A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000

airmic

alarm
THE PUBLIC
RISK MANAGEMENT
ASSOCIATION

irm

Contents

Executive summary

Introduction

Acknowledgements

Part 1: Risk, risk management and ISO 31000

Part 2: Enterprise risk management

Appendices

List of figures

List of tables

Executive summary

Risk management is an increasingly important business driver and stakeholders have become much more concerned about risk. Risk may be a driver of strategic decisions, it may be a cause of uncertainty in the organisation or it may simply be embedded in the activities of the organisation. An enterprise-wide approach to risk management enables an organisation to consider the potential impact of all types of risks on all processes, activities, stakeholders, products and services. Implementing a comprehensive approach will result in an organisation benefiting from what is often referred to as the 'upside of risk'.

The global financial crisis in 2008 demonstrated the importance of adequate risk management. Since that time, new risk management standards have been published, including the international standard, ISO 31000 'Risk management – Principles and guidelines'. This guide draws together these developments to provide a structured approach to implementing enterprise risk management (ERM).

Intended benefits of risk management

For all types of organisations, there is a need to understand the risks being taken when seeking to achieve objectives and attain the desired level of reward. Organisations need to understand the overall level of risk embedded within their processes and activities. It is important for organisations to recognise and prioritise significant risks and identify the weakest critical controls.

When setting out to improve risk management performance, the expected benefits of the risk management initiative should be established in advance. The outputs from successful risk management include compliance, assurance and enhanced decision-making. These outputs will provide benefits by way of improvements in the efficiency of operations, effectiveness of tactics (change projects) and the efficacy of the strategy of the organisation.

Purpose of this guide

A successful enterprise risk management (ERM) initiative can affect the likelihood and consequences of risks materialising, as well as deliver benefits related to better informed strategic decisions, successful delivery of change and increased operational efficiency. Other benefits include reduced cost of capital, more accurate financial reporting, competitive advantage, improved perception of the organisation, better marketplace presence and, in the case of public service organisations, enhanced political and community support.

This guide provides a brief commentary on ISO 31000 as well as setting out advice on the implementation of an ERM initiative. The purpose of the guide is to:

- describe the principles and processes of risk management
- provide a brief overview of the requirements of ISO 31000
- give practical guidance on designing a suitable framework
- give practical advice on implementing enterprise risk management

Introduction

This guide is the result of work by a team drawn from the main risk management organisations in the UK – the Association of Insurance and Risk Managers (AIRMIC), the public sector risk management association (Alarm) and the Institute of Risk Management (IRM). The guide is intended to be applicable to all types of organisations. Throughout the guide, the word Board is used to signify the decision-making body within an organisation. In the public sector, this body may be referred to as the Council, Executive or Authority.

There are many opinions regarding what risk management involves, how it should be implemented and what it can achieve. International Organisation for Standardisation (ISO) standard 31000 was published in 2009 and seeks to answer these questions. This guide includes a brief commentary on ISO 31000, as well as providing further information on the successful implementation of risk management. Importantly, this guide recognises that risk has both an upside and downside.

Risk management principles

Risk management is a process that is underpinned by a set of principles. Also, it needs to be supported by a structure that is appropriate to the organisation and its external environment or context. A successful risk management initiative should be proportionate to the level of risk in the organisation (as related to the size, nature and complexity of the organisation), aligned with other corporate activities, comprehensive in its scope, embedded into routine activities and dynamic by being responsive to changing circumstances.

This approach will enable a risk management initiative to deliver outputs, including compliance with applicable governance requirements, assurance to stakeholders regarding the management of risk and improved decision-making. The impact or benefits associated with these outputs include more efficient operations, effective tactics and efficacious strategy. These benefits need to be measurable and sustainable. Appendix A provides a checklist of actions that should be completed in order to fully satisfy risk management requirements.

COSO ERM framework and ISO 31000

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) published an Enterprise Risk Management (ERM) standard in 2004. The COSO ERM cube is well known to risk management practitioners and it provides a framework for undertaking ERM. It has gained considerable influence because it is linked to the Sarbanes-Oxley requirements for companies listed in the United States. ISO 31000 was published in 2009 as an internationally agreed standard for the implementation of risk management principles.

This guide provides a structured approach to implementing risk management on an enterprise-wide basis that is compatible with both COSO ERM and ISO 31000. However, the guide places more emphasis on ISO 31000 because it is an international standard and many organisations have international operations. At the same time as publishing ISO 31000, ISO also produced Guide 73 'Risk management – Vocabulary – Guidelines for use in standards'.

Acknowledgements

Permission to reproduce extracts from ISO 31000 'Risk management – Code of practice' is granted by the BSI. British Standards can be obtained in PDF or hard copy formats from the BSI online shop: www.bsigroup.com/shop or by contacting BSI Customer Services for hardcopies only: Tel: +44 (0)20 8996 9001, e-mail: cservices@bsigroup.com

Figure 1, Figure 4, Table 2, Table 3 and Table 4 are reproduced with kind permission of Kogan Page Limited from "Fundamentals of Risk Management" (2010) ISBN 978 0 7494 5942 0 www.koganpage.com

Part 1: Risk, risk management and ISO 31000

Part 1 provides an overview of risk and risk management with particular reference to ISO 31000. The terminology used to describe the steps in the risk management process is not consistent and this part reflects on these difficulties. A summary of the risk management requirements that should be in place in order to ensure good standards of risk governance are presented by way of a checklist in Appendix A.

1. Nature and impact of risk

Risks can impact an organisation in the short, medium and long term. These risks are related to operations, tactics and strategy, respectively. Strategy sets out the long-term aims of the organisation, and the strategic planning horizon for an organisation will typically be 3, 5 or more years. Tactics define how an organisation intends to achieve change. Therefore, tactical risks are typically associated with projects, mergers, acquisitions and product developments. Operations are the routine activities of the organisation.

Definition of risk

There are many definitions of risk and risk management. The definition set out in ISO Guide 73 is that risk is the "effect of uncertainty on objectives". In order to assist with the application of this definition, Guide 73 also states that an effect may be positive, negative or a deviation from the expected, and that risk is often described by an event, a change in circumstances or a consequence.

This definition links risks to objectives. Therefore, this definition of risk can most easily be applied when the objectives of the organisation are comprehensive and fully stated. Even when fully stated, the objectives themselves need to be challenged and the assumptions on which they are based should be tested, as part of the risk management process.

For example, consider the infrastructure of an organisation and the implementation of a new IT system. The choice of hardware and software are strategic decisions. If these choices are incorrect, the consequences will not be obvious for some time. The associated risks are strategic risks and these risks will be taken with the intention of achieving benefits. Correct strategic decisions deliver benefits that result in achievement of the upside of risk.

The project to install the new hardware and software will be a change initiative that represents the tactics by which strategy will be implemented. Risks within the project need to be managed, so that the project is delivered on time, within budget and to specification. Again, it is possible to achieve an upside in the execution of the project, whereby the project is delivered early and below budget. It is also possible that the IT hardware and software will deliver greater benefits than anticipated.

Once the new hardware and software has been installed, the system will be vulnerable to operational risks, including computer breakdown, loss of data, virus attacks and operator errors. These operational risks may be very significant, and correct procedures will need to be designed and implemented to minimise potential disruption.

Recording risk assessments

Risk assessment involves the identification of risks followed by their evaluation or ranking. It is important to have a template for recording appropriate information about each risk. Table 1 shows the range of information that may need to be recorded. The objective of a template is to enable the information to be recorded in a table, risk register, spreadsheet or a computer-based system. Although a simple description of a risk is sometimes sufficient, there are circumstances where a detailed risk description may be required in order to facilitate a comprehensive risk assessment process.

The consequences of a risk materialising may be negative (hazard risks), positive (opportunity risks) or may result in greater uncertainty. Organisations need to establish appropriate definitions for the different levels of likelihood and consequences associated with these different risks. Risk ranking can be quantitative, semi-quantitative or qualitative in terms of the likelihood of occurrence and the possible consequences or impact.

Organisations will need to define their own measures of likelihood of occurrence and consequences.

For example, many organisations find that assessing likelihood and consequences as high, medium or low, with the results presented on a 3 x 3 risk matrix is adequate. Other organisations find that more options are necessary and a 4 x 4 or 5 x 5 risk matrix is required. By considering the likelihood and consequences of each risk, it will be possible to prioritise or rank the key risks for further analysis.

Risk classification systems

An important part of analysing a risk is to determine the nature, source or type of impact of the risk. Evaluation of risks in this way may be enhanced by the use of a risk classification system. Risk classification systems are important because they enable an organisation to identify accumulations of similar risks. A risk classification system will also enable an organisation to identify which strategies, tactics and operations are most vulnerable.

Risk classification systems are usually based on the division of risks into those related to financial control, operational efficiency, reputational exposure and commercial activities. However, there is no risk classification system that is universally applicable to all types of organisations.

Table 1: Detailed risk description

1	Name or title of risk	● Unique identifier or risk index
2	Scope of risk	● Scope of risk and details of possible events, including description of the events, their size, type and number
3	Nature of risk	● Classification of risk, timescale of potential impact and description as hazard, opportunity or uncertainty
4	Stakeholders	● Stakeholders, both internal and external, and their expectations
5	Risk evaluation	● Likelihood and magnitude of event and possible impact or consequences should the risk materialise at current level
6	Loss experience	● Previous incidents and prior loss experience of events related to the risk
7	Risk tolerance, appetite or attitude	● Loss potential and anticipated financial impact of the risk ● Target for control of risk and desired level of performance ● Risk attitude, appetite, tolerance or limits for the risk
8	Risk response, treatment and controls	● Existing control mechanisms and activities ● Level of confidence in existing controls ● Procedures for monitoring and review of risk performance
9	Potential for risk improvement	● Potential for cost-effective risk improvement or modification ● Recommendations and deadlines for implementation ● Responsibility for implementing any improvements
10	Strategy and policy developments	● Responsibility for developing strategy related to the risk ● Responsibility for auditing compliance with controls

This may be especially true for organisations operating in the public sector and those involved in the delivery of services to the public.

There are many risk classification systems available and the one selected will depend on the size, nature and complexity of the organisation. ISO 31000 does not recommend a specific risk classification system and each organisation will need to develop the system most appropriate to the range of risks that it faces.

2: Principles of risk management

Risk management is a central part of the strategic management of any organisation. It is the process whereby organisations methodically address the risks attached to their activities. A successful risk management initiative should be proportionate to the level of risk in the organisation, aligned with other corporate activities, comprehensive in its scope, embedded into routine activities and dynamic by being responsive to changing circumstances.

The focus of risk management is the assessment of significant risks and the implementation of suitable risk responses. The objective is to achieve maximum sustainable value from all the activities of the organisation. Risk management enhances the understanding of the potential upside and downside of the factors that can affect an organisation. It increases the probability of success and reduces both the probability of failure and the level of uncertainty associated with achieving the objectives of the organisation.

Context for risk management

Risk management should be a continuous process that supports the development and implementation of the strategy of an organisation. It should methodically address all the risks associated with all of the activities of the organisation. In all types of undertaking, there is the potential for events that constitute opportunities for benefit (upside), threats to success (downside) or an increased degree of uncertainty.

It is often argued that, for health and safety risks, the consequences can only be negative and the management of safety risk should focus on prevention and mitigation of harm. However, for outsourced service providers, setting good standards of health and safety may be part of winning contracts and this demonstrates that there is an upside to safety risk management.

Risk aware culture

Risk management must be integrated into the culture of the organisation and this will include mandate, leadership and commitment from the Board. It must translate risk strategy into tactical and operational objectives, and assign risk management responsibilities throughout the organisation. It should support accountability, performance measurement and reward, thus promoting operational efficiency at all levels. Achieving a good risk aware culture is ensured by establishing an appropriate risk architecture, strategy and protocols.

In order to successfully implement, support and sustain the risk management process, a structure is required. ISO 31000 refers to this structure as the risk management context.

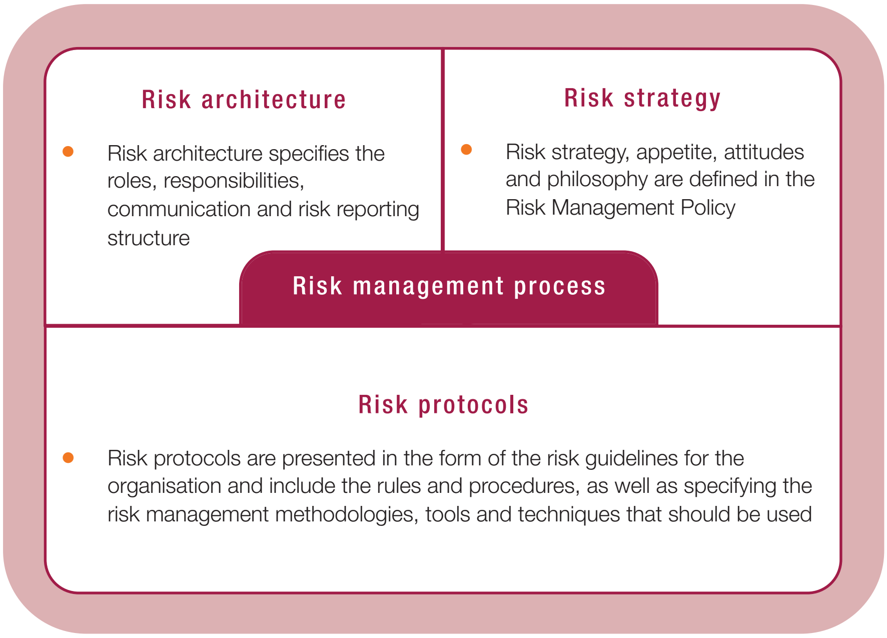
Figure 1 illustrates a suitable structure in terms of the risk architecture, strategy and protocols, and briefly describes the key features of each element. This structure is designed to give context to risk management activities and support the risk management process.

Risk management process

The risk management process can be presented as a list of co-ordinated activities. There are alternative descriptions of this process, but the components listed below are usually present. This list represents the 7Rs and 4Ts of (hazard) risk management:

- recognition or identification of risks
- ranking or evaluation of risks
- responding to significant risks
    - tolerate
    - treat
    - transfer
    - terminate
- resourcing controls
- reaction planning
- reporting and monitoring risk performance
- reviewing the risk management framework

Figure 1: Risk architecture, strategy and protocols


Risk architecture
Risk architecture specifies the roles, responsibilities, communication and risk reporting structure
Risk strategy
Risk strategy, appetite, attitudes and philosophy are defined in the Risk Management Policy
Risk management process
Risk protocols
Risk protocols are presented in the form of the risk guidelines for the organisation and include the rules and procedures, as well as specifying the risk management methodologies, tools and techniques that should be used

Recognition and ranking of risks together form the risk assessment activity. ISO 31000 uses the phrase ‘risk treatment’ to include all of the 4Ts included under the heading ‘risk response’. The scope of risk responses available for hazard risks includes the options of tolerate, treat, transfer or terminate the risk or the activity that gives rise to the risk. For many risks, these responses may be applied in combination. For opportunity risks, the range of available options includes exploiting the risk. Reaction planning includes business continuity planning and disaster recovery planning.

3: Review of ISO 31000

ISO 31000 describes the components of a risk management implementation framework. Figure 2 provides a simplified version of this implementation framework. It includes the essential steps in the implementation and ongoing support of the risk management process. The initial component of the ISO 31000 framework is ‘mandate and commitment’ by the Board and this is followed by:

- design of framework
- implement risk management
- monitor and review framework
- improve framework

Framework for managing risk

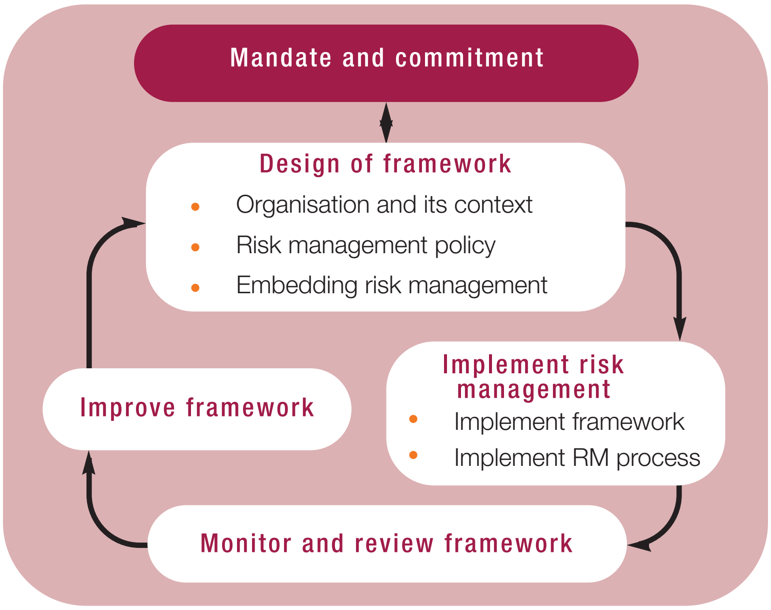
ISO 31000 describes a framework for implementing risk management, rather than a framework for supporting the risk management process. Information on designing the framework that supports the risk management process is not set out in detail in ISO 31000. An organisation will describe its framework for supporting risk management by way of the risk architecture, strategy and protocols for the organisation.

The risk architecture, strategy and protocols shown in Figure 1 represent the internal arrangements for communicating on risk issues. It also sets out the roles and responsibilities of the individuals and committees that support the risk management process. The risk strategy should set out the objectives that risk management activities in the organisation are seeking to achieve. Finally, the risk protocols describe the procedures by which the strategy will be implemented and risks managed.

4: Achieving the benefits of ERM

Figure 3 provides a simplified version of the risk management process from ISO 31000 using the terminology of Guide 73. The key stages in the process are represented as risk assessment and risk treatment. Figure 3 also indicates that the risk management process takes place within the risk management context of the organisation.

Figure 2: Framework for managing risk (based on ISO 31000)



Risk assessment

Risk identification establishes the exposure of the organisation to risk and uncertainty. This requires an intimate knowledge of the organisation, the market in which it operates, the legal, social, political and cultural environment in which it exists, as well as an understanding of strategic and operational objectives. This will include knowledge of the factors critical to success and the threats and opportunities related to the achievement of objectives. It should be approached in a methodical way to ensure that all value-adding activities within the organisation have been evaluated and all the risks flowing from these activities defined.

The result of the risk analysis can be used to produce a risk profile that gives a rating of significance to each risk and provides a tool for prioritising risk treatment efforts. This ranks the relative importance of each identified risk. This process allows the risks to be mapped to the business area affected, describes the primary control mechanisms in place and indicates where the level of investment in controls might be increased, decreased or reapportioned.

The risk analysis activity assists the effective and efficient operation of the organisation by identifying those risks that require attention by management. This will facilitate the ability to prioritise risk control actions in terms of their potential to benefit the organisation. The range of available risk response treatments include tolerate, treat, transfer and terminate. An organisation may decide that there is also a need to improve the control environment.

Risk treatment

Risk treatment is presented in ISO 31000 as the activity of selecting and implementing appropriate control measures to modify the risk. Risk treatment includes as its major element, risk control (or mitigation), but extends further to, for example, risk avoidance, risk transfer and risk financing. Any system of risk treatment should provide efficient and effective internal controls. Effectiveness of internal control is the degree to which the risk will either be eliminated or reduced by the proposed control measures. The cost-effectiveness of internal control relates to the cost of implementing the control compared to the risk reduction benefits achieved.

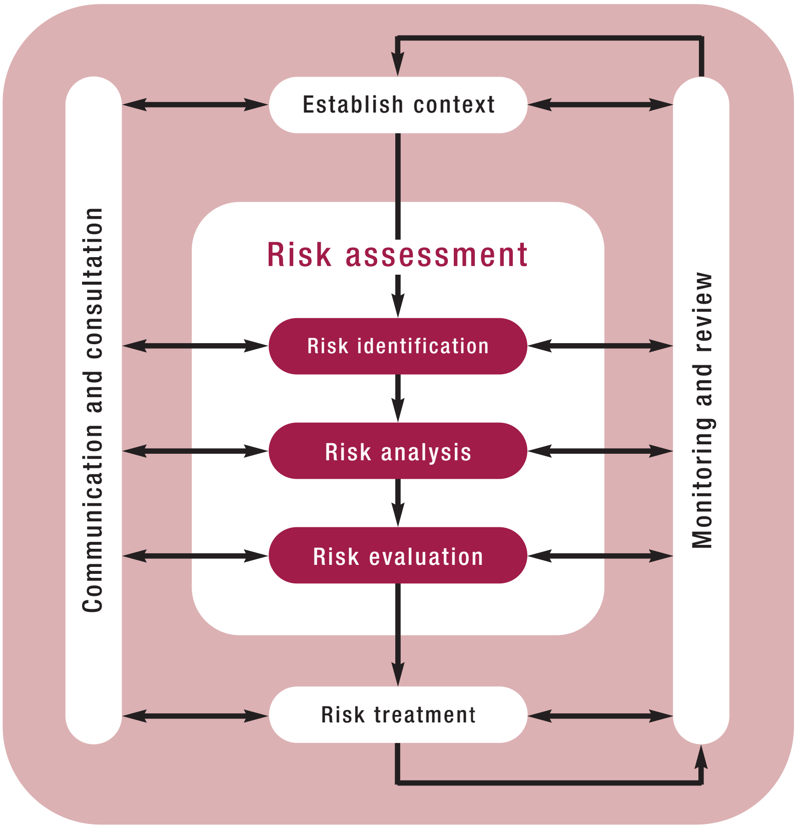
Compliance with laws and regulations is not an option. An organisation must understand the applicable laws and must implement a system of controls that achieves compliance. One method of obtaining financial protection against the impact of risks is through risk financing, including insurance. However, it should be recognised that some losses or elements of a loss may be uninsurable, such as uninsured costs and damage to employee morale and the reputation of the organisation.

Feedback mechanisms

ISO 31000 recognises the importance of feedback by way of two mechanisms. These are monitoring and review of performance and communication and consultation. Monitoring and review ensures that the organisation monitors risk performance and learns from experience. Communication and consultation is presented in ISO 31000 as part of the risk management process, but it may also be considered to be part of the supporting framework.

Reporting and disclosure are only very briefly mentioned in ISO 31000 and they are not included in the process shown in Figure 3. Also, the monitoring and review feedback activities set out in ISO 31000 do not explicitly mention the tasks of monitoring risk performance and reviewing the risk management framework.

Figure 3: Risk management process (based on ISO 31000)



Part 2: Enterprise risk management

Part 2 provides an overview of the steps involved in the implementation of an enterprise risk management (ERM) initiative. The terminology used in this part is based on the 7Rs and 4Ts of (hazard) risk management. A brief description of the steps involved in the implementation of an ERM initiative is provided in Appendix B.

5: Planning and designing

There are a number of factors that should be considered when designing and planning an ERM initiative. Details of the risk architecture, strategy and protocols should be recorded in a risk management policy for the organisation. Table 2 provides information on the contents of a typical risk management policy.

Board mandate and commitment

Many organisations issue an updated version of their risk management policy each year. This ensures that the overall risk management approach is in line with current best practice.
It also gives the organisation the opportunity to focus on the intended benefits for the coming year, identify the risk priorities and ensure that appropriate attention is paid to emerging risks. The policy should also describe the risk architecture of the organisation. Figure 4 illustrates a typical risk architecture of a large listed company.

Mandate and commitment from the Board is critically important and it needs to be continuous and high-profile. Unless this mandate and commitment are forthcoming, the risk management initiative will be unsuccessful. Keeping the risk management policy up to date demonstrates that risk management is a dynamic activity fully supported by the Board.

Table 2: Contents of risk management policy

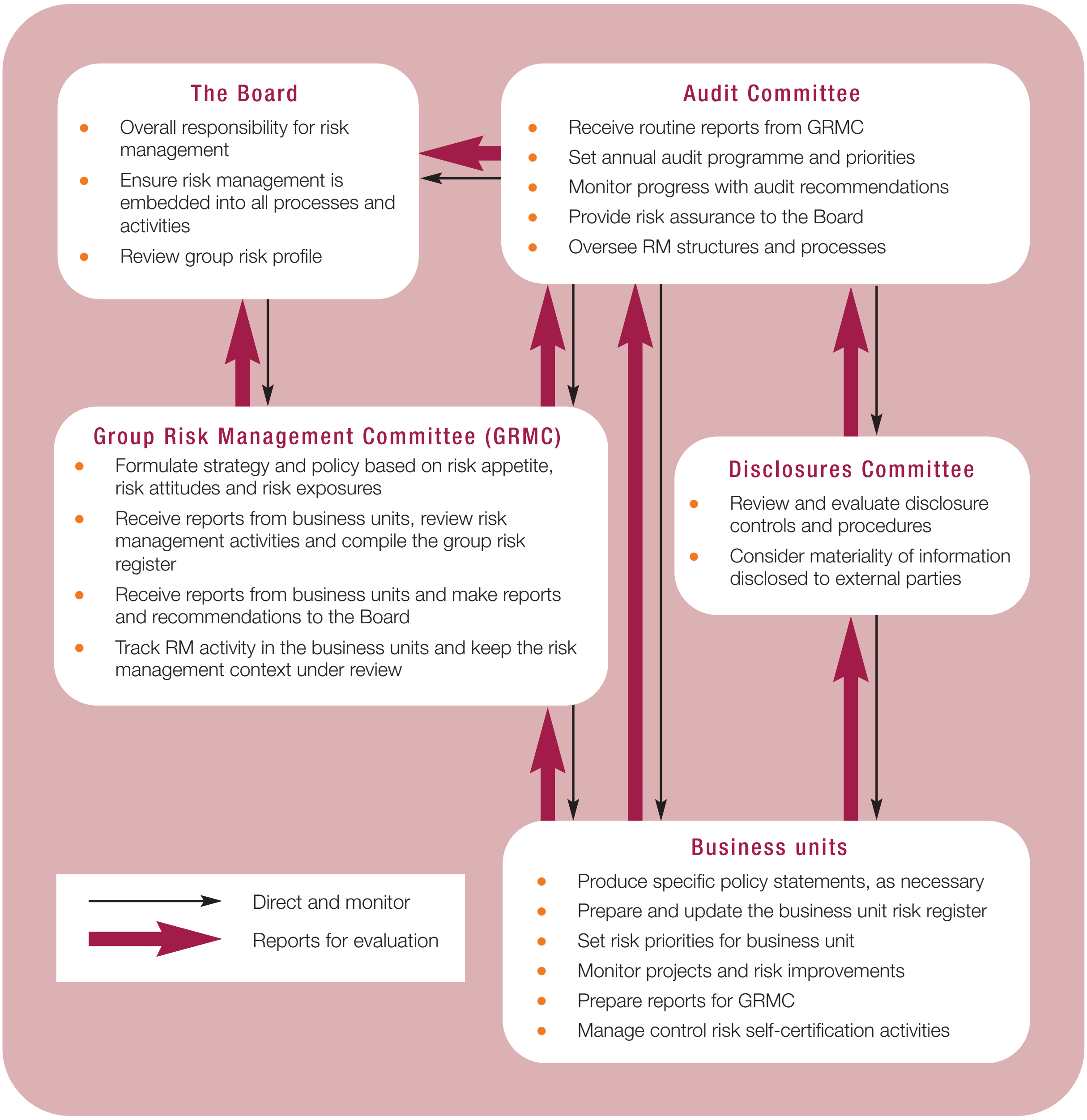
A risk management policy should include the following sections:

- Risk management and internal control objectives (governance)
- Statement of the attitude of the organisation to risk (risk strategy)
- Description of the risk aware culture or control environment
- Level and nature of risk that is acceptable (risk appetite)
- Risk management organisation and arrangements (risk architecture)
- Details of procedures for risk recognition and ranking (risk assessment)
- List of documentation for analysing and reporting risk (risk protocols)
- Risk mitigation requirements and control mechanisms (risk response)
- Allocation of risk management roles and responsibilities
- Risk management training topics and priorities
- Criteria for monitoring and benchmarking of risks
- Allocation of appropriate resources to risk management
- Risk activities and risk priorities for the coming year

Scope of the initiative

In order to be successful, the ERM initiative needs to be comprehensive. However, introducing enhanced standards of risk management is a progressive process that cannot be achieved instantaneously. Therefore, it is necessary for an organisation to decide the scope of the ERM initiative, as it develops. The scope of the initiative will be defined by the range of benefits the organisation is seeking to achieve and this will be influenced by the expectations of the various stakeholders in the organisation.

Figure 4: Risk architecture of a large PLC



The Board

- Overall responsibility for risk management
- Ensure risk management is embedded into all processes and activities
- Review group risk profile

Audit Committee

- Receive routine reports from GRMC
- Set annual audit programme and priorities
- Monitor progress with audit recommendations
- Provide risk assurance to the Board
- Oversee RM structures and processes

Group Risk Management Committee (GRMC)

- Formulate strategy and policy based on risk appetite, risk attitudes and risk exposures
- Receive reports from business units, review risk management activities and compile the group risk register
- Receive reports from business units and make reports and recommendations to the Board
- Track RM activity in the business units and keep the risk management context under review

Disclosures Committee

- Review and evaluate disclosure controls and procedures
- Consider materiality of information disclosed to external parties

Business units

- Produce specific policy statements, as necessary
- Prepare and update the business unit risk register
- Set risk priorities for business unit
- Monitor projects and risk improvements
- Prepare reports for GRMC
- Manage control risk self-certification activities

Risk management framework

Depending on the nature of the organisation, the risk management function may range from a part-time risk manager, to a single risk champion, to a full-scale risk management department. The role of the internal audit function will also differ from one organisation to another. In determining the most appropriate role for internal audit, the organisation needs to ensure that the independence and objectivity of internal audit are not compromised.

The range of risk management responsibilities that need to be allocated in the policy will be broad and extensive. Table 3 sets out examples of the risk management responsibilities that may be allocated in a typical large organisation. The Board has responsibility for determining the strategic direction of the organisation and creating the context for risk management. There need to be arrangements in place to achieve continuous improvement in performance and this responsibility is likely to be allocated to the risk manager.

Table 3: Risk management responsibilities

1. RM responsibilities for the CEO / Board:

- Determine strategic approach to risk and set risk appetite
- Establish the structure for risk management
- Understand the most significant risks
- Manage the organisation in a crisis

2. RM responsibilities for the business unit manager:

- Build risk aware culture within the unit
- Agree risk management performance targets
- Ensure implementation of risk improvement recommendations
- Identify and report changed circumstances / risks

3. RM responsibilities for individual employees:

- Understand, accept and implement RM processes
- Report inefficient, unnecessary or unworkable controls
- Report loss events and near miss incidents
- Co-operate with management on incident investigations

4. RM responsibilities for the risk manager:

- Develop the risk management policy and keep it up to date
- Document the internal risk policies and structures
- Co-ordinate the risk management (and internal control) activities
- Compile risk information and prepare reports for the Board

5. RM responsibilities for specialist risk management functions:

- Assist the company in establishing specialist risk policies
- Develop specialist contingency and recovery plans
- Keep up to date with developments in the specialist area
- Support investigations of incidents and near misses

6. RM responsibilities for internal audit manager:

- Develop a risk-based internal audit programme
- Audit the risk processes across the organisation
- Receive and provide assurance on the management of risk
- Report on the efficiency and effectiveness of internal controls

6: Implementing and benchmarking

Risk assessment is a fundamentally important part of the risk management process. In order to achieve a comprehensive risk management approach, an organisation needs to undertake suitable and sufficient risk assessments. A range of the most common risk assessment techniques is set out in Table 4.

Establish risk assessment procedures

Risk assessment will be required as part of the decision-making processes intended to exploit business opportunities. One way of ensuring that risk is part of business decision-making is to ensure that a risk assessment is attached to all strategy papers presented to the Board. Likewise, risk assessment of all proposed projects should be undertaken and further risk assessments should be undertaken throughout the project. Finally, risk assessments are also required in relation to routine operations.

Other considerations relevant to undertaking risk assessments include decisions on how the risk assessments will be recorded. It is at this stage that an organisation will decide the level of detail that will be recorded about each risk in the risk description. Another important part of the risk assessment procedures will be the identification of the risk classification system to be used by the organisation.

Undertake risk assessments

An organisation should develop benchmarks to determine the significance (or materiality) of the identified risks. The nature of these benchmark tests will depend on the type of risk. For financial risks, a sum of money can be used as the benchmark test of significance. For risks that can cause disruption to operations, the length of disruption may be a suitable test. Reputational risks can be benchmarked in terms of the profile that the report of the event would receive, the likely impact of the event on share price, or the impact on the political and financial support received from key stakeholders.

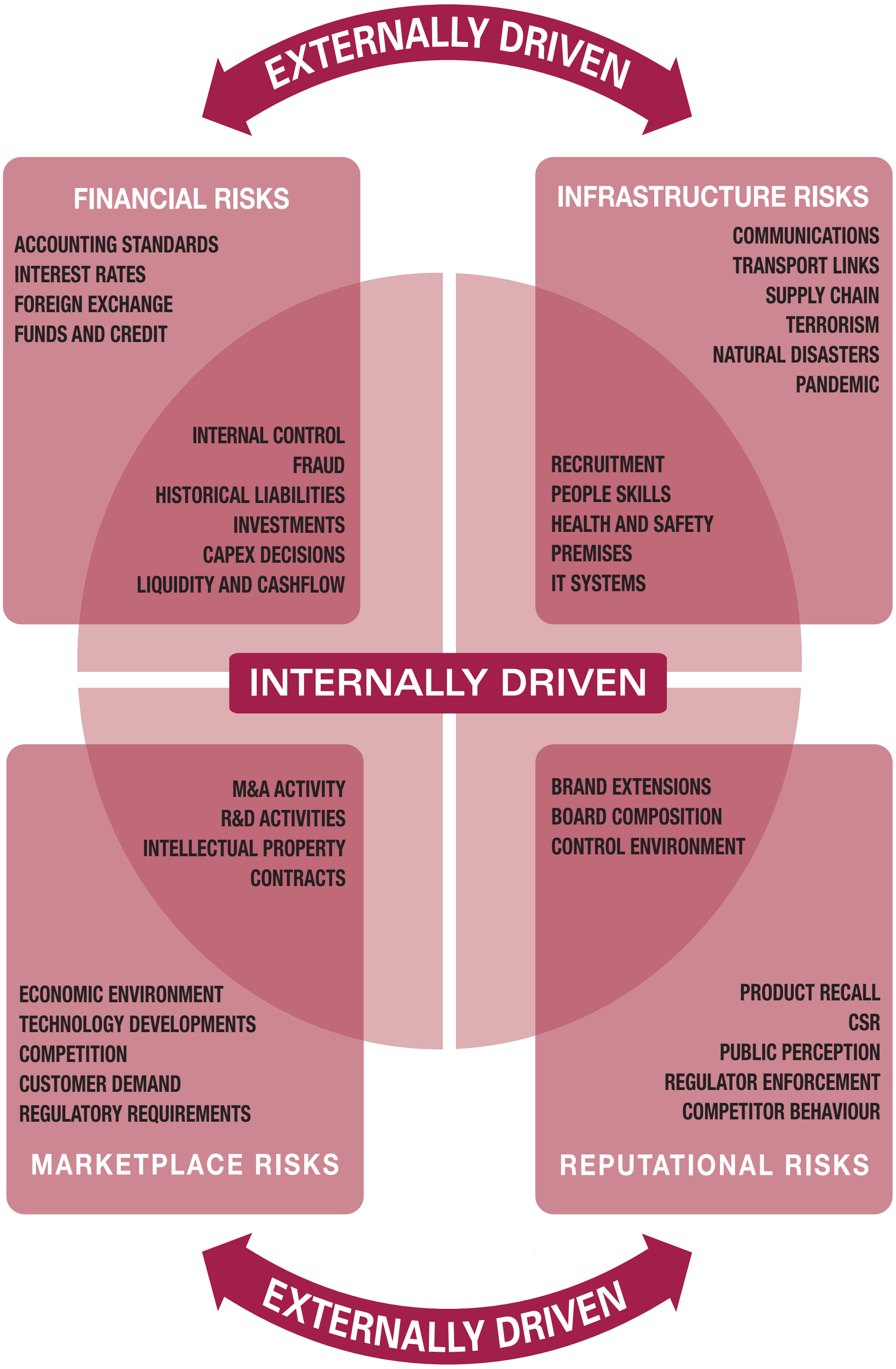
Table 4: Risk assessment techniques

Technique	Brief description
● Questionnaires and checklists	Use of structured questionnaires and checklists to collect information to assist with the recognition of the significant risks
● Workshops and brainstorming	Collection and sharing of ideas and discussion of the events that could impact the objectives, stakeholder expectations or key dependencies
● Inspections and audits	Physical inspections of premises and activities and audits of compliance with established systems and procedures
● Flowcharts and dependency analysis	Analysis of processes and operations within the organisation to identify critical components that are key to success
● HAZOP and FMEA approaches	Hazard and Operability studies and Failure Modes Effects Analysis are quantitative technical failure analysis techniques
● SWOT and PESTLE analyses	Strengths Weaknesses Opportunities Threats (SWOT) and Political Economic Social Technological Legal Environmental (PESTLE) analyses offer structured approaches to risk recognition

Having identified suitable risk assessment procedures and decided the benchmark test of significance for different classes of risks, it will then be possible to identify the appetite or attitude to that type of risk, together with the capacity of the organisation to withstand that risk. Finally, the organisation can determine the overall exposure to the particular type of risk under consideration.

Internal and external factors can give rise to risks. Figure 5 is based on the FIRM Risk Scorecard risk classification system and it provides examples of internal and external key risk drivers. Some risk classification systems have strategic risk as a separate category. However, the FIRM Risk Scorecard approach suggests that strategic (as well as tactical and operational) risks should be identified under all four headings.

Figure 5: Drivers of risk management



Risk appetite and tolerances

It is important that the Board sets rules for risk-taking in respect of all types of risk, and some organisations have produced a risk appetite statement that is applicable to all classes of risk. It is fairly easy for an organisation to confirm that it has no appetite for causing injury and ill health. In practice, however, this may need to be developed into a set of targets for health and safety performance. There is a danger that risk appetite statements fail to be dynamic, and they can constrain behaviour and rapid response.

At Board level, risk appetite is a driver of strategic risk decisions. At executive level, risk appetite translates into a set of procedures to ensure that risk receives adequate attention when making tactical decisions. At operational level, risk appetite dictates operational constraints for routine activities. Despite its importance, it is surprising that the concept of risk appetite is not mentioned in ISO 31000, although it is included in most other risk management standards and stock exchange listing requirements.

7. Measuring and monitoring

It is frequently the case that risk assessments are recorded in a risk register. There is no standard format for a risk register and the organisation should establish a suitable format for this important document. The risk register should not become a static record of the significant risks faced by the organisation. It should be viewed as a risk action plan that includes details of the current controls and details of any further actions that are planned.

These further actions should be written as auditable actions that must be completed within a defined timescale by identified individuals. This will enable the internal audit function to monitor the existing controls and monitor the implementation of any necessary additional controls. The resources required to implement the risk management policy should be clearly established at each level of management and within each business unit. Risk management should be embedded within the strategic planning and budget processes.

As well as monitoring the effectiveness of the existing controls and the implementation of additional controls, the cost-effectiveness of the existing controls should also be monitored. Additionally, monitoring and measuring includes evaluation of the risk aware culture and the risk management framework, and assessment of the extent to which risk management tasks are aligned with other corporate activities.

Evaluate existing controls

Monitoring and measuring extends to the evaluation of culture, performance and preparedness of the organisation. The scope of activities covered by monitoring and measuring also includes monitoring of risk improvement recommendations and evaluation of the embedding of risk management activities in the organisation, as well as routine monitoring of risk performance indicators.

Monitoring the preparedness of the organisation to cope with major disruption is an important part of risk management. This activity normally extends to the development and testing of business continuity plans and disaster recovery plans. There is an overriding need to keep these plans up to date so that the preparedness of the organisation to cope with the identified risk events is assured.

Evaluation of the existing controls will lead to the identification of risk improvement recommendations. These recommendations should be recorded in the risk register by way of a risk action plan. An important part of evaluating the effectiveness of existing controls is to ensure that there is adequate evaluation of the business continuity planning and disaster recovery planning arrangements in place.

Embed risk aware culture

Changes in the organisation and the environment in which it operates must be identified and appropriate modifications made to protocols. Monitoring activities should provide assurance that there are appropriate controls in place and that the procedures are understood and followed. Changes within the organisation and the external business environment must be identified, so that existing procedures can be modified.

Any monitoring and measuring process should also determine whether:

- the measures adopted achieved the intended result
- the procedures adopted were efficient
- sufficient information was available for the risk assessments
- improved knowledge would have helped to reach better decisions
- lessons can be learned for future assessments and controls

Embedding risk management involves an environment that can demonstrate leadership from senior management, involvement of staff at all levels, a culture of learning from experience, appropriate accountability for actions (without developing an automatic blame culture) and good communication on risk issues.

8. Learning and reporting

Completing the feedback loop on the risk management process involves the important steps of learning from experience and reporting on performance. In order to learn from experience, an organisation needs to review risk performance indicators and measure the contribution that enterprise risk management has made to the success of the organisation.

The reasons for undertaking the risk management initiative should have been clearly established. If this has not been done, the organisation will be unable to evaluate whether the contribution was in line with expectations. Monitoring of risk performance indicators should include an evaluation of the contribution being made by risk management, as well as an evaluation of the appropriateness of the control mechanisms that have been selected.

Monitor risk performance

Learning the lessons from risk management also requires investigation of the opinions of key stakeholders both internally and externally. In particular, the opinion of internal audit and evaluation of risk management activities at audit committee will be vitally important. Learning from experience requires more than evaluation of the risk performance indicators.

An annual review of the risk management framework will be necessary, including evaluation of the risk architecture, strategy and protocols. It is important that the organisation has a risk-based audit plan and undertakes appropriate risk reviews.

Other features of learning from experience include evaluation of audit reports and an assessment of the sources of risk assurance available to the Board and the audit committee. An evaluation of the level of assurance that has been obtained is also necessary. Often, a major source of risk assurance for the Board will be self-certification, such as a Control Risk Self Assessment process that provides assurance regarding risk management, risk reporting and disclosure, as well as information about learning from incidents.

Report risk performance

In addition to internal communication and reporting, there will be an obligation on organisations to report externally. Increasingly, these external reports are produced in response to mandatory requirements related to risk management and internal control, such as Turnbull and Sarbanes-Oxley. External risk reporting is designed to provide external stakeholders with assurance that risks have been adequately managed.

External reporting should provide useful information to stakeholders on the status of risk management and the actions that are being taken to ensure continuous improvement in performance. A company needs to report to its stakeholders on a regular basis, setting out its risk management policies and the effectiveness in achieving its objectives. Increasingly, stakeholders look to organisations to provide evidence of appropriate corporate behaviour in such areas as community affairs, human rights, employment practices, health and safety, and the environment.

Risk reporting provides information on historical losses and trends. However, risk disclosure is a more forward-looking activity that anticipates emerging risks. There is a clear difference between measuring and monitoring risk performance and undertaking steps to learn from experience to improve the risk management process and framework. Important lessons can be learned that will assist with improving the design of the support framework and the implementation framework.

Appendix A: Risk management checklist

Risk architecture	
● Statement produced that sets out risk responsibilities and lists the risk-based matters reserved for the Board	
● Risk management responsibilities allocated to an appropriate management committee	
● Arrangements are in place to ensure the availability of appropriate competent advice on risks and controls	
● Risk aware culture exists within the organisation and actions are in hand to enhance the level of risk maturity	
● Sources of risk assurance for the Board have been identified and validated	
Risk strategy	
● Risk management policy produced that describes risk appetite, risk culture and philosophy	
● Key dependencies for success identified, together with the matters that should be avoided	
● Business objectives validated and the assumptions underpinning those objectives tested	
● Significant risks faced by the organisation identified, together with the critical controls required	
● Risk management action plan established that includes the use of key risk indicators, as appropriate	
● Necessary resources identified and provided to support the risk management activities	
Risk protocols	
● Appropriate risk management framework identified and adopted, with modifications as appropriate	
● Suitable and sufficient risk assessments completed and the results recorded in an appropriate manner	
● Procedures to include risk as part of business decision-making established and implemented	
● Details of required risk responses recorded, together with arrangements to track risk improvement recommendations	
● Incident reporting procedures established to facilitate identification of risk trends, together with risk escalation procedures	
● Business continuity plans and disaster recovery plans established and regularly tested	
● Arrangements in place to audit the efficiency and effectiveness of the controls in place for significant risks	
● Arrangements in place for mandatory reporting on risk, including reports on at least the following: ◆ Risk appetite, tolerance and constraints ◆ Risk architecture and risk escalation procedures ◆ Risk aware culture currently in place ◆ Risk assessment arrangements and protocols ◆ Significant risks and key risk indicators ◆ Critical controls and control weaknesses ◆ Sources of assurance available to the Board	

Appendix B: Implementation summary

The table below provides an overview of the steps involved in the implementation of an enterprise risk management (ERM) initiative. Successful implementation of an ERM initiative is an ongoing process that involves working through the 10 steps set out below on a continuous basis. The 10 steps are divided between:

- Planning and designing
- Implementing and benchmarking
- Measuring and monitoring
- Learning and reporting

Activity		Concepts / Tools and techniques
Planning and designing (see Section 5)		
1.	Identify intended benefits of the enterprise risk management initiative and gain Board mandate	● Benefits of ERM ● Embedding risk management
2.	Plan the scope of the ERM initiative and develop common language of risk	● Upside of risk ● Stakeholder expectations
3.	Establish the risk management strategy, framework, and the roles and responsibilities	● Risk management policy ● Risk architecture
Implementing and benchmarking (see Section 6)		
4.	Adopt suitable risk assessment procedures and an agreed risk classification system	● Risk description ● Risk classification systems
5.	Establish risk significance benchmarks and undertake risk assessments	● Risk assessment techniques ● Benchmark tests of significance
6.	Determine risk appetite and risk tolerance levels, and evaluate the existing controls	● Risk register ● Risk appetite
Measuring and monitoring (see Section 7)		
7.	Ensure cost-effectiveness of existing controls and introduce improvements	● Risk improvement plans ● BCP and DRP
8.	Embed risk aware culture and align risk management with other management tasks	● Control environment ● Risk communications
Learning and reporting (see Section 8)		
9.	Monitor and review risk performance indicators to measure ERM contribution	● Audit plan and risk reviews ● Sources of risk assurance
10.	Report risk performance in line with legal and other obligations, and monitor improvement	● Risk reporting ● Legal requirements

airmic

The Association of
Insurance and Risk Managers
Telephone 020 7480 7610

6 Lloyd's Avenue,
London EC3N 3AX
Facsimile 020 7702 3752
Email enquiries@airmic.co.uk
www.airmic.com

alarm

THE PUBLIC
RISK MANAGEMENT
ASSOCIATION

The Public Risk Management Association
Telephone 0333 1230007

Ashton House
Weston
Sidmouth
Devon EX10 0PF
Facsimile 0333 4560007
Email admin@Alarm-uk.org
www.Alarm-uk.org

irm

The Institute of Risk Management
Telephone 020 7709 9808

6 Lloyd's Avenue,
London EC3N 3AX
Facsimile 020 7709 0716
Email enquiries@theirm.org
www.theirm.org

This document is available for download free of charge from the websites of the above organisations.