Management of Risk (M_o_R®) – The Facts

Author

This paper has been written by Graham Williams who is a Lead Assessor for the APM Group Limited (APMG). In addition to his role with the APMG, Graham is also an MSP and PRINCE2 Approved Trainer and a Programme and Project Management, MSP, M_o_R and PRINCE2 Registered Consultant. He was also one of the authors of the 2007 edition of the M_o_R guide.

Synopsis

This paper sets out to explain the UK Government owned risk management guidance Management of Risk: Guidance for Practitioners (M_o_R). It describes the key principles underlying the guidance, the M_o_R Approach, the M_o_R Processes and embedding and reviewing M_o_R. Finally, it describes the benefits of adopting the guidance.

Introduction

The purpose of this paper is to provide a high-level introduction to Management of Risk (M_o_R).

M_o_R is applicable to both the public and private sectors, providing an accessible framework for taking informed decision on managing risk throughout the organisation, from designing policy and strategy to delivering change, and dealing with threats and opportunities in day-to-day operations and service.

The paper focuses on providing the facts about M_o_R to enable the reader to appreciate:

- Why M_o_R should be used to help organisations manage their risks
- Who needs to be involved in risk management
- What M_o_R is and what it consists of
- The benefits of its application

In producing this paper, the author has been particularly careful to keep to the fundamentals of M_o_R and has therefore extracted much of the text directly from the M_o_R guide.

The Name

Management of Risk is commonly referred to as “M_o_R”. M_o_R is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries.

The M_o_R guide is intended to help organisations put in place an effective framework for taking informed decisions about the risks that affect their performance objectives across all organisational activities, whether these be strategic, programme, project or operational. M_o_R defines risk as “an uncertain event or set of events which, should it occur, will have an effect on the achievement of objectives. A risk consists of a combination of the probability of a perceived threat or opportunity occurring and the magnitude of its impact on objectives”. With this definition ‘threat’ is used to describe an uncertain event that could have a negative impact on objectives or benefits; and ‘opportunity’ is used to describe an uncertain event that could have a favourable impact on objectives or benefits.

The Origins

The first edition of this guide was published in 2002 in response to the Turnbull Report to provide a generic framework for risk management across all parts of an organisation. The second edition, published in 2007, was produced to reflect the further developments in the world of risk management such as:

- In the UK public sector HM Treasury had revised its Orange Book which outlines the principles and concepts of risk management
- In the private sector change had been instigated by new regulatory environments such as the Combined Code on Corporate Governance 2006 (UK), Basel II Accord 2004 (Europe), and Sarbanes-Oxley 2002 (US).

The Reasons for adopting M_o_R

A major factor influencing the drive towards more formalised approaches to risk management has been the increased focus given to corporate governance in both the UK and the US following high-profile collapses of companies such as Bank of Credit and Commerce International, the Maxwell Communication Corporation plc, and Enron and WorldCom.

Corporate governance can be defined as the ongoing activity of maintaining a sound system of internal control by which the directors and officers of an organisation ensure that effective management systems, including financial monitoring and control systems, have been put in place to protect assets, earnings capacity and the reputation of the organisation. Corporate Governance covers a wide range of topics, including directors’ remuneration, accountability and audit; and relations with shareholders. One aspect of accountability and audit is internal control and one aspect of internal control is risk management.

The Audience for M_o_R

Risk management should be most rigorously applied where critical decisions are being made. Decisions about risk will vary depending on whether the risk relates to long-, medium- or short-term goals.

- **Strategic** decisions are primarily concerned with long-term goals; these set the context for decisions at other levels of the organisation. The risks associated with strategic decisions may not become apparent until well into the future. Thus it is essential to review these decisions and associated risks on a regular basis
- Medium-term goals are usually addressed through **programmes** and **projects** to bring about business change. Decisions relating to medium-term goals are narrower in scope than strategic ones, particularly in terms of timeframe and financial responsibilities
- At the **operational** level the emphasis is on the short-term goals to ensure ongoing continuity of business services; however, decisions about risk at this level must also support the achievement of the long- and medium-term goals.

Those involved in risk management will depend on the organisational perspective under question:

Strategic Perspective
Those with key responsibilities for risk management from this perspective will be the Management Board, The Accounting Officer (public sector) or CEO (private sector), the Executive Management Team and the Head(s) of the Audit and/or Risk Committees.

The likely risk management stakeholders include the owners/shareholder, investors/ funders, key customers, political, legal or regulatory bodies, the wider community within which the organisation exists, strategic partners/supplier and the organisation's employees.

Programme Perspective
Those with key responsibilities for risk management from this perspective will be the Sponsoring Group, Programme Board, Senior Responsible Owner (SRO), Programme Manager and Business Change Managers (BCMs).

The likely risk management stakeholders include in the owners/shareholders who are sponsoring the programme, customers/consumers affected by the programme, internal and/or external audit, security, trade unions, political or regulatory bodies, the wider community affected by the programme and members of the programme management team and project management teams.

Project Perspective
Those with key responsibilities for risk management from this perspective will be the Project Board, Project Sponsor (or SRO or Executive), and Project Manager.

The likely risk management stakeholders include the internal/external suppliers, customers/recipients of the project deliverables, political or regulatory bodies, project sponsors, team managers and members.

Operational Perspective
Those with key responsibilities for risk management from this perspective will be the Executive Management Team, Operational Directors / Heads of Operations, and Operational Managers.

The likely risk management stakeholders include the owners/shareholders, customers/consumers affected by the service or products delivered, counterparties, business partners/suppliers, other departments, internal and/or external audit, compliance, security, health and safety, business continuity, trade unions, political or regulatory bodies, the wider community and any programme/project management teams delivering change into the operation.

The M_o_R Framework
The M_o_R framework is based on four core concepts of:

- **M_o_R Principles.** These are essential for the development of good risk management practice. They are all derived from corporate governance principles in the recognition that risk management is a subset of an organisation's internal controls.
- **M_o_R Approach.** The principles need to be adapted and adopted to suit each individual organisation. Accordingly, an organisation's approach to the principles needs to be agreed and defined within a Risk Management Policy, Process Guide and Strategies, and supported by the use of Risk Registers and Issue Logs.
- **M_o_R Processes.** There are four main process steps, which describe the inputs, outputs and activities involved in ensuring that risks are identified, assessed and controlled.
- **Embedding and Reviewing M_o_R.** Having put in place the principles, approach and processes, an organisation needs to ensure that they are consistently applied across the organisation and that their application undergoes continual improvement in order for them to be effective.

M_o_R is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries.

Principles

M_o_R principles are not intended to be prescriptive but provide supportive guidance to enable organisations to develop their own polices, processes, strategies and plan to meet their specific needs. They are evolutionary in nature in that the way they are applied may need to change over time to reflect changes in circumstances.

The twelve principles are:

Principle:	**Description:**
Organisational context	The starting point for risk management is to understand the context of the organisation or activity under examination and hence avoid blind spots. Context includes the political, economic, social, technological, legal and environmental backdrop.
Stakeholder involvement	Risk management should engage with all primary stakeholders to ensure that the objectives of the organisation or activity under examination are established and agreed.
Organisational objectives	As the purpose of risk management is to strive to understand and manage the threats and opportunities arising from the objectives of the organisation or activity, risk management can only commence when it is clear what these objectives are.
M_o_R approach	Organisations should develop an approach to the management of risk that reflects their unique objectives. It is common for organisations to describe their approach through their policies, processes, strategies and plans.
Reporting	The governing body of the organisation should receive, review and act on risk management reports. As a result, a fundamental aspect of risk management is the timely communication of risk information to the management team to enable it to make informed decisions.
Roles and responsibilities	Organisations should establish clear roles and responsibilities for the management of risk in terms of leadership, direction, control, ongoing risk management, reporting and reviewing.
Support structure	A risk management team is required to ensure that the policies are adhered to, the process is followed, appropriate techniques are adopted, reports are issued to meet senor management and board requirements, the regulators' guidelines are adhered to and best practice is followed – all at the appropriate time.
Early warning indicators	Organisations should establish early warning indicators for critical business activities to provide information on the potential sources of risk. These will enable risk management to be proactive and to anticipate potential problems.
Review cycle	As with an organisation's objectives, its internal organisation and environment within which it operates are continually evolving. A sound and effective risk process is contingent on regular reviews of the risks faced and the policies, processes and strategies it is adopting to manage them.
Overcoming barriers to M_o_R	There needs to be recognition that even though an organisation has risk management policies, processes and strategies in place, this will not automatically lead to robust, effective and efficient risk management practices. There are a number of barriers to the implementation of risk management that need to be addressed.
Supportive culture	Organisations should establish the right culture to support management of risk throughout the organisation. A supportive culture will be one that embeds risk management into day-to-day operations and recognises the benefits of risk management.
Continual improvement	Organisations that are interested in continual improvement should develop strategies to improve their risk maturity to enable them to plan and implement step changes in their risk management practices.

Management of Risk Approach

The way in which the M_o_R principles are implemented will vary from organisation to organisation. Collectively they provide a base on which the organisation's risk practices can be developed. These practices describe how risk management will be undertaken throughout the organisation, i.e. the M_o_R approach.

To capture and communicate these practices it is common to create a series of living documents called:

- Risk Management Policy
- Risk Management Process Guide
- Risk Management Strategies
- Risk Register
- Issue Log

Risk Management Policy
The purpose of the Risk Management Policy is to communicate how risk management will be implemented throughout an organisation to support the realisation of its strategic objectives. The policy communicates why risk management should be undertaken and how it relates to the corporate objectives, and it provides a common language. It strives to accomplish uniformity across risk management processes; it aims to remove ambiguity about the organisation's risk appetite and when to escalate risk, and describes the format, timing and content of reports.

Risk Management Process Guide
The purpose of the Risk Management Process Guide is to describe the series of steps and the respective associated activities, necessary to implement risk management. The process should be tailored to the organisation and be suitable for types of activity across the organisation. It should be applicable to all levels of management and activity. This document should describe a best practice approach that will support a consistent method and deliver effective risk management. This guide could be incorporated into the Risk Management Policy.

Risk Management Strategies
The purpose of the Risk Management Strategy is to describe for a particular organisational activity the specific risk management activities that will be undertaken. Strategies are typically prepared for a particular strategic initiative, a programme, a project or an operational area within the organisation. Each strategy should be tailored to each specific activity, while at the same time reflecting the Risk Management Policy and Process Guide.

Risk Register
The purpose of the Risk Register is to capture and maintain information on all of the identified threats and opportunities relating to a specific organisational activity. The precise content of the Risk Register will vary but the layout of the register should reflect the sequence in which the information is captured.

Issue Log
The purpose of the issue Log is to capture and maintain information in a consistent, structured manner on all of the identified issues that have already occurred and require action. These issues may include risks that have materialised and have changed from possible events to actual events. As with the Risk Register the precise content of the Issue Log will vary but the layout of the log should reflect the sequence in which the information is captured.

Management of Risk Processes

This diagram shows the overall risk management process consisting of four steps represented as a circle of arrows as it is common for the entire process to be completed several times in the lifecycle of an organisational activity. The activity 'Communicate' deliberately stands alone as the findings of any individual step may be communicated to management for action prior to completion of the overall process.

'Embed and Review' embraces all of the steps in the process as this activity looks at each individual step in turn to determine its contribution to the overall effectiveness of the complete process. The management of risk principles form the foundation of all risk management activities and permeate all risk management processes.

<<INSERT FIGURE 4.1 FROM M_o_R>>

Identify
This process is divided into two steps:

- **Identify – Context.** The primary purpose of this step is to obtain information about the planned activity. This will include understanding what the activity objectives are, what the scope of the activity is, what assumptions have been made, how complete the information is, who the stakeholders are and what their objectives are, where the activity fits in relation to the organisational structure, the organisation's own environment and the organisation's approach to risk management. The Risk Management Policy and Process Guide are inputs into this step and the Risk Management Strategy is one of the outputs.
- **Identify – Risks.** The primary goal of this step is to identify the risks to the organisation that would reduce or remove the likelihood of the organisation reaching its objectives while maximising the opportunities that could lead to improved performance. This will include identifying the threats and opportunities to the activity, preparing a Risk Register, preparing key performance indicators and understanding the stakeholders' view of risks.

Assess
This process is also divided into two steps:

- **Assess – Estimate.** The primary goal of this step is to assess each of the threats and the opportunities to the organisation in terms of their probability and impact. The risk proximity will also be of interest to gauge how quickly the risk is likely to materialise if no action were taken. The Risk Register is updated with the results of these estimates.

- **Assess – Evaluate.** The primary goal of this step is to understand the net effect of the identified threats and opportunities on an activity when aggregated together. This may include preparing an estimated monetary value calculation which records the weighted average of the anticipated impact, a risk model which aggregates the risks together using a simulation technique or calculating a net present value using an accepted discount rate.

Plan
The primary goal of the plan step is to prepare specific management responses to the threats and opportunities identified, ideally to remove or reduce the threats and to maximise the opportunities. Attention to this step ensures as far as possible that the business and its staff are not taken by surprise if a risk materialises. The Risk Register is updated to include the risk responses.

Implement
The primary goal of this step is to ensure that the planned risk management actions are implemented and monitored as to their effectiveness, and corrective action is taken where responses do not match expectations.

Communicate
Rather than being a distinct step in the process, communication is an activity that is carried out throughout the whole process. Effective communication is key to the identification of new threats and opportunities or changes to existing risks. It is also important for management to engage with and seek the participation of staff and the wider stakeholders population. Communication will play a major role in achieving such engagement and participation.

Embedding and Reviewing Management of Risk

Risk management needs to be integrated into the culture of the organisation. How an organisation manages its risks demonstrates a part of that organisation’s core values and improves stakeholder confidence in the organisation’s ability to cope with and manage its risks. The organisation therefore needs to ensure that risk management has been integrated successfully, has the necessary support, is addressed in an appropriate way and is successful. A key component of the management of risk integration within an organisation is the cultural acceptance and change required to embed management of risk principles and values within the organisation. This can best be achieved through a structured programme of activities that lead to the achievement of risk knowledge, understanding and education within the organisation.

An organisation needs to be able to measure the effectiveness and appropriateness of risk management, including the organisation’s progress in embedding management of risk, and also its ability to develop its management of risk capability and maturity. The latter can be assessed using a maturity model and the appropriateness of risk management can be assessed against the organisation’s risk appetite.

The Benefits

Finally, the main benefit of applying an effective approach to risk management is the likely improvement of the organisation against its objectives by contributing towards:

- Better service delivery
- Reduction in management time spent fire-fighting
- Increased likelihood of change initiatives being achieved
- More focus internally on doing the right things properly
- Better basis for strategy setting
- Achievement of competitive advantage
- Fewer sudden shocks and unwelcome surprises
- More efficient use of resources
- Reduced waste and fraud, and better value for money
- Improved innovation

M_o_R is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries.

- Better management of contingent and maintenance activities