

A Risk Management Standard



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.

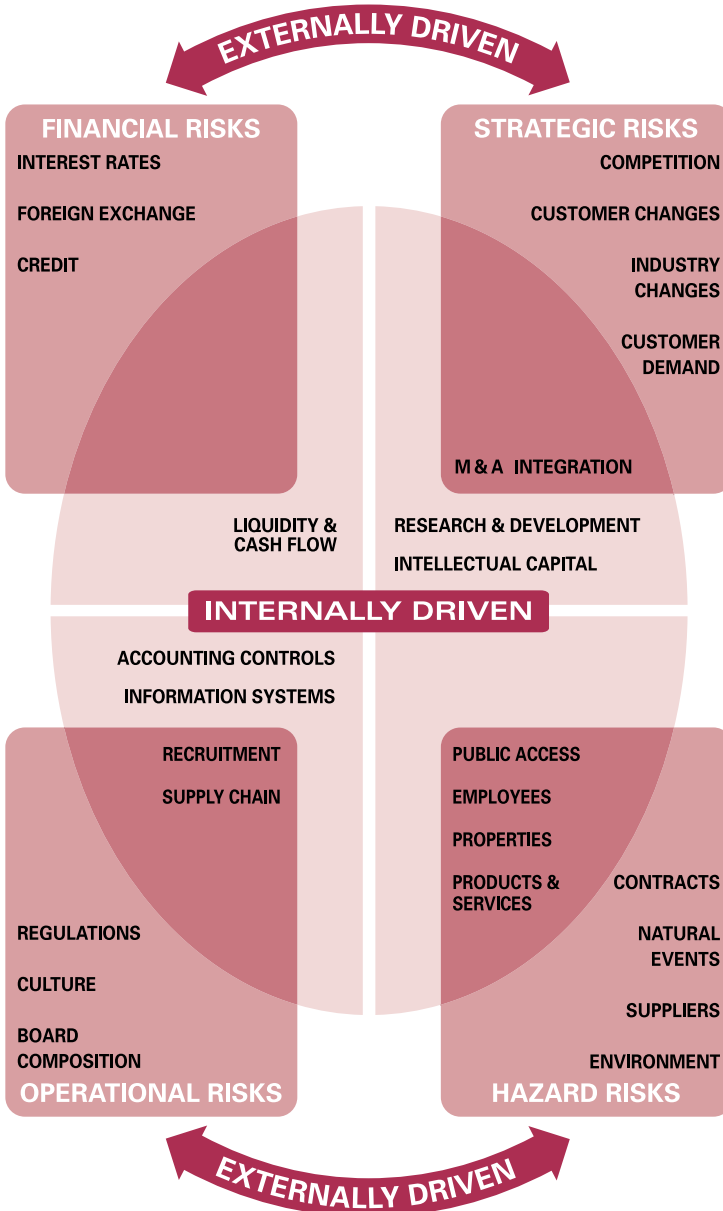
It must be integrated into the culture of the organisation with an effective policy and a programme led by the most senior management. It must translate the strategy into tactical and operational objectives, assigning responsibility throughout the organisation with each manager and employee responsible 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 than £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 reappropriated.

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)

ISO/IEC Guide 73

Risk Management - Vocabulary - Guidelines for use in standards

1. Scope

This Guide provides standards writers with generic definitions of risk management terms. It is intended as a top-level generic document in the preparation or revision of standards that include aspects of risk management.

The aim of this Guide is to promote a coherent approach to the description of risk management activities and the use of risk management terminology. Its purpose is to contribute towards mutual understanding amongst the members of ISO and IEC rather than provide guidance on risk management practice.

ISO/IEC Guide 51 deals with safety aspects.

NOTE 1 The term "standard" - used throughout this Guide - includes Technical Reports and Guides.

NOTE 2 Such standards can deal exclusively with risk management or can include clauses specific to risk management.

2. Overview of risk management terms and definitions

The relationships between the terms and definitions for risk management are shown in Figures 1 to 3 of ISO/IEC Guide 73.

Risk management is part of the broader management processes of organizations. Risk management depends on the context in which it is used. The words used in each context may vary.

Where terms related to risk management are used in a standard, it is imperative that their intended meanings within the context of the standard are not misinterpreted or misunderstood. Accordingly, this Guide provides definitions for the various meanings that each term is likely to have, without giving definitions that contradict each other. Increasingly, organizations utilize risk management processes in order to optimize the management of potential opportunities. This differs from the risk assessment process explained in ISO/IEC Guide 51, where risk is

taken as producing only negative consequences. However, since the business community increasingly adopts the broader approach to risk, this Guide seeks to address both situations. The definitions in this Guide are broader in concept than those in ISO/IEC Guide 51. For all safety-related matters, the definitions given in ISO/IEC Guide 51 apply. These are given in annex A of ISO/IEC Guide 73. An alphabetical list of terms is given in both English and French.

NOTE When a term which is defined in this Guide is cited in another definition, it is given in boldface with its cross-reference. Terms cited in the notes are in boldface but without cross-references.

3. Terms and definitions

3.1 Basic terms

3.1.1 risk

combination of the **probability** (3.1.3) of an **event** (3.1.4) and its **consequence** (3.1.2)

NOTE 1 The term "risk" is generally used only when there is at least the possibility of negative consequences.

NOTE 2 In some situations, risk arises from the possibility of deviation from the expected outcome or event.

NOTE 3 See ISO/IEC Guide 51 for issues related to safety.

3.1.2 consequence

outcome of an **event** (3.1.4)

NOTE 1 There can be more than one consequence from one event

NOTE 2 Consequences can range from positive to negative. However, consequences are always negative for safety aspects.

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

3.1.3 probability

extent to which an **event** (3.1.4) is likely to occur

NOTE 1 ISO 3534-1: 1993, definition 1.1, gives the mathematical definition of probability as "a real number in the scale 0 to 1 attached to a random event. It can be related to a long-run relative frequency of occurrence or to a degree of belief that an event will occur. For a high degree of belief, the probability is near 1."

NOTE 2 Frequency rather than probability may be used in describing **risk**.

NOTE 3 Degrees of belief about probability can be chosen as classes or ranks, such as

– rare/unlikely/moderate/likely/almost certain, or
– incredible/improbable/remote/occasional/
probable/frequent

3.1.4 event

occurrence of a particular set of circumstances

NOTE 1 The event can be certain or uncertain.

NOTE 2 The event can be a single occurrence or a series of occurrences.

NOTE 3 The **probability** associated with the event can be estimated for a given period of time.

3.1.5 source

item or activity having a potential for a **consequence** (3.1.2)

NOTE In the context of safety, source is a hazard (refer to annex A and ISO/IEC Guide 51:1999).

3.1.6 risk criteria

terms of reference by which the significance of **risk** (3.1.1) is assessed

NOTE Risk criteria can include associated cost and benefits, legal and statutory requirements, socio-economic and environmental aspects, the concerns of **stakeholders**, priorities and other inputs to the assessment.

3.1.7 risk management

coordinated activities to direct and control an organization with regard to **risk** (3.1.1)

NOTE Risk management generally includes **risk assessment, risk treatment, risk acceptance** and **risk communication**.

3.1.8 risk management system

set of elements of an organization's management system concerned with managing **risk** (3.1.1)

NOTE 1 Management system elements can include strategic planning, decision making, and other processes for dealing with risk.

NOTE 2 The culture of an organization is reflected in its risk management system.

3.2 Terms related to people or organizations affected by risk

3.2.1 stakeholder

any individual, group or organization that can affect, be affected by, or perceive itself to be affected by, a **risk** (3.1.1)

NOTE 1 The decision-maker is also a stakeholder.

NOTE 2 The term "stakeholder" includes but has a broader meaning than **interested party** (which is defined in ISO 9000:2000).

3.2.2 interested party

person or group having an interest in the performance or success of an organization
EXAMPLES: Customers, owners, people in an organization, suppliers, bankers, unions, partners or society.

NOTE A group can comprise an organization, a part thereof, or more than one organization.

[ISO 9000:2000, definition 3.3.7]

3.2.3 risk perception

way in which a **stakeholder** (3.2.1) views a **risk** (3.1.1), based on a set of values or concerns

NOTE 1 Risk perception depends on the stakeholder's needs, issues and knowledge.

NOTE 2 Risk perception can differ from objective data.

3.2.4 risk communication

exchange or sharing of information about **risk** (3.1.1) between the decision-maker and other **stakeholders** (3.2.1)

NOTE The information can relate to the existence, nature, form, **probability**, severity, acceptability, treatment or other aspects of risk.

3.3 Terms related to risk assessment

3.3.1 risk assessment

overall process of **risk analysis** (3.3.2) and **risk evaluation** (3.3.6)

3.3.2 risk analysis

systematic use of information to identify **sources** (3.1.5) and to estimate the **risk** (3.1.1)

NOTE 1 Risk analysis provides a basis for **risk evaluation, risk treatment** and **risk acceptance**.

NOTE 2 Information can include historical data, theoretical analysis, informed opinions, and the concerns of **stakeholders**.

NOTE 3 See ISO/IEC Guide 51 for risk analysis in the context of safety.

3.3.3 risk identification

process to find, list and characterize elements of **risk** (3.1.1)

NOTE 1 Elements can include **source** or hazard, **event, consequence** and **probability**.

NOTE 2 Risk identification can also reflect the concerns of **stakeholders**.

3.3.4 source identification

process to find, list and characterize **sources** (3.1.5)

NOTE In the context of safety, source identification is called hazard identification (see ISO/IEC Guide 51).

3.3.5 risk estimation

process used to assign values to the **probability** (3.1.3) and **consequences** (3.1.2) of a **risk** (3.1.1)

NOTE Risk estimation can consider cost, benefits, the concerns of **stakeholders** and other variables, as appropriate for **risk evaluation**.

3.3.6 risk evaluation

process of comparing the estimated **risk** (3.1.1) against given **risk criteria** (3.1.6) to determine the significance of the risk

NOTE 1 Risk evaluation may be used to assist in the decision to accept or to treat a risk.

NOTE 2 See ISO/IEC Guide 51 for risk evaluation in the context of safety.

3.4 Terms related to risk treatment and control

3.4.1 risk treatment

process of selection and implementation of measures to modify **risk** (3.1.1)

NOTE 1 The term “risk treatment” is sometimes used for the measures themselves.

NOTE 2 Risk treatment measures can include avoiding, optimizing, transferring or retaining risk.

3.4.2 risk control

actions implementing **risk management** (3.1.7) decisions

NOTE Risk control may involve monitoring, re-evaluation, and compliance with decisions.

3.4.3 risk optimization

process, related to a **risk** (3.1.1), to minimize the negative and to maximize the positive **consequences** (3.1.2) and their respective **probabilities** (3.1.3)

NOTE 1 In the context of safety, risk optimization is focused on reducing the risk.

NOTE 2 Risk optimization depends upon **risk criteria**, including costs and legal requirements.

NOTE 3 Risks associated with **risk control** can be considered.

3.4.4 risk reduction

actions taken to lessen the **probability** (3.1.3), negative **consequences** (3.1.2) or both, associated with a **risk** (3.1.1)

3.4.5 mitigation

limitation of any negative **consequence** (3.1.2) of a particular **event** (3.1.4)

3.4.6 risk avoidance

decision not to become involved in, or action to withdraw from, a risk situation

NOTE The decision may be taken based on the result of **risk evaluation**.

3.4.7 risk transfer

sharing with another party the burden of loss or benefit of gain, for a **risk** (3.1.1)

NOTE 1 Legal or statutory requirements can limit, prohibit or mandate the transfer of certain risk.

NOTE 2 Risk transfer can be carried out through insurance or other agreements.

NOTE 3 Risk transfer can create new risks or modify existing risk.

NOTE 4 Relocation of the **source** is not risk transfer.

3.4.8 risk financing

provision of funds to meet the cost of implementing **risk treatment** (3.4.1) and related costs

NOTE In some industries, risk financing refers to funding only the financial consequences related to the **risk**.

3.4.9 risk retention

acceptance of the burden of loss, or benefit of gain, from a particular **risk** (3.1.1)

NOTE 1 Risk retention includes the acceptance of risks that have not been identified.

NOTE 2 Risk retention does not include treatments involving insurance, or transfer by other means.

NOTE 3 There can be variability in the degree of acceptance and dependence on **risk criteria**.

3.4.10 risk acceptance

decision to accept a **risk** (3.1.1)

NOTE 1 The verb “to accept” is chosen to convey the idea that acceptance has its basic dictionary meaning.

NOTE 2 Risk acceptance depends on **risk criteria**.

3.4.11 residual risk

risk (3.1.1) remaining after **risk treatment** (3.4.1)

NOTE See ISO/IEC Guide 51 for safety-related applications.



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



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