementation of effective risk management practices by operational management.

Performance monitoring is also a vital component of the second line of defence as well as assisting operational management in the reporting of information to key stakeholder groups.

The principal functions of risk management depicted within the three lines of defence model maintain distinct similarities to those portrayed within modern codes of corporate governance (see above), however, it also includes additional activities such as the identification and reporting of:

— Emerging issues

— Movement in the organisation's implicit risk appetite

— Changing risk and regulatory scenarios

Third line of defence

Assurance: The organisation's senior management team need to receive regular information and assurances on the performance of the organisation. This requirement includes receiving reports on the overall performance of the risk management systems. Using a risk-based approach, an independent internal audit function should be able to provide the necessary assurance to senior management teams.

Other agencies

Other agencies, such as external auditors and regulators should also be regarded as stakeholders within the context of the three lines of defence as they exert certain influences on the overall internal control strategies in place and /or require risk and performance information to be reported directly to them.

The Recent Past

We are all painfully aware of the continuing times of austerity and the funding pressures that many organisations are facing. Increasing organisational risk appetites is a natural consequence of these pressures, as organisations are seeking to innovate and create new delivery models in order to satisfy stakeholder requirements while making the necessary financial adjustments. Shared services, strategic partnerships, outsourcing and collaborative working arrangements are just some examples of the risks which are being taken. Additional evidence of increasing risk appetite comes in the form of cuts or reductions to services and the reduction in human resources. The loss of human resources can result in the loss of organisational knowledge and expertise which can then adversely affect the quality, efficiency and effectiveness of service delivery.

Recent history confirms to us that the risks which organisations are facing today stretch well beyond that of austerity. Devastating human tragedies, significant cyber security breaches, financial failures, extreme weather events, terrorist incidents, and the uncertainty created by the UK's impending exit from the European Union serve to illustrate the diversity and magnitude of risk which organisations need to manage robustly.

These events, as well as others, also serve to remind us of the importance and value of effective internal control and risk management systems in both a preventative capacity and to mitigate the unwanted consequences. In addition to prevention and mitigation, the purpose of risk management is to maximise value and ultimately assist an organisation in achieving outcomes and objectives. Risk-taking is an essential component of modern organisational existence as it allows organisations to improve performance and evolve to meet the ever changing needs of stakeholders. However, risk-taking must be undertaken using approved and fully informed decision-making protocols and correspond directly with the expressed risk appetite of the relevant organisation.

A Risk Management Health Check

In order to assist organisations in gaining assurance in their risk management frameworks and systems, RMP has developed a Risk Management Health Check. It is a multi-level assessment of the degree of maturity and effectiveness of an organisation's risk management standards and is designed to provide a third-party perspective on the strengths of current standards and identify opportunities for potential improvement where they may exist.

Using accepted best practice standards, the health check focuses upon key issues such as:

— Leadership and management (including risk appetite);

— Strategy and policy;

— People;

— Partnerships, shared risks and resources;

— Processes;

— Risk handling and assurance; and

— Outcomes and delivery.

It is constructed using a series of pre-determined question-sets.

Comprehensive stakeholder engagement is essential to the success of the health check process. As well as a series of one-to-one interviews, a wider engagement with the organisation's management hierarchy can be achieved through the use of an online risk management survey which is based upon the same risk management best practice standards featured within the one-to-one interviews.

A desk-top review of relevant strategies, policies and protocols can often inform directly on the health check process.

On completion of the one-to-one interviews and optional online survey process, a structured report will be formulated which will present the outcomes of the health check process, seeking to identify the strengths of the organisation's current risk management approach and any potential opportunities for improvement.

Conclusion

It is a recommendation of modern codes of corporate governance that organisations regularly monitor and review their risk management frameworks and systems to ensure performance is optimised.

Organisations evolve, risks change in character and in value, and control measures fail. The prevalent risk that existing frameworks and systems can fall into disrepair over time, resulting in a failure to detect changes in risk and control dynamics and a loss of efficiency and effectiveness, including agility, in management and control standards.

Left untreated, degrading risk management frameworks and systems can lead organisations to be facing far greater levels of risk than they acknowledge, with false representations of reality and misleading information on controls assurance being reported to key stakeholders including the senior management teams and other stakeholders. In these circumstances, the organisation is not fully prepared for what may happen, and are open to surprises and the adverse consequences than can follow.

References

1 'Delivering Good Governance in Local Government', the Chartered Institute of Public Finance and Accountancy and the Society of Local Authority Chief Executives (2016).

2 'Governance of Risk: Three lines of defence', the Chartered Institute of Internal Auditors (2015)

Further information

For access to further RMP Resources you may find helpful in reducing your organisation's cost of risk, please access the RMP Resources or RMP Articles pages on our website. To join the debate follow us on our LinkedIn page.

Get in touch

For more information, please contact your RMP risk control consultant or account director.

contact@rmpartners.co.uk

rmp

Risk Management Partners

The Walbrook Building
25 Walbrook
London EC4N 8AW

020 7204 1800
rmpartners.co.uk