


**rmp**

## **Risk control**

Time for a check-up?



In partnership with

  
**GALLAGHER  
BASSETT**  
GUIDE. GUARD. GO BEYOND.

# 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 significant 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 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, at least in part, a direct consequence of these events as their occurrence emphasised a real need for a more holistic and effective approach to the task.

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, and the transparency and validity of risk information and how it was being reported, or not 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 21<sup>st</sup> 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<sup>1</sup>. 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, becoming an integral part of everyday 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 Model published by The Chartered Institute of Internal Auditors<sup>2</sup> (2020) clarifies the essential roles required for effective internal control.

In the model presented, the key roles are clearly defined:

### The Governing Body

The governing body should accept accountability for oversight of the organisation, and engage with its stakeholders to monitor their interests and communicate transparently on the achievement of objectives.

It should also:

- Create a culture which promotes ethical behaviour and accountability
- Establish organisational structures and processes for effective governance
- Delegate responsibility as appropriate and provide resources to management to achieve organisational objectives

- Set the organisational appetite for risk and exercise oversight of risk management
- Maintain effective oversight of compliance (legal, regulatory, and ethical)
- Establish and oversee an independent, objective, and competent internal audit function

### Management

Management roles can be split into first line and second line functions.

#### First Line

- Direct actions and use resources to achieve organisational objectives
- Maintain continuous dialogue and report performance in respect of achieving organisational objectives
- Establish and maintain effective structures and processes for the management of operations and risk
- Ensure compliance (legal, regulatory, and ethical)

#### Second Line

- Provide complementary expertise, support, monitoring, and challenge related to the management of risk
- Provide analysis and reports on the effectiveness of risk management

### Internal Audit

The Internal Audit function should maintain primary accountability to the governing body and independence from the responsibilities of management.

Its primary role is to:

- Communicate independent and objective assurance and advice to management and the governing body on the adequacy and effectiveness of governance and risk management

### External Assurance Providers

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

They can provide assurance to:

- Satisfy legislative and regulatory expectations
- Satisfy requests by management and the governing body to complement internal sources of assurance

## The Recent Past

The risks which organisations are exposed to today stretch well beyond that of reduced funding. Of course, funding is a significant issue in its own right. However, devastating human tragedies, significant cyber security breaches, financial failures, extreme weather events, terrorist incidents, pandemics, supply scarcity, and significant increases in the cost of doing business serve to illustrate the diversity of risks which organisations need to manage robustly.

These events 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 any unwanted consequences. In addition to prevention and mitigation, the purpose of risk management is to maximise value and ultimately assist an organisation in achieving 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 defined risk appetite of the organisation.

## A Risk Management Health Check

In order to assist organisations in gaining assurance in their risk management approach, 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
- Outcomes and delivery

It has been 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 produced 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 value, and control measures can degrade and fail. Organisational 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, failing risk management frameworks and systems can lead organisations to face far greater levels of risk than they acknowledge, with false representations of reality and misleading information on controls assurance being reported to key stakeholder groups including senior management teams. In these circumstances, the organisation is not fully prepared for what may happen, and are open to surprises and the adverse consequences that may 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 'The IIA's Three Lines Model', the Chartered Institute of Internal Auditors (2020)

## 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 broker, RMP risk control consultant or account director.

[contact@rmpartners.co.uk](mailto:contact@rmpartners.co.uk)



### **Risk Management Partners**

The Walbrook Building  
25 Walbrook  
London EC4N 8AW

020 7204 1800  
[rmpartners.co.uk](http://rmpartners.co.uk)

This newsletter does not purport to be comprehensive or to give legal advice. While every effort has been made to ensure accuracy, Risk Management Partners cannot be held liable for any errors, omissions or inaccuracies contained within the document. Readers should not act upon (or refrain from acting upon) information in this document without first taking further specialist or professional advice.

Risk Management Partners Limited is authorised and regulated by the Financial Conduct Authority. Registered office: The Walbrook Building, 25 Walbrook, London EC4N 8AW. Registered in England and Wales. Company no. 2989025.