A Risk Management Standard

IRM

airmic

ALARM

MANAGING RISK

Published by AIRMIC, ALARM, IRM: 2002

Introduction

This Risk Management Standard is the result of work by a team drawn from the major risk management organisations in the UK - The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) and ALARM The National Forum for Risk Management in the Public Sector.

In addition, the team sought the views and opinions of a wide range of other professional bodies with interests in risk management, during an extensive period of consultation.

Risk management is a rapidly developing discipline and there are many and varied views and descriptions of what risk management involves, how it should be conducted and what it is for. Some form of standard is needed to ensure that there is an agreed:

- *terminology related to the words used*
- *process by which risk management can be carried out*
- *organisation structure for risk management*
- *objective for risk management*

Importantly, the standard recognises that risk has both an upside and a downside.

Risk management is not just something for corporations or public organisations, but for any activity whether short or long term. The benefits and opportunities should be viewed not just in the context of the activity itself but in relation to the many and varied stakeholders who can be affected.

There are many ways of achieving the objectives of risk management and it would be impossible to try to set them all out in a single document. Therefore it was never intended to produce a prescriptive standard which would have led to a box ticking approach nor to establish a certifiable process. By meeting the various component parts of this standard, albeit in different ways, organisations will be in a position to report that they are in compliance. The standard represents best practice against which organisations can measure themselves.

The standard has wherever possible used the terminology for risk set out by the International Organization for Standardization (ISO) in its recent document ISO/IEC Guide 73 Risk Management - Vocabulary - Guidelines for use in standards.

In view of the rapid developments in this area the authors would appreciate feedback from organisations as they put the standard into use (addresses to be found on the back cover of this Guide). It is intended that regular modifications will be made to the standard in the light of best practice.

1. Risk

Risk can be defined as the combination of the probability of an event and its consequences (ISO/IEC Guide 73).

In all types of undertaking, there is the potential for events and consequences that constitute opportunities for benefit (upside) or threats to success (downside).

Risk Management is increasingly recognised as being concerned with both positive and negative aspects of risk. Therefore this standard considers risk from both perspectives.

In the safety field, it is generally recognised that consequences are only negative and therefore the management of safety risk is focused on prevention and mitigation of harm.

2. Risk Management

Risk management is a central part of any organisation's strategic management. It is the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.

The focus of good risk management is the identification and treatment of these risks. Its objective is to add maximum sustainable value to all the activities of the organisation. It marshals the understanding of the potential upside and downside of all those factors which can affect the organisation. It increases the probability of success, and reduces both the probability of failure and the uncertainty of achieving the organisation's overall objectives.

Risk management should be a continuous and developing process which runs throughout the organisation's strategy and the implementation of that strategy. It should address methodically all the risks surrounding the organisation's activities past, present and in particular, future.

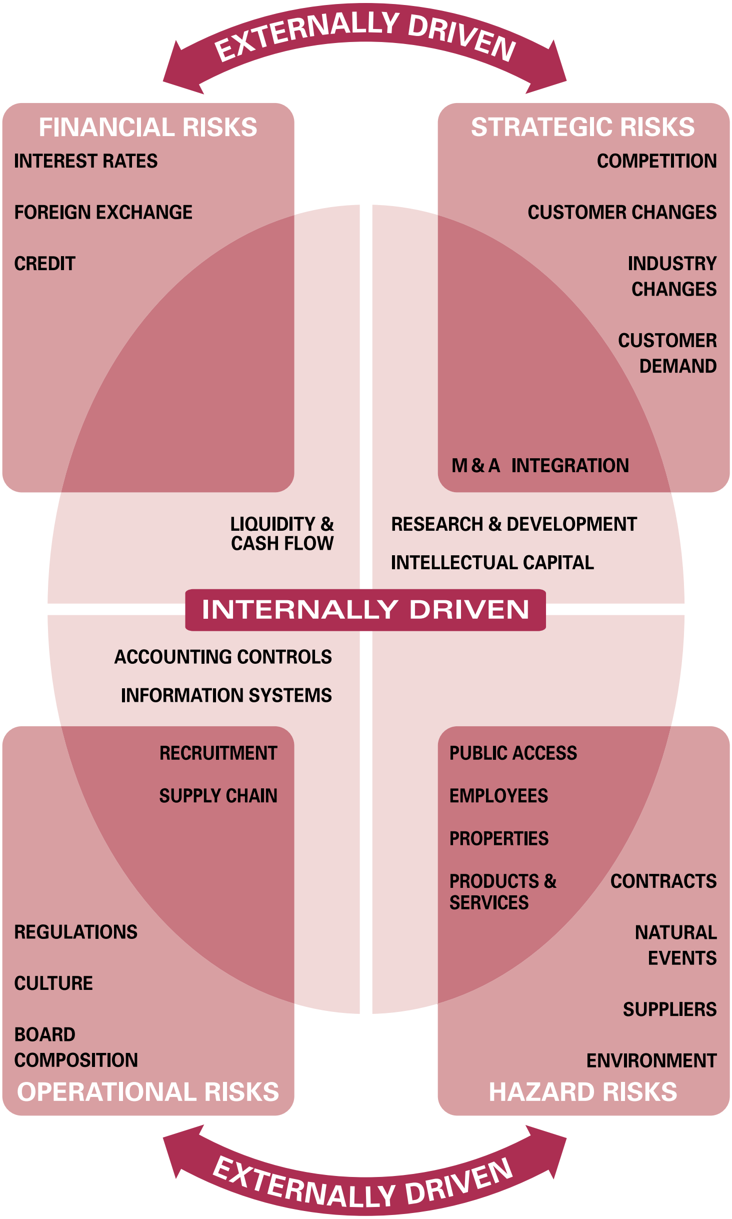
It must be integrated into the culture of the organisation with an effective policy and a programme led by the most senior management. It must translate the strategy into tactical and operational objectives, assigning responsibility throughout the organisation with each manager and employee responsible for the management of risk as part of their job description. It supports accountability, performance measurement and reward, thus promoting operational efficiency at all levels.

2.1 External and Internal Factors

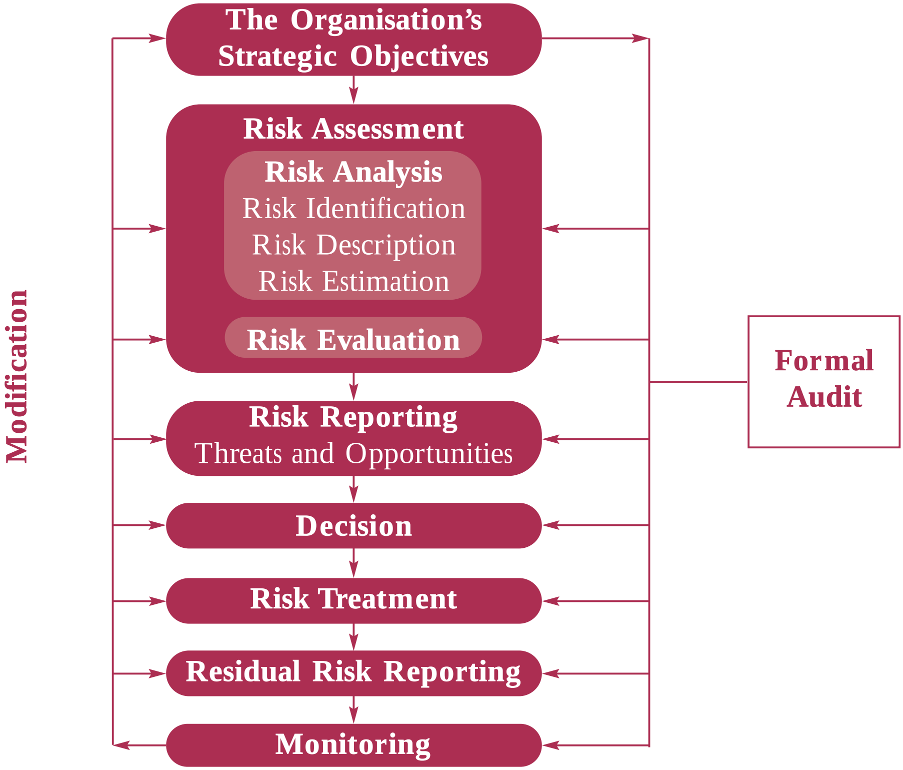
The risks facing an organisation and its operations can result from factors both external and internal to the organisation.

The diagram overleaf summarises examples of key risks in these areas and shows that some specific risks can have both external and internal drivers and therefore overlap the two areas. They can be categorised further into types of risk such as strategic, financial, operational, hazard, etc.

2.1 Examples of the Drivers of Key Risks



2.2 The Risk Management Process



Risk management protects and adds value to the organisation and its stakeholders through supporting the organisation's objectives by:

- *providing a framework for an organisation that enables future activity to take place in a consistent and controlled manner*
- *improving decision making, planning and prioritisation by comprehensive and structured understanding of business activity, volatility and project opportunity/threat*
- *contributing to more efficient use/allocation of capital and resources within the organisation*
- *reducing volatility in the non essential areas of the business*
- *protecting and enhancing assets and company image*
- *developing and supporting people and the organisation's knowledge base*
- *optimising operational efficiency*

3. Risk Assessment

Risk Assessment is defined by the ISO/ IEC Guide 73 as the overall process of **risk analysis** and **risk evaluation**. *(See appendix)*

4. Risk Analysis

4.1 Risk Identification

Risk identification sets out to identify an organisation's exposure to 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 the development of a sound understanding of its strategic and operational objectives, including factors critical to its success and the threats and opportunities related to the achievement of these objectives.

Risk identification should be approached in a methodical way to ensure that all significant activities within the organisation have been identified and all the risks flowing from these activities defined. All associated volatility related to these activities should be identified and categorised.

Business activities and decisions can be classified in a range of ways, examples of which include:

- *Strategic - These concern the long-term strategic objectives of the organisation. They can be affected by such areas as capital availability, sovereign and political risks, legal and regulatory changes, reputation and changes in the physical environment.*
- *Operational - These concern the day-to-day issues that the organisation is confronted with as it strives to deliver its strategic objectives.*
- *Financial - These concern the effective management and control of the finances of the organisation and the effects of external factors such as availability of credit, foreign exchange rates, interest rate movement and other market exposures.*
- *Knowledge management - These concern the effective management and control of the knowledge resources, the production, protection and communication thereof. External factors might include the unauthorised use or abuse of intellectual property, area power failures, and competitive technology. Internal factors might be system malfunction or loss of key staff.*
- *Compliance - These concern such issues as health & safety, environmental, trade descriptions, consumer protection, data protection, employment practices and regulatory issues.*

Whilst risk identification can be carried out by outside consultants, an in-house approach with well communicated, consistent and co-ordinated processes and tools (see Appendix, page 14) is likely to be more effective. In-house 'ownership' of the risk management process is essential.

4.2 Risk Description

The objective of risk description is to display the identified risks in a structured format, for example, by using a table. The risk description table overleaf can be used to facilitate the description and assessment of risks. The use of a well designed structure is necessary to ensure a comprehensive risk identification, description and assessment process. By considering the consequence and probability of each of the risks set out in the table, it should be possible to prioritise the key risks that need to be analysed in more detail. Identification of the risks associated with business activities and decision making may be categorised as strategic, project/ tactical, operational. It is important to incorporate risk management at the conceptual stage of projects as well as throughout the life of a specific project.

4.2.1 Table - Risk Description

1. Name of Risk	
2. Scope of Risk	Qualitative description of the events, their size, type, number and dependencies
3. Nature of Risk	Eg. strategic, operational, financial, knowledge or compliance
4. Stakeholders	Stakeholders and their expectations
5. Quantification of Risk	Significance and Probability
6. Risk Tolerance/ Appetite	Loss potential and financial impact of risk Value at risk Probability and size of potential losses/gains Objective(s) for control of the risk and desired level of performance
7. Risk Treatment & Control Mechanisms	Primary means by which the risk is currently managed Levels of confidence in existing control Identification of protocols for monitoring and review
8. Potential Action for Improvement	Recommendations to reduce risk
9. Strategy and Policy Developments	Identification of function responsible for developing strategy and policy

4.3 Risk Estimation

Risk estimation can be quantitative, semi-quantitative or qualitative in terms of the probability of occurrence and the possible consequence.

For example, consequences both in terms of threats (downside risks) and opportunities (upside risks) may be high, medium or low (see table 4.3.1). Probability may be high, medium or low but requires different definitions in respect of threats and opportunities (see tables 4.3.2 and 4.3.3).

Examples are given in the tables overleaf. Different organisations will find that different measures of consequence and probability will suit their needs best.

For example many organisations find that assessing consequence and probability as high, medium or low is quite adequate for their needs and can be presented as a 3 x 3 matrix.

Other organisations find that assessing consequence and probability using a 5 x 5 matrix gives them a better evaluation.

Table 4.3.1 Consequences - Both Threats and Opportunities

High	Financial impact on the organisation is likely to exceed £x Significant impact on the organisation's strategy or operational activities Significant stakeholder concern
Medium	Financial impact on the organisation likely to be between £x and £y Moderate impact on the organisation's strategy or operational activities Moderate stakeholder concern
Low	Financial impact on the organisation likely to be less that £y Low impact on the organisation's strategy or operational activities Low stakeholder concern

Table 4.3.2 Probability of Occurrence - Threats

Estimation	Description	Indicators
High (Probable)	Likely to occur each year or more than 25% chance of occurrence.	Potential of it occurring several times within the time period (for example - ten years). Has occurred recently.
Medium (Possible)	Likely to occur in a ten year time period or less than 25% chance of occurrence.	Could occur more than once within the time period (for example - ten years). Could be difficult to control due to some external influences. Is there a history of occurrence?
Low (Remote)	Not likely to occur in a ten year period or less than 2% chance of occurrence.	Has not occurred. Unlikely to occur.

Table 4.3.3 Probability of Occurrence - Opportunities

Estimation	Description	Indicators
High (Probable)	Favourable outcome is likely to be achieved in one year or better than 75% chance of occurrence.	Clear opportunity which can be relied on with reasonable certainty, to be achieved in the short term based on current management processes.
Medium (Possible)	Reasonable prospects of favourable results in one year of 25% to 75% chance of occurrence.	Opportunities which may be achievable but which require careful management. Opportunities which may arise over and above the plan.
Low (Remote)	Some chance of favourable outcome in the medium term or less than 25% chance of occurrence.	Possible opportunity which has yet to be fully investigated by management. Opportunity for which the likelihood of success is low on the basis of management resources currently being applied.

4.4 Risk Analysis methods and techniques

A range of techniques can be used to analyse risks. These can be specific to upside or downside risk or be capable of dealing with both. (See Appendix, page 14, for examples).

4.5 Risk Profile

The result of the risk analysis process can be used to produce a risk profile which gives a significance rating to each risk and provides a tool for prioritising risk treatment efforts. This ranks each identified risk so as to give a view of the relative importance.

This process allows the risk to be mapped to the business area affected, describes the primary control procedures in place and indicates areas where the level of risk control investment might be increased, decreased or reapportioned.

Accountability helps to ensure that 'ownership' of the risk is recognised and the appropriate management resource allocated.

5. Risk Evaluation

When the risk analysis process has been completed, it is necessary to compare the estimated risks against risk criteria which the organisation has established. The risk criteria may include associated costs and benefits, legal requirements, socio-economic and environmental factors, concerns of stakeholders, etc. Risk evaluation therefore, is used to make decisions about the significance of risks to the organisation and whether each specific risk should be accepted or treated.

6. Risk Reporting and Communication

6.1 Internal Reporting

Different levels within an organisation need different information from the risk management process.

The Board of Directors should:

- *know about the most significant risks facing the organisation*
- *know the possible effects on shareholder value of deviations to expected performance ranges*
- *ensure appropriate levels of awareness throughout the organisation*
- *know how the organisation will manage a crisis*
- *know the importance of stakeholder confidence in the organisation*
- *know how to manage communications with the investment community where applicable*
- *be assured that the risk management process is working effectively*
- *publish a clear risk management policy covering risk management philosophy and responsibilities*

Business Units should:

- *be aware of risks which fall into their area of responsibility, the possible impacts these may have on other areas and the consequences other areas may have on them*
- *have performance indicators which allow them to monitor the key business and financial activities, progress towards objectives and identify developments which require intervention (e.g. forecasts and budgets)*
- *have systems which communicate variances in budgets and forecasts at appropriate frequency to allow action to be taken*
- *report systematically and promptly to senior management any perceived new risks or failures of existing control measures*

Individuals should:

- *understand their accountability for individual risks*
- *understand how they can enable continuous improvement of risk management response*
- *understand that risk management and risk awareness are a key part of the organisation's culture*
- *report systematically and promptly to senior management any perceived new risks or failures of existing control measures*

6.2 External Reporting

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 effective management of the organisation's non-financial performance in such areas as community affairs, human rights, employment practices, health and safety and the environment.

Good corporate governance requires that companies adopt a methodical approach to risk management which:

- *protects the interests of their stakeholders*
- *ensures that the Board of Directors discharges its duties to direct strategy, build value and monitor performance of the organisation*
- *ensures that management controls are in place and are performing adequately*

The arrangements for the formal reporting of risk management should be clearly stated and be available to the stakeholders.

The formal reporting should address:

- *the control methods - particularly management responsibilities for risk management*
- *the processes used to identify risks and how they are addressed by the risk management systems*
- *the primary control systems in place to manage significant risks*
- *the monitoring and review system in place*

Any significant deficiencies uncovered by the system, or in the system itself, should be reported together with the steps taken to deal with them.

7. Risk Treatment

Risk treatment is the process of selecting and implementing measures to modify the risk. Risk treatment includes as its major element, risk control/mitigation, but extends further to, for example, risk avoidance, risk transfer, risk financing, etc.

NOTE: In this standard, risk financing refers to the mechanisms (eg insurance programmes) for funding the financial consequences of risk. Risk financing is not generally considered to be the provision of funds to meet the cost of implementing risk treatment (as defined by ISO/IEC Guide 73; see page 17).

Any system of risk treatment should provide as a minimum:

- *effective and efficient operation of the organisation*
- *effective internal controls*
- *compliance with laws and regulations.*

The risk analysis process assists the effective and efficient operation of the organisation by identifying those risks which require attention by management. They will need to prioritise risk control actions in terms of their potential to benefit the organisation.

Effectiveness of internal control is the degree to which the risk will either be eliminated or reduced by the proposed control measures.

Cost effectiveness of internal control relates to the cost of implementing the control compared to the risk reduction benefits expected.

The proposed controls need to be measured in terms of potential economic effect if no action is taken versus the cost of the proposed action(s) and invariably require more detailed information and assumptions than are immediately available.

Firstly, the cost of implementation has to be established. This has to be calculated with some accuracy since it quickly becomes the baseline against which cost effectiveness is measured. The loss to be expected if no action is taken must also be estimated and by comparing the results, management can decide whether or not to implement the risk control measures.

Compliance with laws and regulations is not an option. An organisation must understand the applicable laws and must implement a system of controls to achieve compliance. There is only occasionally some flexibility where the cost of reducing a risk may be totally disproportionate to that risk.

One method of obtaining financial protection against the impact of risks is through risk financing which includes insurance. However, it should be recognised that some losses or elements of a loss will be uninsurable eg the uninsured costs associated with work-related health, safety or environmental incidents, which may include damage to employee morale and the organisation's reputation.

8. Monitoring and Review of the Risk Management Process

Effective risk management requires a reporting and review structure to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place. Regular audits of policy and standards compliance should be carried out and standards performance reviewed to identify opportunities for improvement. It should be remembered that organisations are dynamic and operate in dynamic environments. Changes in the organisation and the environment in which it operates must be identified and appropriate modifications made to systems.

The monitoring process should provide assurance that there are appropriate controls in place for the organisation's activities and that the procedures are understood and followed.

Changes in the organisation and the environment in which it operates must be identified and appropriate changes made to systems.

Any monitoring and review process should also determine whether:

- *the measures adopted resulted in what was intended*
- *the procedures adopted and information gathered for undertaking the assessment were appropriate*
- *improved knowledge would have helped to reach better decisions and identify what lessons could be learned for future assessments and management of risks*

9. The Structure and Administration of Risk Management

9.1 Risk Management Policy

An organisation's risk management policy should set out its approach to and appetite for risk and its approach to risk management. The policy should also set out responsibilities for risk management throughout the organisation.

Furthermore, it should refer to any legal requirements for policy statements eg. for Health and Safety.

Attaching to the risk management process is an integrated set of tools and techniques for use in the various stages of the business process. To work effectively, the risk management process requires:

- *commitment from the chief executive and executive management of the organisation*
- *assignment of responsibilities within the organisation*
- *allocation of appropriate resources for training and the development of an enhanced risk awareness by all stakeholders.*

9.2 Role of the Board

The Board has responsibility for determining the strategic direction of the organisation and for creating the environment and the structures for risk management to operate effectively.

This may be through an executive group, a non-executive committee, an audit committee or such other function that suits the organisation's way of operating and is capable of acting as a 'sponsor' for risk management.

The Board should, as a minimum, consider, in evaluating its system of internal control:

- *the nature and extent of downside risks acceptable for the company to bear within its particular business*
- *the likelihood of such risks becoming a reality*
- *how unacceptable risks should be managed*
- *the company's ability to minimise the probability and impact on the business*
- *the costs and benefits of the risk and control activity undertaken*
- *the effectiveness of the risk management process*
- *the risk implications of board decisions*

9.3 Role of the Business Units

This includes the following:

- *the business units have primary responsibility for managing risk on a day-to-day basis*
- *business unit management is responsible for promoting risk awareness within their operations; they should introduce risk management objectives into their business*
- *risk management should be a regular management-meeting item to allow consideration of exposures and to reprioritise work in the light of effective risk analysis*
- *business unit management should ensure that risk management is incorporated at the conceptual stage of projects as well as throughout a project*

9.4 Role of the Risk Management Function

Depending on the size of the organisation the risk management function may range from a single risk champion, a part time risk manager, to a full scale risk management department. The role of the Risk Management function should include the following:

- *setting policy and strategy for risk management*
- *primary champion of risk management at strategic and operational level*
- *building a risk aware culture within the organisation including appropriate education*
- *establishing internal risk policy and structures for business units*
- *designing and reviewing processes for risk management*
- *co-ordinating the various functional activities which advise on risk management issues within the organisation*
- *developing risk response processes, including contingency and business continuity programmes*
- *preparing reports on risk for the board and the stakeholders*

9.5 Role of Internal Audit

The role of Internal Audit is likely to differ from one organisation to another. In practice, Internal Audit's role may include some or all of the following:

- *focusing the internal audit work on the significant risks, as identified by management, and auditing the risk management processes across an organisation*
- *providing assurance on the management of risk*
- *providing active support and involvement in the risk management process*
- *facilitating risk identification/assessment and educating line staff in risk management and internal control*
- *co-ordinating risk reporting to the board, audit committee, etc*

In determining the most appropriate role for a particular organisation, Internal Audit should ensure that the professional requirements for independence and objectivity are not breached.

9.6 Resources and Implementation

The resources required to implement the organisation's risk management policy should be clearly established at each level of management and within each business unit.

In addition to other operational functions they may have, those involved in risk management should have their roles in co-ordinating risk management policy/strategy clearly defined. The same clear definition is also required for those involved in the audit and review of internal controls and facilitating the risk management process.

Risk management should be embedded within the organisation through the strategy and budget processes. It should be highlighted in induction and all other training and development as well as within operational processes e.g. product/service development projects.

10. Appendix

Risk Identification Techniques - examples

- *Brainstorming*
- *Questionnaires*
- *Business studies which look at each business process and describe both the internal processes and external factors which can influence those processes*
- *Industry benchmarking*
- *Scenario analysis*
- *Risk assessment workshops*
- *Incident investigation*
- *Auditing and inspection*
- *HAZOP (Hazard & Operability Studies)*

Risk Analysis Methods and Techniques - examples

Upside risk

- *Market survey*
- *Prospecting*
- *Test marketing*
- *Research and Development*
- *Business impact analysis*

Both

- *Dependency modelling*
- *SWOT analysis (Strengths, Weaknesses, Opportunities, Threats)*
- *Event tree analysis*
- *Business continuity planning*
- *BPEST (Business, Political, Economic, Social, Technological) analysis*
- *Real Option Modelling*
- *Decision taking under conditions of risk and uncertainty*
- *Statistical inference*
- *Measures of central tendency and dispersion*
- *PESTLE (Political Economic Social Technical Legal Environmental)*

Downside risk

- *Threat analysis*
- *Fault tree analysis*
- *FMEA (Failure Mode & Effect Analysis)*

On the following pages are extracts from the document PD ISO/IEC Guide 73: 2002 reproduced with the permission of British Standards Institution under licence number 2002SK/0313. British Standards can be obtained from BSI Customer Services, 389 Chiswick High Road, London W4 4AL. (Tel + 44 (0) 20 8996 9001)

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

ALARM The National Forum for
Risk Management in the Public Sector
Telephone 01395 223399

Queens Drive, Exmouth
Devon, EX8 2AY
Facsimile 01395 223304
Email admin@alarm.uk.com
www.alarm-uk.com

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

This publication is available from the above organisations for download from their respective websites free of charge.
Please contact the individual associations if you wish to purchase more copies of this Risk Management Standard in printed form