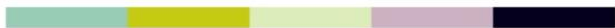**Investors in Risk Management**

A Practical Guide to
Enterprise Risk Management

Creating value through effective risk management

www.iirmglobal.com

Disclaimer

This document provides general information. The information contained in this communication does not constitute advice and should not be relied upon as such. Professional advice should be sought prior to actions being taken on any of the information.

Investors in Risk Management (IIRM) disclaim all responsibility and liability arising from anything done or omitted to be done by any party in reliance, whether wholly or partially, on any of the information. Any party that relies on the information does so at its own risk.

CONTENTS

1. Introduction

2. Developing a risk management framework

3. Implementing a risk management framework

4. Reviewing and enhancing a risk management framework

5. Appendices

Executive summary

Driven by its purpose of creating value through effective risk management: Investors in Risk Management enables organisations to create, implement and enhance their risk management capabilities. We provide Risk Management Accreditation (Certification) services to public sector and private organisations. Successful accreditation against our Risk Management Maturity Model is the sign of a great organisation with a clear commitment to risk management and sustainability.

Our independent expert advisory services also provide practical risk management guidance and assist organisations to manage their risks effectively through the application of their risk management processes at varying levels and within their specific contexts.

Our highly competent people use their expertise to assess the risk management maturity level of public sector and private organisations to enhance an organisation-wide risk management framework to ensure that key risks are effectively identified and responded to in a manner that is appropriate to:

- the nature of the risks faced by the organisation
- the organisation's ability to accept and/or manage risk/s
- the resources available to manage risks within the organisation
- the organisation's culture.

At IIRM, we believe that an organisation may have highly sophisticated processes and structures established to manage risks. However, unless these structures and processes are supported by management and staff with the appropriate competencies, attitudes and behaviours, the framework is likely to be ineffective.

To render a risk management framework effective, we ensure that there is an appropriate balance in focus between the "hard" aspects of risk management (i.e. processes and structures) and the "soft" aspects (i.e. culture and people).

IIRM adopts organisation-wide risk management frameworks that provide a holistic approach to correctly identifying, assessing, managing, monitoring and prioritising responses to all critical risks across the organisation in a manner that supports business strategies and plans in both public sector and private organisations.

Purpose of the Guide

The guide aims to provide practical guidance to organisations for developing, implementing and enhancing their risk management frameworks.

The guide is primarily targeted at risk managers or their equivalents and is designed to assist them to better embed risk management practices within their respective organisations. The guide may also be used by other stakeholder groups including the board, executives, and employees during the execution of their risk management responsibilities. The guide is primarily developed for medium-to-large organisations; however, the majority of the content is applicable to smaller organisations as well. Some of the more 'advanced' risk management framework attributes may not be feasible or appropriate for smaller organisations.

The guide is developed to support organisations with varying degrees of risk management maturity, recognising that risk management is a continuous journey. Using this guide, organisations with less mature risk management practices can incrementally enhance and progress their risk management frameworks.

No single risk maturity level will be appropriate for all organisations. Each organisation's board and executives should decide on the appropriate level of risk management sophistication that they aspire to achieve. The desired level of risk maturity may change over time to reflect changes in the organisation's complexity, size and risk appetite.

The scope of the guide is focused primarily on providing generic guidance on the management of organisational-level risk.

Overview of the document

The document is structured into three key sections:

- Developing a risk management framework
- Implementing a risk management framework
- Reviewing and enhancing a risk management framework

Each section provides guidance on specific topics of developing, implementing, and reviewing/enhancing a risk management framework.

Key definitions and terminology

The risk management 'glossary' based on the Risk Standard is appended to this document. However, some more common definitions are noted below:

- **Risk** – Effect of uncertainty on objectives;
  Risk is often characterised with reference to potential events and consequences, or a combination of these. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
- **Risk management** – Coordinated activities to direct and control an organisation with regard to risk.
- **Risk management framework** – A set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

Acknowledgements

- Permission to produce extracts from Vigilant Risk Manager is granted by the Vigilant Risk Manager.
- Text has been used from The Orange Book under Crown copyright.
- Material has been used and changes have been made for specific use under a Creative Commons Attribution 3.0 Australia licence from © State of Victoria through the Victorian Managed Insurance Authority 2014.

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2 Developing a risk management framework

2.1 Overview - Risk Management Framework

A risk management framework aims to assist an organisation to manage its risks effectively through the application of the risk management process at varying levels and within specific contexts of the organisation. Such a framework should ensure that risk information derived from these processes is adequately reported and used as a basis for decision-making at all levels.

What is a risk management framework?

A risk management framework is defined by the ISO Guide 73 as:

A set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

The Guide notes that

1. The foundations include the policy, objectives, mandate and commitment to manage risk.
2. The organisational arrangements include plans, relationships, accountabilities, resources, processes and activities
3. The risk management framework should be embedded within the organisation's overall strategic and operational policies and practices.

Purpose of a risk management framework

The purpose of establishing an organisational risk management framework is to ensure that key risks are effectively identified and responded to in a manner that is appropriate to:

- the nature of the risks faced by the organisation
- the organisation's ability to accept and/or manage risk/s
- the resources available to manage risks within the organisation
- the organisation's culture

Ultimately, risk needs to be managed in order that the organisation might maximise its ability to meet its strategic objectives as well as associated operational targets and goals.

## "Hard" versus "soft" aspects of risk management

For a risk management framework to be effective there must be an appropriate balance in focus on both the "hard" aspects of risk management (i.e. processes and structures) and the "soft" aspects (i.e. culture and people).

www.iirmglobal.com

For example, an organisation may have highly sophisticated processes and structures established to manage risks. However, unless these structures and processes are supported by management and staff with the appropriate competencies, attitudes and behaviours, the framework is likely to be ineffective.

IIRM Risk Management Framework
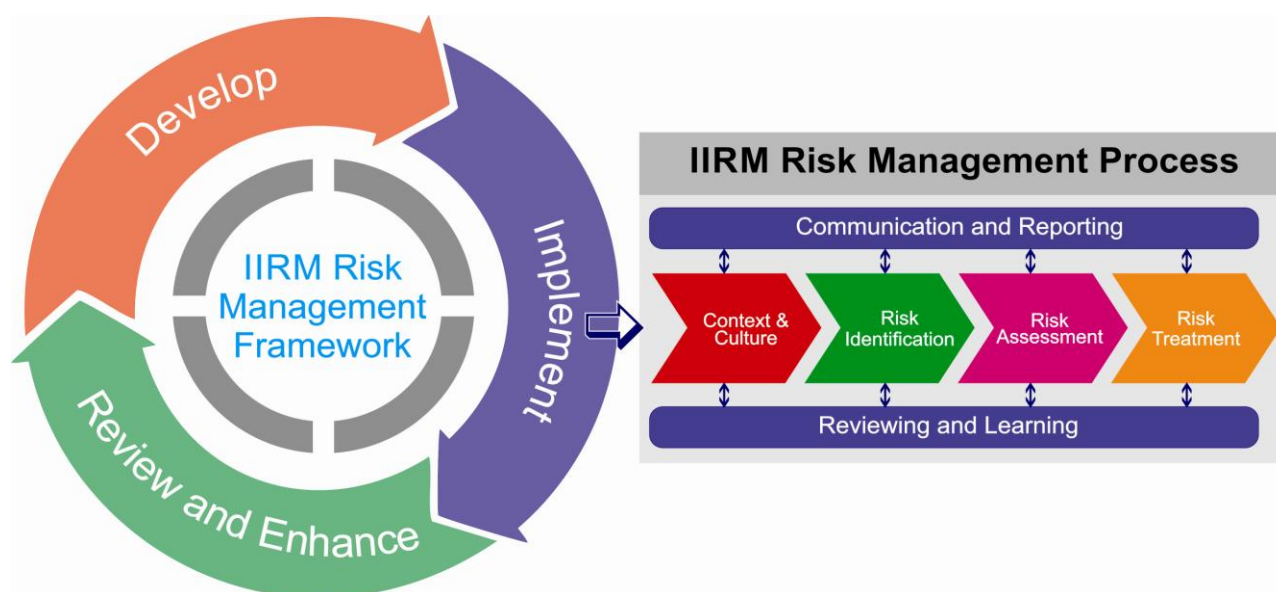
The key elements of the IIRM risk management framework are as follows:

1. Develop a risk management framework
2. Implement a risk management framework
3. Review and enhance a risk management framework

Linking risk management with other processes

Risk management is not a stand-alone discipline. To maximise risk management benefits and opportunities, it needs to be integrated with existing business processes. The following section lists some of the key business processes with which risk alignment is necessary.

2

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk management framework
2.3   Documenting a risk management framework
2.4   Risk management governance
2.5   Risk management information systems

Internal audit

Internal audit reviews the effectiveness of controls. Alignment between the internal audit function and that of the controls within the risk management process is critical, and the role/s of the risk and compliance/ internal audit manager will seek to align these core processes.

The requirement to follow a risk-based approach to internal audit planning means that risk management outputs, particularly risk assessment outcomes and risk profiles, need to be available as an input to the internal audit function.

Similarly, internal audit plays a critical role in the risk management process, specifically in identifying and assessing operational risks, as well as providing assurance that specific risk controls are well designed and are operating effectively.

Business planning (including budgeting)

Identifying risks during the business planning process allows realistic delivery timelines to be set for strategies/ activities or the choice of removing a strategy/ activity if the associated risks are too high or unmanageable. The impact of changing risk levels over the year/s can then be mapped to the relevant objective, enabling organisations to conduct more timely expectation management with key stakeholders.

Performance management

Individual performance plans should include all risk responsibilities whether a general responsibility to use the risk management process or specific responsibilities such as risk ownership or implementation of risk treatments.

Linking strategic planning and risk

Risk management is a process that aims to enhance an organisation's ability to meet its strategic and operational objectives. Equally, risk management outputs provide boards, executives and management with valuable insights and information that support improved decision-making and planning.

To maximise the benefits of risk management, it is important that risk management processes be integrated as closely as possible into existing strategic planning and operational processes.

Strategic and operational planning is about the formulation, implementation and evaluation of cross-functional decisions that will enable the organisation to achieve its objectives. Risk management is designed to identify, assess, treat, review and report those risks that have been identified from strategic and operational planning processes which could prevent the achievement of its objectives.

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk management framework
2.3   Documenting a risk management framework
2.4   Risk management governance
2.5   Risk management information systems

Incorporating risk management within projects

Projects can be distinguished from normal business processes by the fact that projects have the following:

- A defined start and end date
- A clearly documented set of deliverables or outputs that need to be delivered on time, within an agreed budget and in accordance with pre-defined quality criteria for the project to succeed
- Project success criteria, budgets and accountabilities that are defined and agreed before the project commences.

Many of the principles of project management are now being applied to on-going business processes to improve accountability, monitoring and business performance.

When establishing your organisational risk framework, consider:

- Including project management risk as a category of risk against which you report
- Whether all project risks are reported in the organisational risk register or whether the project/ program manager should maintain a separate risk register per project, with only strategic or extreme risks being incorporated into the main risk register, and project risk profiles being reported to the project steering committee
- Establishing customised Likelihood and Consequence scales for major projects. A cost overrun of 100% of a project budget may be extreme within the context of the project but only moderate or low within the broader organisational context. Similarly, many organisations use project-specific consequence descriptors, such as the following:

    - ❖ Time (timeframes exceeded)
    - ❖ Cost (budget overruns)
    - ❖ Quality (project does not deliver pre-defined quality/ functionality criteria)
    - ❖ Reputation (adverse publicity, laws breached etc.)

Frequency of reporting on project risk

Typically more frequent than organisational risk updates and reporting, it is common for risk updates to be provided to the steering committee whenever it meets.

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk management framework
2.3   Documenting a risk management framework
2.4   Risk management governance
2.5   Risk management information systems

2.2 Key considerations when developing a risk management framework

Before developing or revising a risk management framework, the organisation should critically review and assess those elements of the risk management process that are already in place.

Some of the key questions that need to be answered are:

- How advanced should the risk management framework be?
- How effective are current risk management practices?
- What is the most effective and efficient way of closing the gap?

These questions are explored in further detail in the following sections.

How advanced should a risk management framework be?

An organisation's risk management framework should ensure that key risks are effectively identified and responded to in a manner that is appropriate to the organisation.

No single risk framework will be appropriate for all organisations. Every organisation's board and executives should decide on the appropriate level of risk management sophistication that they aspire to achieve. The desired level of risk maturity may change over time to reflect changes in the organisation's complexity, size and risk appetite.

Some external and internal factors would need to be considered to determine the appropriate level of risk management maturity. Some of the most important factors are discussed in the following sections.

Context for Risk Management

External Environment

Political
Economic
Social
Technological
Legal
Environmental

Understanding the Context for Risk Management

Internal Environment

Strategies
Objectives
Capabilities
Processes
Structure
Systems
Culture

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk management framework
2.3   Documenting a risk management framework
2.4   Risk management governance
2.5   Risk management information systems

How effective are current risk management practices?

When reviewing the effectiveness of current risk management practices, it is necessary to consider both the "hard" and the "soft" aspects of risk management. The two key questions that need to be answered are as follows:

1. Are the current risk management practices and framework "fit-for-purpose" given the organisational context (e.g. objectives, size, complexity, structure, culture, risk appetite etc.)?
2. Are they operating as anticipated (i.e. do people do what they are expected to do)?

Towards organisation-wide risk management

There are many names to describe the approach used when looking at all risks across a company, organisation or entity. Such an approach can be referred to as enterprise-wide, the whole of the entity, organisation-wide, holistic, integrated, etc.

In general, organisation-wide risk management is the risk management practices that aim to look at all risk across a company, organisation or entity. There are many competing definitions and several frameworks that attempt to define organisation-wide risk management, but there is no universally accepted definition or standard. This is probably because organisation-wide risk management, in practice, differs depending on the background of the practitioner, the size and nature of the company, and the time at which organisation-wide risk management was adopted.

Holistic risk management approach

Organisation-wide risk management is a holistic approach to managing and prioritising responses to critical risks across the organisation in a manner that will support business strategy and plans. Effective risk assessment essentially consists of risk identification and evaluation across all areas of the organisation, followed by a process to ensure that critical risks are treated and managed in accordance with the organisation's risk appetite.

Organisation-wide risk management seeks to provide a consolidated view of risk across the organisation. The scope of organisation-wide risk management, therefore, encompasses the use of common risk language, risk assessment techniques and response strategies across all functional and risk/assurance functions within the organisation, such as the following:

- occupational health and safety risk
- loss control and internal audit
- legal and regulatory compliance risk
- IT and information security
- clinical healthcare risk
- strategic risk

2.1	Overview – Risk management framework
2.2	**Key considerations when developing a risk management framework**
2.3	Documenting a risk management framework
2.4	Risk management governance
2.5	Risk management information systems

DEVELOPING A RISK MANAGEMENT FRAMEWORK

While physical hazards and financial management represent significant sources of risk for most organisations, other risk areas such as operational and strategic are often neglected. For many organisations, strategic and operational risks may be the greatest threat to achieving strategic objectives and meeting stakeholder expectations.

For example, misaligned products, supplier problems and cost overruns all indicate that organisations need to pay increased attention to identifying and managing their strategic and operational risks. This will assist in achieving objectives and delivering on stakeholder expectations.

Public and private sector organisations are increasingly adopting organisation-wide risk management frameworks that provide a holistic approach to identifying, assessing, managing, monitoring and prioritising responses to all critical risks across the organisation in a manner that supports business strategies and plans. The chart below illustrates the key attributes of an organisation-wide risk management framework.

Traditional Risk Management	Organisation-wide Risk Management
• Emphasis on protecting assets • Focus on physical and financial assets • Risks managed within functional silos • Inconsistent approaches	• Board/executive support of risk management • Clear accountabilities • Appropriate risk oversight structures • Dedicated risk management coordinator • Explicit consideration of both operational and strategic risks • Risk management integrated with operational and general management processes • Clear accountabilities and timeframes for treatment of risks • Differentiated risk reporting tailored to specific stakeholders • Regular reviews of risk and risk management processes

Optimising risk management maturity

When determining an organisation's desired risk management maturity, the objective should be to maximise the value created through the risk management framework and practices.

The value of risk management can be defined as follows: Value = Benefits – Costs

The cost side of the equation is normally relatively easy to quantify and will include:
- direct costs associated with increasing the maturity of the organisation's risk management framework, as well as the direct costs associated with maintaining the desired level of risk management maturity
- indirect costs associated with increased focus on risk management activities. These will effectively be the opportunity costs associated with the additional time spent on risk management activities by management and staff.

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk management framework
2.3   Documenting a risk management framework
2.4   Risk management governance
2.5   Risk management information systems

The benefits of risk management are often harder to quantify. Some of the benefits typically achieved by organisations with "advanced" risk management practices include:

- appropriate balance between realising opportunities for gains while minimising losses
- opportunities for gains while minimising losses
- better corporate governance, including risk oversight
- improved decision-making and facilitating continuous improvement in performance
- organisations that manage risk effectively and efficiently are more likely to achieve their objectives and do so at overall lower cost

Key observations:

- Targeted risk management maturity will differ for each organisation depending on a range of internal and external considerations as outlined above.
- The value of increasing an organisation's risk management maturity will increase as long as the benefits exceed the costs. However, the increase in value is not linear. For example, the value of shifting an organisation's maturity from basic to mature is normally higher than from shifting from mature to advanced. This is because most organisations can move from basic to mature without spending significant resources while the benefits are likely to be significant. Moving from mature to advanced is more expensive, as it typically requires significant investments in software and other infrastructure, as well as significant time commitments by management and staff.
- Improving risk management maturity requires time and resources. Time can to some extent be substituted by increased focus/effort. Accordingly:
  a. An organisation with limited resources and low risk management commitment would take a very long time to reach the desired level of risk management maturity.
  b. Organisations with extensive resources and strong commitment to rapidly enhancing their risk practices may be able to shorten the time required to reach their desired level of risk management maturity.
- Improving risk management maturity requires balanced enhancement.
- Developing a proactive risk management culture and embedding/integrating risk management practices in business processes always takes time.

What is the most effective and efficient way of closing the gap?

Once the organisation has taken a critical look at the effectiveness of its current risk management practices and determined an appropriate level of risk management maturity, it needs to determine how to get there.

Developing a plan

The likelihood of successfully enhancing the maturity of your risk management framework to the desired level increases dramatically if you plan it well. The best way to do this is often through the development of a formal risk management strategy or plan, and associated risk policy and procedure documents. This will outline how the

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk management framework
2.3   Documenting a risk management framework
2.4   Risk management governance
2.5   Risk management information systems

organisation intends to achieve its targeted level of risk management maturity while clarifying the responsibility and processes for achieving risk management goals.

Avoiding the common pitfalls

Common areas where organisations struggle to embed risk management include:

- ensuring business planning is integrated with risk management
- better definitions of risk
- improving identification of risks
- aligning risk committee and board with what is happening on the ground
- linking internal audit and risk management
- improving the quality and content of risk registers
- embedding operational risk management
- identifying controls and their effectiveness
- allocating accountability for risk
- improving risk reporting and measurement
- project risk management

Characteristics of high achievers

- commitment from the executive and board
- integration of risk and corporate planning processes
- well defined governance framework
- strong reporting processes
- risk support systems, processes and infrastructure for managing risk
- clearly defined roles and responsibilities
- a strong risk culture

Public Sector Challenges

There are many challenges in implementing a successful organisation-wide risk framework. Some of the most compelling are:

- competing objectives of delivering more with less
- risk compliance often competes with "risk culture"
- public sector risk management expertise
- the public and private sectors are becoming more connected, requiring a whole-of-government approach to risk management
- attaining risk maturity is a long road.

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk
         management framework
2.3   Documenting a risk management framework
2.4   Risk management governance
2.5   Risk management information systems

To those that overcome the challenges, some of the benefits to be reaped include:

- strengthened corporate governance processes
- improved controls assurance
- more informed decisions aligned to the delivery of objectives
- a source of competitive advantage
- improved shareholder/stakeholder value

DEVELOPING A RISK
MANAGEMENT FRAMEWORK

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk
       management framework
2.3   Documenting a risk management framework
2.4   Risk management governance
2.5   Risk management information systems

2.3 Documenting a risk management framework

Documenting an organisation's risk management framework and recording each step of the risk management process is critical for a number of reasons, including:

- demonstrating to stakeholders that the process has been conducted properly
- providing evidence of a systematic approach to risk identification and analysis
- enabling decisions or processes to be reviewed
- providing a record of risks and developing the organisation's knowledge database
- providing decision-makers with a risk management plan for approval and subsequent implementation
- providing an accountability mechanism and tool
- facilitating on-going monitoring, review and continuous improvement
- providing an audit trail
- sharing and communicating information

What needs to be documented?

The following areas of an organisation's risk management framework need to be documented:

- objectives and rationale for managing risk
- accountabilities and responsibilities for managing and overseeing risks
- processes and methods to be used for managing risks – i.e. how the IIRM Risk Management process will be applied in the organisation
- commitment to the periodic review and verification of the risk management framework and its continuous improvement
- the way in which risk management performance will be measured and reported
- resources available to assist those accountable or responsible for managing risks
- organisation's risk appetite translated into risk-rating criteria
- links between risk management and the organisation's strategic and operational objectives
- links between risk management and other processes and activities
- scope and application of risk management within the organisation
- requirements for recording and documenting the risk management process (e.g. communications plan, stakeholder analysis, risk register, risk profile, and risk reporting).

Is there a preferred way to structure the documentation?

There is no preferred way for organisations to structure their risk management framework documentation but the following may be included in a risk framework:

- Objectives
- Mandate and commitment to manage
- Operational policies
- Procedures and practices
- Risk management plan/s and allocation of responsibilities.

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk management framework
2.3   Documenting a risk management framework
2.4   Risk management governance
2.5   Risk management information systems

Some organisations may include all of the above components into a single plan, or they may create separate policy, procedure and plan documents. As long as the required areas of the framework have been documented, it is up to the organisation to select an appropriate document structure.

An example of how key framework elements might be documented is shown below:

Risk Management Framework Documentation		
Risk Management Plan	**Risk Management Policy**	**Risk Management Procedure**
➢ Intentions and direction	➢ Scope of risk management	➢ Detailed roles and responsibilities
➢ Risk management purpose/objectives	➢ Strategy and approach	➢ Detailed description of process steps
➢ Key roles & responsibilities	➢ Resources	➢ Risk rating scales
➢ Risk management governance arrangements	➢ Procedures	➢ Risk reporting templates
➢ Procedures	➢ Responsibilities	➢ Risk management activities
	➢ Sequence and timing of activities	
	➢ Roadmap for enhancement of risk management practices	

The framework documents typically include, or are accompanied by, detailed documentation such as:

- charters for the board, board audit committee, board risk committee, executive committee, internal audit function, etc
- position descriptions describing risk responsibilities
- risk management tools, templates and guidelines
- risk management training schedule/s
- risk register/s
- operational plans for risk treatment
- risk management reports

The indicative content of core risk management framework documentation is included in the following sections.

Risk management strategy

A risk management strategy typically documents factors such as:

- objectives and rationale for managing risk
- the organisation's overall appetite/tolerance for risks
- the organisation's strategic objectives and the strategies deployed to achieve these objectives
- key risks associated with these strategies within a one-to-three-year timeframe

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1 Overview – Risk management framework
2.2 Key considerations when developing a risk management framework
2.3 **Documenting a risk management framework**
2.4 Risk management governance
2.5 Risk management information systems

- the organisation's high-level approach to managing these risks
- a plan for progressive enhancement of the organisation's risk management practices and competencies, including key risk management initiatives.

The following key questions would need to be answered in the process of formulating a risk management strategy:

- what are the organisation's key objectives and strategies?
- what are the risks associated with these?
- how is the organisation assessing, managing and monitoring these risks?
- are the risk management processes working effectively?

There is no prescribed format for how a risk management strategy should be documented.

- some organisations disclose their risk management strategy in their annual reports
- some organisations chose to have a separate document, in addition to a risk management policy and procedure document
- some organisations incorporate their risk management strategy within their Business Plan, outlining how risks associated with business plan objectives will be managed.

Risk management policy

The risk management policy should clearly articulate the organisation's objectives for and commitment to risk management. The policy typically specifies:

- accountabilities and responsibilities for managing risk
- commitment to the periodic review and verification of the risk management policy and framework, and its continuous improvement
- links between this policy and the organisation's objectives
- the organisation's risk appetite
- the organisation's rationale for managing risk
- processes and methods to be used for managing risk
- resources available to assist those accountable or responsible for managing risk
- the way in which risk management performance will be measured and reported.

Risk management procedures

The risk management policy is typically supported by a more comprehensive risk management procedure document outlining the organisation's detailed approach to managing risk.

Typical contents of the risk management procedure include:

- Risk management definitions/language – a common risk language will promote a consistent understanding of risk management concepts and provide clarity of communication and action.

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk management framework
2.3   Documenting a risk management framework
2.4   Risk management governance
2.5   Risk management information systems

- Risk management roles and responsibilities – an organisation's ability to conduct effective risk management is dependent upon having an appropriate risk governance structure and well-defined roles and responsibilities.
- Relationship and integration with other initiatives – risk management is not a stand-alone discipline. Risk management needs to be integrated with existing business processes to maximise its benefits and opportunities
- Description of how each step of the risk management process will be applied within the organisation
- Overview of risk reporting framework – content, format, frequency and recipients of risk reports
- Risk assessment criteria – agreed criteria for assessment of risk likelihood, consequence, and overall risk rating.

Is it acceptable to combine risk management policy, strategy, and procedures into a single risk management plan or manual?

Many organisations have successfully combined these into one document. As long as the right areas are documented, it is reasonable to maintain them as one document.

Risk register

A risk register is a comprehensive record of all risks across an organisation, business unit or project depending on the purpose/context of the register.

Risk register content

At a minimum, the risks register records:
- the risk
- how and why the risk can occur
- the existing internal controls that may minimise the likelihood of the risk occurring
- the likelihood and consequences of the risk to the organisation, business unit or project
- a risk-level rating based on pre-established criteria
- a framework, including an assessment of whether the risk is acceptable or whether it needs to be treated
- a clear prioritisation of risks (risk profile)
- accountability for risk treatment (may be part of the risk treatment plan)
- the timeframe for risk treatment.

Risk register format

Risk registers may take various forms, including:
- Excel/Word-based
- risk management software/system.
    I.   Internally developed
    II.   Externally developed

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk
       management framework
2.3   Documenting a risk management framework
2.4   Risk management governance
2.5   Risk management information systems

DEVELOPING A RISK MANAGEMENT FRAMEWORK

Risk treatment plans

Risk treatment plans identify responsibilities, schedules, the expected outcome of treatments, budgets, performance measures and the review process to be put in place.

The risk treatment plan usually provides details on:

- actions to be taken and the risks they address
- who has responsibility for implementing the plan
- what resources are to be utilised
- the budget allocation
- the timetable for implementation
- details of the mechanism and frequency of review of the status of the treatment plan

Risk and risk management reports

Regular reports should be made available to executive management, boards and audit committees explaining how key risks are being managed.

Some of the basic questions that risk reports should answer include the following:

- what are the risks?
- what is the level of each risk?
- what has been done about them?
- who is responsible for managing the risk?
- has the level of risks changed as a result of implementing risk treatments?
- what are the risks that need to be escalated to strategic risks?
- what are the risks that are no longer regarded as strategic risks and why?

DEVELOPING A RISK
MANAGEMENT FRAMEWORK

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk
       management framework
2.3   Documenting a risk management framework
2.4   Risk management governance
2.5   Risk management information systems

2.4 Risk management governance

An organisation's ability to conduct effective risk management is dependent upon having an appropriate risk management governance structure and well-defined roles and responsibilities.

It is important for everyone to be aware of individual and collective risk management responsibilities. For risks to be effectively managed, it is essential that people behave in a way that is consistent with the organisation's approved approach.

This indicates that risk management is not merely about having a well-defined process but also about facilitating the behavioural change necessary for risk management to be embedded in all organisational activities.

Mandate and commitment

Any major organisational initiative needs appropriate sponsorship to be successfully implemented and sustained. Given its importance and strategic nature, risk management requires strong and sustained commitment by the organisation's board, audit/risk committee, and the CEO / Secretary.

Management should:
- articulate and endorse the risk management policy
- communicate the benefits of risk management to all stakeholders
- define risk management performance indicators that are aligned with organisational performance
- ensure alignment of risk management objectives with the objectives and strategies of the organisation
- ensure legal and regulatory compliance
- ensure that the necessary resources are allocated to risk management

The board, risk committee and executive can all play a leading role in setting the tone for effective risk management throughout the organisation. This can be demonstrated in a number of ways but it is often achieved through the authorisation and sponsorship of key risk management documentation that outlines both the 'why' and the 'how' behind effective risk management.

The board, risk committee and executive can also help to drive effective risk management by incorporating risk management and reporting into the corporate and strategic planning processes, thereby setting an example on how it can be incorporated into normal operations.

Accountability

The organisation should ensure that there is accountability and authority for:
- managing risks
- adequacy and effectiveness of risk controls
- implementing and sustaining the risk management framework/process

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk management framework
2.3   Documenting a risk management framework
2.4   **Risk management governance**
2.5   Risk management information systems

This may be facilitated by:

- ensuring appropriate levels of recognition, reward, approval, and sanction
- establishing performance measurement and internal and/or external reporting and escalation processes
- specifying risk owners for implementing risk treatments, maintenance of risk controls and internal reporting of relevant risk information
- specifying who is accountable for the development, implementation and maintenance of the framework for the management of risk.

What are the key factors to consider when developing a risk management governance structure?

A number of factors should be considered when determining an organisation's risk management governance structure, including:

- current organisational structure and authorities
- the current level of understanding, appreciation, and commitment to risk management by key individuals
- the current level of change readiness within the organisation (often evolutionary change works better than revolutionary change)
- key types of risks faced by the organisation and functions currently managing the key risks
- the existence of logical "risk champions" within the organisation.

Indicative roles and responsibilities for risk management

Proactive communication and dialogue with the board and audit/risk committee is a critical element of effective risk management governance. The board and its committees retain an obligation to remain informed not only of the risks to the organisation but also of the effectiveness of risk management efforts. The board and the audit/risk committee have a responsibility to the stakeholders of the organisation to ensure that the risk management framework of the organisation is appropriate to the nature of the organisation and the risks the organisation faces.

A key component of effective risk management governance is to establish clear lines of risk and risk management accountability. The specific roles of the various parties such as the board, audit/risk committee, the CEO/Secretary, executive management, and staff will vary according to the organisational structure, complexity, size and maturity. A sample risk governance structure is illustrated as follows:

The roles and accountabilities of each of the key parties to whom risk management duties have been delegated are as follows:

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk management framework
2.3   Documenting a risk management framework
2.4   **Risk management governance**
2.5   Risk management information systems

Board

The board provides direction and oversight of risk management across the organisation. The board's key risk management responsibilities may include:

- approving the organisation's risk management documentation including the strategic risk profile, risk appetite and tolerance, risk management policy and risk management procedure
- setting the standards and expectations of the organisation with respect to conduct and behaviour, and ensuring that effective risk management is enforced through an effective performance management system
- monitoring the management of high and significant risks, and the effectiveness of associated controls through the review and discussion of risk management reports
- satisfying itself that risks with lower ratings are effectively managed, with appropriate controls in place and effective reporting structures
- approving major decisions affecting the organisation's risk profile or exposure.

Chief Executive Officer (and Secretary)

The CEO's / Secretary's key risk management responsibilities may include:

- participating in the review and update of the strategic risk profile
- reviewing key risk information, identifying key risk trends and assessing the impact for the organisation as a whole
- monitoring the management of high and significant risks and the effectiveness of associated controls through the review and discussion of regular risk management reports
- ensuring that adequate processes are being followed about lower-level risks
- setting the tone and promoting a strong risk management culture by providing a firm and visible support for risk management.

Audit /risk committee

The audit /risk committee is accountable to the board, and meets and reports to the board advising of its activities, findings and recommendations, including risk management policies.

The primary objective of the audit / risk committee is to assist the board in discharging its responsibilities to exercise due care, diligence and skill in relation to business operations and to advise on any matters of financial or regulatory significance which may be referred to it from time to time.Also, the committee is to assist the board in fulfilling its responsibilities relating to compliance by the organisation with legal and contractual obligations.

The organisation may also choose to have an executive risk management committee to promote the coordination and oversight of risk management activities.

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk management framework
2.3   Documenting a risk management framework
2.4   **Risk management governance**
2.5   Risk management information systems

Executive and management

The executive and management are responsible for the oversight of the risk management framework, including the consideration and review of risk management policies and procedures on an annual basis. The executive and management are also responsible for establishing policies and reviewing the effectiveness of the organisation's approach to risk management including the status of major business risks.

The typical composition of an executive risk management committee would be:

Core Members:

- CEO
- Risk Manager
- Chief Financial Officer
- Operations Manager
- Internal Auditor
- Occupational Health and Safety Officer

Optional Members:

- Human Resources Manager
- IT Manager
- Legal Counsel
- Other functional specialists

Chief risk officer /risk manager

It is important to note that most 'risk managers' act primarily as advisors and coordinators for risk and do not typically have a direct operational responsibility for specific categories of risk.

Operational responsibility for specific types of risk generally rests with functional area line management. For example, an IT and Systems Manager would take responsibility for managing IT-related risk/s. Some organisations create a risk management job role that incorporates operational responsibility for a particular risk area. For example, the Risk Manager may also act as the organisation's OH&S Officer.

Chief risk officers, risk managers (or equivalent) are typically employed to:

- develop, enhance and implement appropriate risk management policies, procedures and systems
- co-ordinate and monitor the implementation of risk management initiatives within an organisation
- work with risk owners to ensure that the risk management processes are implemented in accordance with agreed risk management policy and strategy
- collate and review all risk registers for consistency and completeness
- provide advice and tools to staff, management, the Executive and Board on risk management issues within the organisation, including facilitating workshops in risk identification

19

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1 Overview – Risk management framework
2.2 Key considerations when developing a risk management framework
2.3 Documenting a risk management framework
2.4 Risk management governance
2.5 Risk management information systems

- promote understanding of and support for risk management, including delivery of risk management training
- oversee and update organisational-wide risk profiles, with input from risk owners
- ensure that relevant risk information is reported and escalated or cascaded, as the case may be, in a timely manner that supports organisational requirements
- attend risk committee or audit committees where risk management issues are discussed
- ensure that, regardless of the job title or function, there is clarity about roles and responsibilities to progress risk management throughout the organisation.

Risk owners

Risk owners are typically line managers or functional specialists who assume responsibility for designing, implementing and/or monitoring risk treatments.

Risk owners may be responsible for the following:

- managing the risk for which they have accountability
- reviewing the risk on a regular basis
- identifying where current control deficiencies may exist;
- updating risk information about the risk
- escalating the risk where the risk is increasing in likelihood or consequence
- providing information about the risk when it is requested.

Staff and contractors

It is the responsibility of all personnel, stakeholders and contractors to apply the risk management process to their respective roles. Their focus should be on identifying risks and reporting these to the relevant risk owner. Where possible and appropriate, they should also manage these risks.

2.1	Overview – Risk management framework
2.2	Key considerations when developing a risk management framework
2.3	Documenting a risk management framework
2.4	Risk management governance
2.5	Risk management information systems

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.5 Risk management information systems

Developing a risk management framework involves identifying the appropriate tools and technology that will help the organisation capture, analyse and communicate risk-related information.

The objective is to provide the right information to the right people at the right time to make appropriate decisions with regard to risks.

In general, risk management information systems should possess the capability to:

- record details of risks, controls and priorities and show any changes within
- record risk treatments and associated resource requirements
- record details of incidents and loss events and the lessons learned
- track accountability for risks, controls and treatments
- track progress and record the completion of risk treatment actions
- allow progress against the risk management plan/strategy to be measured
- trigger monitoring and assurance activity.

This section provides guidelines for identifying suitable tools and technology to enable your risk management framework.

Identifying your requirements

The first step in the process of managing risk information is to identify your requirements. The key questions to ask are:

- What risk information or data do you need to capture?
- How do you capture this risk information?
- Who are your end-users and what do they need?

The requirements will generally involve capturing risk data, monitoring and recording risk information, developing the capability to analyse and report risk performance, and communicating relevant and timely risk management information to the right stakeholders.

Developing appropriate tools and technology

Developing the appropriate tools and technology according to the requirements will generally depend on the scale and scope of the risk management framework as well as the stakeholders involved. For instance, who are the users of the tools and technology? To which parts of the business will the tools and technology be applied?

Choose the appropriate tools that provide comprehensive, relevant, timely and accurate risk information. This will facilitate better and more informed decision-making.

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1 Overview – Risk management framework
2.2 Key considerations when developing a risk management framework
2.3 Documenting a risk management framework
2.4 Risk management governance
2.5 Risk management information systems

An organisation may find that the costs associated with acquiring and maintaining software exceeds the benefits. In such circumstances, it is probably preferable to invest these resources in improving other areas of risk management – e.g. to fund critical risk treatments/controls, or to train staff.

Capturing risk information

To effectively identify risks, it will be useful to have tools that capture risk information from various sources across the organisation, including:

- leadership team
- business unit managers
- selected staff
- other stakeholders

Your tools and technology should be able to capture typical risk management information, including:

- actual losses, potential losses, and near-miss events
- business risk profile, including new and changed exposure to key risks
- significant control weaknesses, (which affect significant risks)
- progress on action plans to deal with significant risk or control weaknesses

Monitoring and recording risk information

Many organisations use tools and technology with functionality to generate risk reports with information about:

- extreme risks
- the total risk profile
- reasons for risk rating movements
- risk treatment actions
- assurance coverage of key risks
- risk management strategy
- new and emerging risk issues
- detailed risk register

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk management framework
2.3   Documenting a risk management framework
2.4   Risk management governance
2.5   Risk management information systems

Capability to analyse and report risk performance

To effectively analyse and report risk performance, one will need tools and technology that:

- analyse risks based on quantitative or qualitative parameters
  - ❖ qualitative risk analysis will require tools that have the capability to classify risks, according to categories, impact and likelihood.
  - ❖ quantitative risk analysis will require tools that have the capability to calculate and/or simulate value of risk.
- facilitate ranking or prioritisation of risks
- facilitate trend analysis
- aggregate risk information at various levels as required by different levels of staff/management.

Communicating risk management information

Effective communication facilitates awareness, understanding, and adoption of and commitment to the risk management framework.

The communication tools you will require should ideally have the capability to:
- provide easy reporting of and access to risk information for all relevant stakeholders
- archive lessons learned from implementing the risk management framework
- store risk management policies, procedures and other documents
- trace user access to determine reach utilisation
- provide an audit trail to ensure the integrity of information
- enable escalation of risk-related issues and incidents.

Selecting your risk management software

Depending on factors such as size and complexity of an organisation and the nature of the risks it manages, it may be feasible to acquire or develop risk management software to facilitate the recording, analysis and reporting of risk management information.

The key areas to consider when assessing an organisation's need for risk management software are:

- costs
- functionality
- accessibility
- scalability

Various risk management systems that meet different requirements are available in the market. As a guide, consider the following in choosing the most suitable option.

DEVELOPING A RISK MANAGEMENT FRAMEWORK

2.1   Overview – Risk management framework
2.2   Key considerations when developing a risk management framework
2.3   Documenting a risk management framework
2.4   Risk management governance
2.5   Risk management information systems

Costs

Determine the costs associated with the software. How much does the licence cost? Ensure that you understand the software's licencing conditions.

Functionality

What functions does the software provide? Does it meet all your requirements?

Accessibility

Does the software allow users to access it easily, anytime, anywhere, as and when required? Does it provide control of access to ensure the integrity of risk management information?

Scalability

Does the software allow the expansion of user/s and functions without significant additional costs? If you expand the scope of your risk management framework, will the software still be applicable?

IMPLEMENTING A RISK
MANAGEMENT FRAMEWORK

3.1   Overview of the risk management process
3.2   Context and culture
3.3   Risk identification
3.4   Risk assessment
3.5   Risk management
3.6   Communication and reporting
3.7   Reviewing and learning

3 Implementing a risk management framework

3.1 Overview of the risk management process

This section provides an overview of how a risk management process consistent with that outlined in the guide might be implemented across an organisation. It also provides guidance on the process and content of risk and risk management reporting and outlines a practical approach to developing a proactive risk management culture.

The key steps in implementing a risk management process are illustrated in the following figure:

As depicted in the figure above, reviewing and reporting, and communication and learning are on-going activities that occur at each stage in the risk management process. Accordingly, these activities are discussed both as separate risk management process steps and as sub-activities of each of the other risk management process steps (i.e. Risk Context and Culture, Risk Identification, Risk Assessment and Risk Treatment).

The subsequent sections will describe each of the steps in the risk management process in detail.

The sections aim to answer the following questions:

1.   what is the purpose of each step in the process?
2.   why is it important?
3.   how do you implement it?
4.   how do you communicate /learn /review and report?
5.   what tools and techniques are used to implement it?
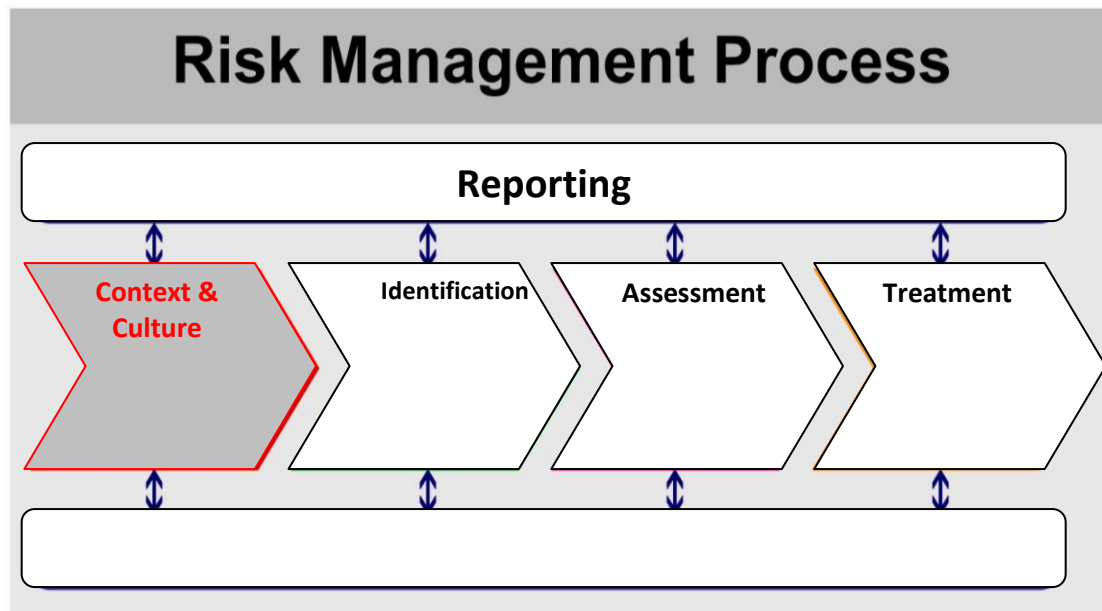
3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk management
3.6 Communication and reporting
3.7 Reviewing and learning

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

The following table summarises the key risk management processes, the input, output tools and techniques.

	Context & Culture	Risk Indetification	Risk Assesment	Risk Treatment

INPUT	• External Context
	  – external environment information
	• Internal Context
	  – organisational information
		• Stake holder consultation
		• Organisational records
			• Risk rating criteria
			  – likelihood rating
			  – consequence rating
			• Risk tolerance
				• Treatment Options
				• Risk Ownership

OUTPUT	• Risk Criteria
	• Risk Tolerance
	• Risk Management Policy
	• Risk Management Framework
		• Risks that matter
		• Risk Register
			• Likelihood of risks
			• Consequence of risks
			• Current controls around risks
			• Overall risk rating
			• Risk profile
			• Risk priorities
			• Inter-relationship among the risks
				• Treatment plan:
				  – to reduce likelihood
				  – to reduce consequence
				  – to maximise upside risks
				• Resources and timeframe

TOOLS AND TECHNIQUES	• Stakeholder consultation plan • Communication plan	• Brainstorming • "What-if" and scenario analysis • Process mapping & flowcharting • Systems analysis • Operational modelling • Expert opinion	• Qualitative analysis • Semi-quantitative analysis • Quantitative analysis • Heat map • Numerical ranking of risks • Decision trees	• Risk transfer, i.e. insurance, outsourcing • Risk mitigation • Risk avoidance • Cost-benefit analysis

www.iirmglobal.com

IMPLEMENTING A RISK
MANAGEMENT FRAMEWORK

3.1   Overview of the risk management process
3.2   Context and culture
3.3   Risk identification
3.4   Risk assessment
3.5   Risk management
3.6   Communication and reporting
3.7   Reviewing and learning

3.2 Context and Culture

What is Context?

Establishing the context is concerned with understanding the background of the organisation and its risks, scoping the risk management activities being undertaken and developing a structure for the risk management tasks to follow.
Many of the internal and external parameters that constitute an organisation's context are similar to those considered when developing the risk management framework. However, when applied to the risk management process, they need to be considered in greater detail, in particular how they relate to each step of the risk management process.

How to establish the context

This process requires the following key steps:

- understand your external context
- understand your internal context
- develop your risk management context

Understand external context

The external context defines the external environment in which the organisation operates. It also defines the relationship between the organisation and its external environment.

3.1   Overview of the risk management process
3.2   Context and culture
3.3   Risk identification
3.4   Risk assessment
3.5   Risk management
3.6   Communication and reporting
3.7   Reviewing and learning

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

Understanding the external context is important to ensure that stakeholders and their objectives are considered when developing risk management criteria and that externally generated threats and opportunities are captured during the "risk identification" step.

Key elements of external context:

- Political, Economic, Social, Technological, Environmental and Legal , be they international, national or regional
- Key drivers and trends having an impact on the objectives of the organisation
- Perceptions and values of external stakeholders. It is particularly important to take into account the perceptions and values of external stakeholders and to establish policies to communicate with these parties.

Understand internal context

An understanding of the organisation is required before commencing any risk management activity, at any level. Understanding the internal context is important because:

- risk management takes place in the context of the goals and objectives of the organisation.
- the major risk for most organisations is that they fail to achieve their strategic, business or project objectives or are perceived to have failed by stakeholders.
- organisational objectives, policies, and processes help define the organisation's risk management policy, specific objectives and criteria of a project.

For risk management systems and processes to reflect each organisation's specific needs, the following steps should be taken prior to conducting formal risk identification exercises.

- Identifying key stakeholders who would need to be involved in risk management communication
- Defining risk categories to reflect the types of risk faced by the organisation
- Defining and approving risk criteria (risk rating scales) to be used when assessing and prioritising risks.

Key elements of internal context:

- Capabilities (e.g. capital, people, competencies, processes, systems and technologies)
- Information flows and decision-making processes
- Internal stakeholders
- Objectives and strategies in place to achieve them
- Perceptions, values and culture
- Policies and processes
- Standards and reference models adopted by the organisation
- Structures (e.g. governance, roles and accountabilities)

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk management
3.6 Communication and reporting
3.7 Reviewing and learning

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

Develop risk management context

After understanding the internal and external contexts, the next step is to develop the risk management context for an organisation. It is recommended that the following be taken into consideration when developing a risk management context:

- objectives and strategies for risk management
- scope, i.e. parts of the organisation in which you apply the risk management processes
- parameters for risk management activities
- resources required
- records to be established.

The outcome of this process is to ensure that the risk management approach adopted is appropriate and proportionate to the situation of the organisation and the risks affecting the achievement of its objectives.

Risk management context application:

Risk tolerance

Once the risk management context is understood and established, a key output of the process is risk tolerance. Risk tolerance is defined as …*an organisation's readiness to bear the risk, after treatments in order to achieve its objectives.*

Organisations are prepared to 'tolerate' some risks under certain circumstances in return for specified benefits. Tolerance levels may vary by context and are influenced by:

- the ability and willingness of the board and executive to take and manage risks
- the size and type of organisation
- the maturity and sophistication of risk management processes and control environments
- the financial strength of the organisation and its ability to withstand shocks
- the sector in which the organisation operates.

How to establish risk tolerance?

The typical steps involved in establishing and implementing risk tolerance are as follows:

1. Complete an analysis of the organisation's ability to physically and financially recover from a significant event (e.g. risk such as human influenza pandemic, loss of major plant or facility, inability to supply or manufacture product, loss of major business partner, credit crunch, etc).
2. The above analysis will highlight the need for and importance of contingency plans, financial, physical and human resources, and controls. From the analysis, determine the tolerance the organisation can bear or accept.

IMPLEMENTING A RISK
MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk management
3.6 Communication and reporting
3.7 Reviewing and learning

3. Management determines the level of tolerance that should then be endorsed by the board.

The risk tolerance levels set by the organisation will be reflected in the risk rating scales used to assess organisational risks.

How do you define risk tolerance levels?

Risk tolerance levels can be defined by dividing risks into a number of bands as appropriate for the organisation (four in this example):

- An upper band where adverse risks are intolerable, whatever benefits the activity may bring, and risk reduction measures are essential whatever their cost
- Middle bands where costs and benefits are taken into account and opportunities are balanced against potential adverse consequences
- A lower band where positive or negative risks are negligible, or the costs associated with implementing treatment actions outweigh the costs of the impact of the risk, should it occur.

These levels of risk tolerance will help determine the type and extent of actions required to treat risks and the level of management/board attention required to manage and monitor the risks. Risk tolerance levels can be practically defined through the colour coding of a risk likelihood/consequence matrix. This is illustrated in the following sample risk matrix (or heat map):

▦	Insignificant	Minor	Moderate	Major	Catastrophic
Almost certain	11	16	20	23	25
Likely	7	12 2	17	21 2	24
Possible	4	8	13 1	18 1	22 2
Unlikely	2	5 1	9	14	19 5
Rare	1	3	6	10	15 1

Risk management context application:

Risk criteria

Having established its risk tolerance, the organisation can now develop its risk criteria. The risk criteria take into consideration the risk management context. They are the basis on which risks are analysed and evaluated.

3.1   Overview of the risk management process
3.2   Context and culture
3.3   Risk identification
3.4   Risk assessment
3.5   Risk management
3.6   Communication and reporting
3.7   Reviewing and learning

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

Risk criteria express the organisation's values, objectives and resources. Some criteria may be imposed by, or derived from, legal and regulatory requirements. Risk criteria should be consistent with the organisation's risk management policy.

When defining risk criteria, factors to be considered should include the following:

- How likelihood will be defined
- How the level of risk is to be determined
- Nature and types of consequences that may occur and how they will be measured
- The level at which risk becomes acceptable
- The timeframe of the likelihood and/or consequence
- What level of risk may require treatment
- Whether combinations of multiple risks should be taken into account.

The following diagrams illustrate what risk criteria may look like and the key elements included.

Risk Criteria: Consequences / Impacts				
Rating / Description	Financial	Legal	Service Delivery	Safety
5 / Catastrophic	Loss over $5m	Extreme failure to comply with regulations and legislations	Outage of non-critical service for 1-2 weeks. Outage of critical service for less than one day	Single fatality or significant irreversible disability to more than two persons
4 / Major	Loss between $1m and $5m	Major failure to comply with regulations and legislations	Outage of non-critical service for 3-7 days	Significant irreversible disability to fewer than two persons or significant reversible disability to more than two persons
3 / Moderate	Loss between $200k & $1m	Serious failure to comply with regulations and legislations	Outage of non-critical service for 3-7 days	Significant reversible disability to fewer than two persons
2 / Minor	Loss between $100k & 200k	Minor legal issues. Non-complianceand/or breaches	Outage of non-critical service for 1-3 days	Minor medical attention required
1 / Insignificant	Loss less than $100k	Minor legal issues that would be easily resolved	Outage of non-critical service for less than 1 day.	First aid treatment only

Risk Criteria: Likelihood	
Rating / Description	Frequency
5 / Almost Certain	Expected to occur once a year or more frequently
4 / Likely	Expected to occur once every two years

IMPLEMENTING A RISK
MANAGEMENT FRAMEWORK

3.1   Overview of the risk management process
3.2   Context and culture
3.3   Risk identification
3.4   Risk assessment
3.5   Risk management
3.6   Communication and reporting
3.7   Reviewing and learning

3 / Possible	Expected to occur once every five years
2 / Unlikely	Expected to occur once every ten years
1 / Rare	Expected to occur once every 30 years

Control effectiveness criteria:

When analysing a risk, it is important to understand the effectiveness of current controls that are in place. Controls are systems, processes, policies etc. that are implemented to reduce risk levels, either by reducing the consequence of a risk if it does occur and/or to reduce the likelihood of the risk occurring.

Rating	Description
Good	Control is well designed for the risk and nothing more needs to be done except reviewing and monitoring. Control is effective and reliable all the time.
Satisfactory	Control is designed perfectly and is in place and effective. Some more work needs to be done to improve effectiveness. Management has doubts about the operational effectiveness and reliability.
Poor	The design of the control may be largely correct but it is not very effective. Or, control does not seem to be correctly designed and does not operate effectively
Very Poor	Control does not operate at all effectively
Uncontrolled	Virtually no credible control. Management has no confidence that any degree of control is being achieved due to poor design and/or very limited operational effectiveness

Periodic independent assurance is also needed to provide an objective view – based on the testing of controls – of the adequacy and effectiveness of the controls. Independent verification of control effectiveness can be sought from external and internal auditors.

What is risk management culture?

Culture is defined as "the way we work around here". It is the collective way of doing things, through accepted behaviours and processes.

A risk management culture specifically refers to the way risk management is applied in the way people work within an organisation. It is about the accepted ways of being and doing with regard to risk and risk management. Risk culture involves how people recognise and respond to risk and how risk is considered when making decisions.

Why is risk management culture important?

Culture is intrinsic to risk management. The accepted behaviour or norms around 'maximising potential opportunities while managing adverse effects' determines how embedded risk management is in your organisation. Hence, having an effective risk management process or framework in place means having an appropriate culture that works for your organisation. If risk management is not working, a change in culture may be necessary.

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk management
3.6 Communication and reporting
3.7 Reviewing and learning

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

The appropriate risk management culture will vary depending on the unique context of the organisation. To determine this, a starting point is to understand the key drivers of culture.
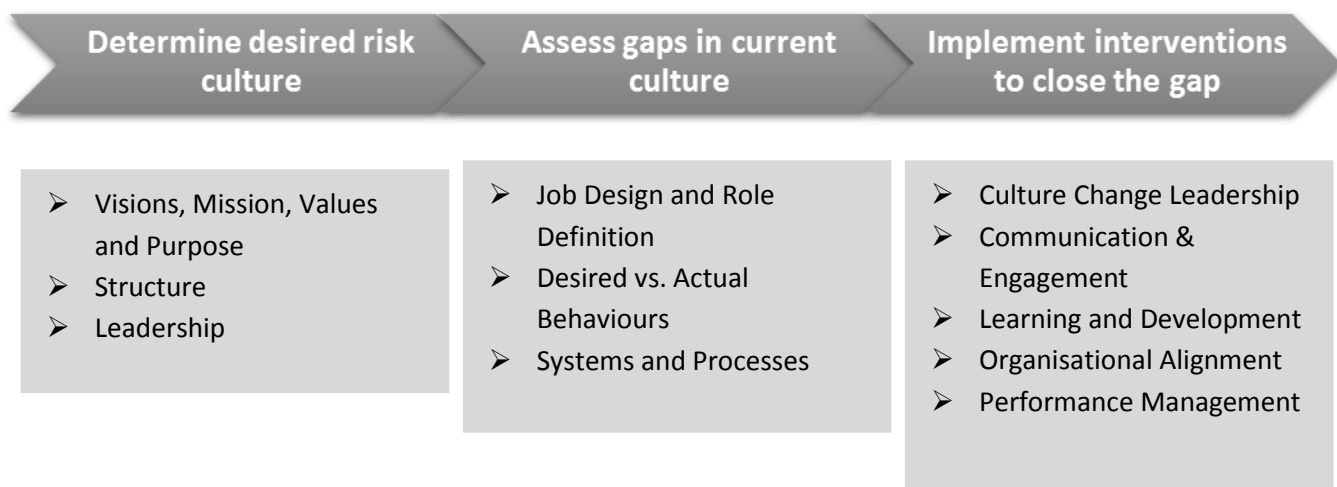
Drivers of culture

There are various drivers within an organisation that shape its culture. These drivers influence how well risk management is embedded throughout the organisation.

Cultural Drivers	Risk Management Culture
Mission, Vision, Values, Purpose	• Risks are managed on a day-to-day basis as part of applying the values of the organisation. • The mission, vision and purpose promote a risk culture
Systems and processes	• The management systems and processes enable effective and efficient risk management. • The process for managing risk is integrated with day-to-day processes
Structure	• There is a risk organisational structure to enhance accountability and delegation • The structure enables risk-based decision-making without bureaucracy, making jobs easier and delivering better outcomes
Leadership	• Leadership skills and attributes around risk management are fostered and rewarded and implemented across the business • Leaders do not tolerate poor behaviours or practices around risk management
Job Design and Role Definition	• Jobs are designed to reflect risk management and risk policies • Job definitions include performance expectations around risk management • Accountabilities with regard to risk and risk management are clearly articulated
Desired vs. Actual Behaviours	• There is a clearly articulated consensus around desired behaviours across the business • Leaders model these and people are responsive to these desired behaviours

Embedding desired risk management culture

Embedding your desired risk management culture is a journey of change. Managing change means shifting the organisation from where it is (current state) to where it wants to be (future state).

Determine desired risk culture	Assess gaps in current culture	Implement interventions to close the gap
➢ Visions, Mission, Values and Purpose ➢ Structure ➢ Leadership	➢ Job Design and Role Definition ➢ Desired vs. Actual Behaviours ➢ Systems and Processes	➢ Culture Change Leadership ➢ Communication & Engagement ➢ Learning and Development ➢ Organisational Alignment ➢ Performance Management

33

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk management
3.6 Communication and reporting
3.7 Reviewing and learning

Essentially, this involves three key steps:

- Clearly define where your organisation wants to be in terms of risk management culture.
- Define the level of involvement in risk management that you would like the whole organisation to have.
- Identify and articulate the desired behaviours around risk management. This includes tolerance for risk, how people respond to risks and risk events, and the general awareness of risk and risk management.

The desired culture will continue to evolve, as it will depend on the level of maturity that is acceptable to your organisation within a given period. Tools that might help you define the desired culture are benchmarking, surveys, workshops with senior management and independent risk framework assessments. Often, the definition process will be a top-down approach, followed by consultation down the line to engage buy-in (i.e. staff briefings, roundtable discussions, forums).
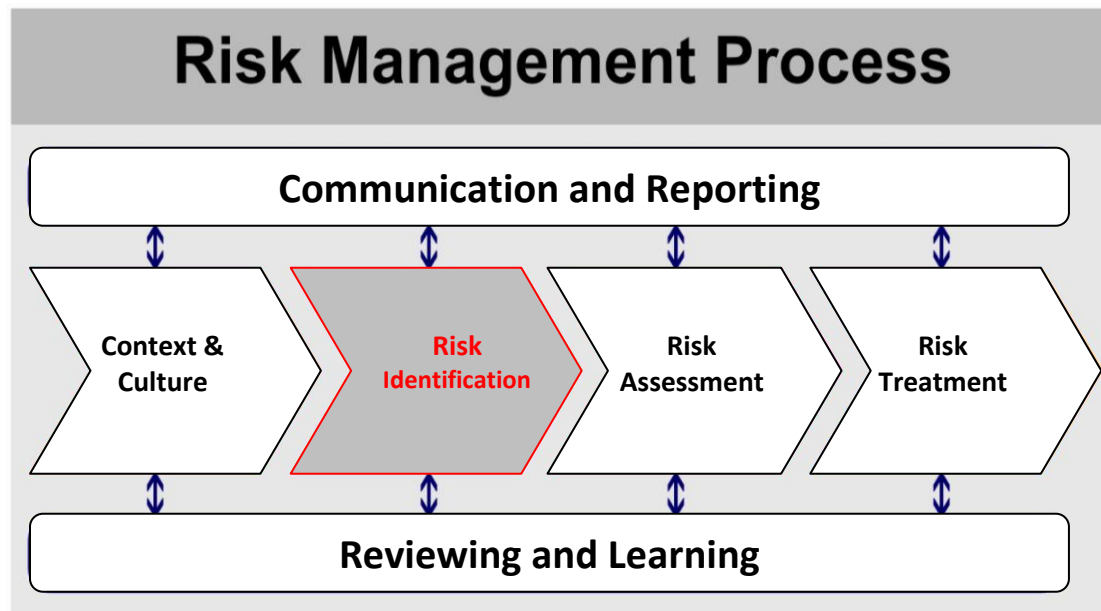
Assess your organisation's current risk culture

The current risk culture is an outcome of collective behaviour driven by existing norms around risk management. Determining your organisation's current culture and identifying the key drivers will be useful for identifying the appropriate interventions to achieve the desired risk culture.

The most commonly used tools for assessing current culture are interviews, focus group discussions and surveys. When conducting the assessment, it will be useful to gain input from a sample of participants or respondents across the different parts of the organisation, and across different levels.

- Determine what cultural and behavioural interventions are useful to help close the gap.
- Determine the cultural and behavioural intervention will help you close the gap between where you currently are and where you want to be in your risk culture. The assessment provides a useful starting point in prioritising and developing your options for culture change.

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.3. Risk Identification

What is Risk Identification?

The process of determining what, where, when, why, and how something could happen.

Why do it?

The objective of risk identification is to generate a comprehensive list of risks based on those events and circumstances that might enhance, prevent, degrade or delay the achievement of the objectives. This list of risks is then used to guide the assessment, treatment and review of key risks.

Comprehensive identification and recording is critical because a risk that is not identified at this stage may be excluded from further analysis. The risk identification process should include all risks, whether or not they are under the control of the organisation.

In identifying risks, it is also important to consider the risks associated with not pursuing an opportunity, e.g. loss of market share.

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

How to identify risks

This section will cover the key steps necessary to effectively identify risks from across the organisation. These steps are as follows:

1. understand what to consider when identifying risks
2. gather information from different sources to identify risks
3. apply risk identification tools and techniques
4. use risk categories for comprehensiveness
5. document the risks
6. document the risk identification process
7. assess the effectiveness of the risk identification process.

1. Understand what to consider

To develop a comprehensive list of risks, a systematic process should be used that starts with the statement of context. To demonstrate that risks have been identified effectively, it is useful to step through the process, project or activity in a structured way using the key elements defined while establishing the context. This can help provide confidence that the process of risk identification is complete and major issues have not been missed.

What might happen that could:

- Increase or decrease the effective achievement of objectives?
- Make the achievement of the objectives more or less efficient (e.g. financial, people, time)?
- Cause stakeholders to take action that may influence the achievement of objectives?
- Produce additional benefits?

Other Considerations:

- What would be the effect on objectives?
- When, where, why, how are these risks (both positive and negative) likely to occur?
- Who might be involved or impacted?
- What controls currently exist to treat this risk (maximise positive risks or minimise negative risks)?
- What might prevent the control from having the desired effect on the risk?

2. Gather information to identify risks

Good-quality information is important for identifying risks. The starting point for risk identification may be historical information about this or similar organisations, followed by discussions with a wide range of stakeholders about historical, current and evolving issues.

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1   Overview of the risk management process
3.2   Context and culture
3.3   Risk identification
3.4   Risk assessment
3.5   Risk treatment
3.6   Communication and reporting
3.7   Reviewing and learning

3. Apply risk identification tools and techniques

Organisations apply a set of risk identification tools and techniques that are suited to their objectives and capabilities, and to the risks they face. Relevant and up-to-date information is important in identifying risks. This should include suitable background information where possible. People with appropriate knowledge should be involved in identifying risks.

Approaches used to identify risks might include the use of checklists, judgements based on experience and records, flow charts, brainstorming, systems analysis and scenario analysis. The approach used will depend on the nature of the activities under review, types of risks, the organisational context, and the purpose of the risk management exercise.

- Team-based brainstorming, for example, where facilitated workshops are a preferred approach as they encourage commitment, consider different perspectives and incorporate differing experiences.
- Structured techniques such as flowcharting, system design review, systems analysis, Hazard and Operability (HAZOP) studies and operational modelling should be used where the potential consequences are catastrophic and the use of such intensive techniques is cost-effective.
- For less clearly defined situations, such as the identification of strategic risks, processes with a more general structure, such as 'what-if' and scenario analysis might be used.
- Where the resources available for risk identification and analysis are constrained, the structure and approach may have to be adapted to achieve efficient outcomes within budget limitations. For example, where less time is available, a smaller number of key elements might be considered at a higher level, or a checklist may be used.

4. Use relevant risk categories for comprehensiveness

The risk profiles of public sector organisations may differ from those of commercial organisations, given the difference in organisational objectives and stakeholder groups.

5. Document the risks identified

The risks identified during the risk identification are typically documented in a risk register that, at this stage in the risk assessment process, includes:

- risk description
- how and why the risk can happen (i.e. causes and consequences)
- the existing internal controls that that may reduce the likelihood or consequences of the risks.

It is critically important at this stage to understand the cause-effect relationships between a risk, its causes, and the potential consequences should the risk occur. If the "wrong" risk is identified at this stage (e.g. causes or consequences, rather than the actual risk itself), this will reduce the value of the rest of the risk management process.

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

One of the weakest elements of an organisation's risk framework may be the capturing and defining of risks. It is essential when describing a risk to consider the following three elements:

- description/event – an occurrence or a particular set of circumstances
- causes - the factors that may contribute to a risk occurring or increase the likelihood of a risk occurring
- consequences – the outcome(s) or impact(s) of an event.

It is the combination of these elements that makes up a risk, and this level of detail will enable an organisation to more completely understand the risk.

6. Document your risk identification process

In addition to documenting the risks identified, it is also necessary to document the risk identification to help guide future risk identification exercises and to ensure that good practices are maintained by drawing on lessons learned from previous exercises. Documentation of this step should include:

- the approach or method used for identifying risks
- the scope covered by the identification
- the participants in the risk identification and the information sources consulted.

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.4 Risk Assessment

Risk Management Process

Communication and ReportingCommunication and

Context & Culture	Risk Identification / Risk	Risk Assessment / Risk	Risk Treatment / Risk

Reviewing and LearningReviewing and Learning

What is Risk Assessment?

Risk assessment can be described in two parts:

- Risk analysis
- Risk evaluation

Risk Analysis

The risk analysis step aims to develop an understanding of the risk. It provides an input to decisions on whether risks need to be treated and the most appropriate and cost-effective risk treatment strategies.

Why do it?

Risk analysis is a fundamental component of the risk management process. It helps to guide the evaluation of risk by defining the key parameters of the risk and how these may impact the achievement of organisational objectives. One of the key outcomes of the risk analysis process is the determination of the levels of risk exposure for the organisation.

In addition, the data and related information collected during the risk analysis process can be used to assist in guiding risk treatment decisions.

IMPLEMENTING A RISK
MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

How to analyse risks

Risk analysis involves the following key steps:

1) identify and evaluate existing control effectiveness
2) determine risk likelihood (probability or frequency of risk occurrence)
3) determine risk consequence (outcome or impact of an event)
4) determine risk level.

The following section on how to analyse risks is structured as follows:

i) identify and evaluate existing controls
ii) determine risk consequence and the likelihood
iii) determine the overall risk level
iv) document your risk analysis process.

i) Identify and evaluate existing controls

When assessing a risk, it is important to identify what controls are in place to mitigate the risk. Many controls are built into existing business operations and systems.

Examples of controls:

- Controlled physical access (e.g. security codes, access cards, security personnel)
- Employee code of conduct
- Media and public relations strategies/protocols
- Specified training (e.g. software, hazardous substances)
- Automated software controls (e.g. temperature control)
- Policies and procedures
- Standardised business processes
- Insurance
- Quality control management
- Budget management
- Outsourcing functions to specialists
- Formalised contracts and Service Level Agreements
- Audits (internal and external).

Controls should be considered on the basis of:

- design effectiveness – is the control "fit for purpose" in theory, i.e. is the control designed appropriately for the function for which it is intended?
- operational effectiveness – does the control work as practically intended?

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

To understand the level of residual risk remaining after controls have been taken into account, it is essential as part of the risk analysis process to be able to estimate the effectiveness of existing controls.

In the first instance, management should be able to make a subjective assessment of the effectiveness of the controls using a rating scale. Periodic independent assurance is also needed to provide an objective view - based on testing - of the adequacy and effectiveness of the controls e.g. internal and external audits.

It is useful to involve staff with an understanding of the controls when rating them. Internal audit, business analysts and operational/ financial management can all provide input into control identification and assessment.

A well-designed and implemented control can often mitigate or reduce more than one risk or type of risk.

ii) Determine risk consequence and likelihood

The magnitude of the consequences of an event, should it occur, and the likelihood of the event and its associated consequences should be assessed in the context of the effectiveness of the existing strategies and controls.

Consequences and likelihood may be estimated using statistical analysis and calculations. Where no reliable or relevant past data are available, subjective estimates may be made which reflect an individual's or group's degree of belief that a particular event or outcome will occur.

The most relevant sources of information and techniques should be used when analysing consequences and likelihood.

Sources of information:

- Past records
- Practice and relevant experience
- Relevant published literature
- Market research
- The results of public consultation
- Experiments and prototypes
- Economic, engineering or other models
- Specialist and expert judgements.

Techniques:

- Structured interviews with experts in the area of interest
- Use of multidisciplinary groups of experts
- Individual evaluations using questionnaires
- Use of models and simulations.

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

Types of Analysis

- Risk analysis may be undertaken in varying degrees of detail depending upon the risk, the purpose of the analysis, and the information, data and resources available. The analysis may be qualitative, semi-quantitative or quantitative or a combination of these, depending on the circumstances.

- The order of complexity and costs of these analyses, in ascending order, are qualitative, semi-quantitative and quantitative. In practice, qualitative analysis is often used first to obtain a general indication of the level of risk and to reveal the major risk issues. Later it may be necessary to undertake more specific or quantitative analysis of the major risk issues.

- The form of analysis should be consistent with the risk evaluation criteria developed as part of establishing the risk management context.

Qualitative Analysis

- Use of words to describe the magnitude of potential consequences and the likelihood that those consequences will occur
- Scales can be adjusted to suit the circumstances, and different descriptions may be used for different risks
- Typically used in presenting overall risk profile, i.e. heat map.

Current Risk Heat Map

	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	11	16	20	23	25
Likely	7	12	17	21 1	24
Possible	4	8	13	18	22
Unlikely	2	5	9	14 1	19
Rare	1	3	6	10	15

Semi-quantitative Analysis

- Use of nominal ranking scales, i.e. values are assigned to likelihood and consequence scales
- Numbers should only be combined using a formula that recognises the limitations of the kinds of scales used
- Scales are context-specific
- Typically used in prioritising risks based on numerical ranking.

Quantitative Analysis

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

- Use of numerical values for both consequences and likelihood
- Quality of analysis depends on accuracy and completeness of numerical values used
- Consequences may be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or past data
- Typically used in deriving financial risk reserves.

LIKELIHOOD:	50% (Within 1 Year) - Possible
CONSEQUENCE:	$120,000 - Significant
OVERALL EXPOSURE:	50% x $120,000 = $60,000

Before you determine the overall risk rating, you will need to determine the level of likelihood and consequence for each risk. Each organisation will need to establish its own likelihood and consequence tables.
It is also necessary to establish your likelihood table.

iii) Determine the overall risk rating

Once you have rated the likelihood and consequence, combine the two to determine the overall risk rating.
Based on the risk analysis, risks are classified by level to determine the appropriate level of response to those risks. Specific responses are defined in the "Treat Risks" phase.

Risk Score	Risk Rating	Likely Response
1-6	Low	• No immediate response required. • Risk ownership may not be allocated. • Could be excluded from risk monitoring activities. • An infrequent re-evaluation of risk.
7-10	Medium	• Regular monitoring and re-evaluation of potential risk and any factors that may increase consequence or likelihood occurrence. • Allocate accountability for responding to risk to individual responsible for overseeing risk treatment/s as resources/ circumstances permit.
11-19	High	• Develop risk response strategies as part of risk management and operational processes. • On-going monitoring of risk and progress of risk response or treatment plans. • Allocate accountability for responding to risk to individual responsible for overseeing risk treatment/s.
20-25	Extreme	• The immediate escalation of risk to senior management/ executive for prioritised response and treatment plan development. • Incorporate management of risk into established strategic governance and operational processes. • Allocate accountability for responding to risk to individual responsible for overseeing risk treatment/s.

iv) Document your risk analysis process

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

Documentation of the risk analysis process provides a record of how risks were analysed in previous periods, thereby informing future risk analysis exercises. A key outcome of documenting the risk analysis process is the enabling of accurate tracking of risks over time using historical reference data.

Documentation should include:

- key assumptions and limitations
- sources of information used
- explanation of the analysis method, and the definitions of the terms used to specify the likelihood and consequences of each risk
- existing controls and their effectiveness
- description and severity of consequences
- the likelihood of these specific occurrences
- resulting level of risk.

Detailed documentation may not be required for very low risks; however, a record should be kept of the rationale for initial screening of very low risks.

Risk Evaluation

Risk evaluation involves comparing a risk's overall exposure against the organisation's risk tolerance.

This allows the determination of whether further controls are required to bring the risk to a level acceptable to the organisation. The output of the risk evaluation phase is a prioritised list of risks.

Why do it?

The purpose of risk evaluation is to make decisions, based on the outcomes of risk analysis, about which risks need treatment and to prioritise treatments.
The output of a risk evaluation generally consists of a prioritised list of risks that require further action.

How to evaluate risks?

The following key steps are involved in evaluating risks:

  i.   Rank the risks based on the outcome of the risk analysis process
  ii.   Consider the overall risk profile
  iii.   Develop a list of priority risks.

i) Rank the risks

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1   Overview of the risk management process
3.2   Context and culture
3.3   Risk identification
3.4   Risk assessment
3.5   Risk treatment
3.6   Communication and reporting
3.7   Reviewing and learning

Risks can be ranked either qualitatively or quantitatively. Applying qualitative analysis, you can rank the risks using a heat map. The heat map is a colour-coded matrix with each colour indicating the level of risk. This heat map represents the tolerance level of your organisation. This will have been developed in the earlier phase of "Establish Context", as it is a part of the organisation's risk management context.

Based on the control effectiveness rating, the likelihood of the risk occurring and potential consequences identified in the earlier phase, plot the risks against the matrix. The completed matrix is your risk profile.
Applying semi-quantitative analysis, the organisation can also rank the risks based on their numerical value. The numerical value is a combination of the values assigned by the organisation to control effectiveness, likelihood and consequence.

The most common approach to visually recording risk is to use a 5 x 5 heat map as illustrated below. A risk heat map is sometimes referred to as a risk matrix.

Current Risk Heat Map

	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	11	16	20	23	25
Likely	7	12	17	21 1	24
Possible	4	8	13	18	22
Unlikely	2	5	9	14 1	19
Rare	1	3	6	10	15

The matrices you select will reflect your organisation's risk rating scales.
For example: If your risk consequence and likelihood used 5-point scales, such as those shown above, a 5 x 5 heat map would be appropriate.

ii) Consider the overall risk profile

Once the initial risk profile has been developed, the organisation may need to consider how each risk ranks in relation to the other risks. This step allows the organisation to conduct a "sanity check" of the risks that have been placed on the heat map to ensure that risks are rated correctly when compared to one another (e.g. "Risk manager may be off sick with flu" is not rated the same as "Project objectives may not be met").

Possible outcomes of this step include:

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
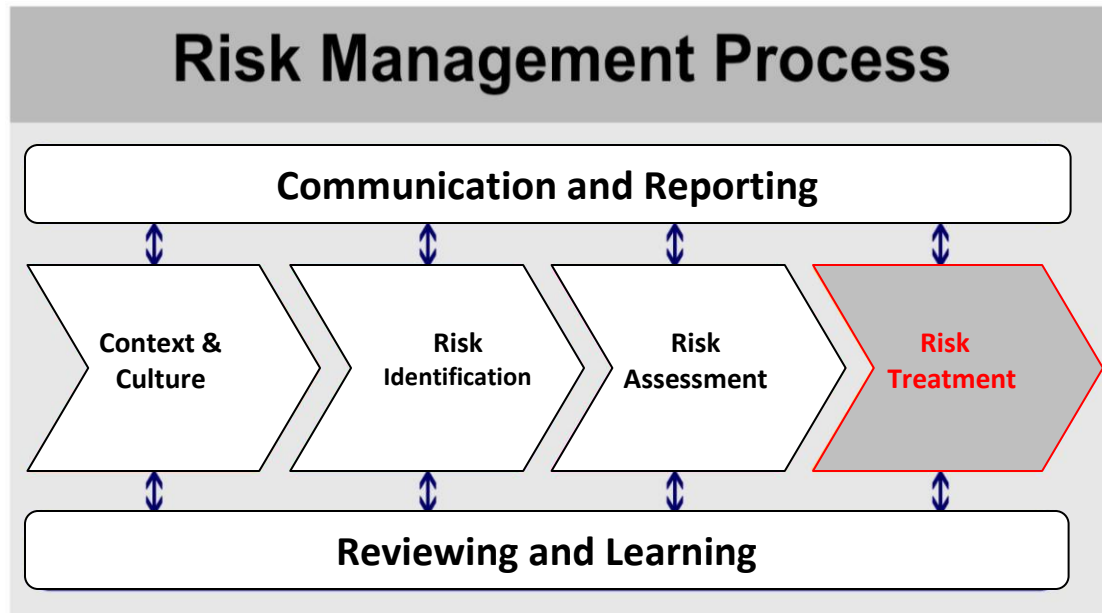3.6 Communication and reporting
3.7 Reviewing and learning

- The organisation may reassess the rating of some of the risks if it is felt that the overall spread of the risks relative to one another is not a true reflection of reality
- The organisation may recognise that some risks are similar to the other risks or are contributing factors to other risks. Hence, they may be incorporated into the risk description of other risks within the risk register
- The organisation may consider the interdependencies between the risks and consider the consequences for the organisation if more than one risk were to occur at the same time. This may result in changes to the overall risk ratings.

iii) Develop a priority list of risks

The primary objective of the evaluation is to prioritise risks. This helps to inform the allocation of resources to manage risks, both non-financial and financial.

The priority list can be categorised by a number of different criteria dependent on what is most relevant for the organisation, e.g. risk rating, functional area or by type of impact (i.e. strategic or operational). This will further refine the focus for risk treatment.

3.1   Overview of the risk management process
3.2   Context and culture
3.3   Risk identification
3.4   Risk assessment
3.5   **Risk treatment**
3.6   Communication and reporting
3.7   Reviewing and learning

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.5 Risk Treatment

Risk Treatment

Risk treatment involves identifying the range of options for treating risks, assessing these options, and preparing and implementing treatment plans.

Risk treatment may involve a cyclical process of assessing a risk treatment, deciding that current risk levels are not tolerable, generating new risk treatment/s, and assessing the effect of that treatment until a level of risk is reached that the organisation can tolerate based on the agreed risk criteria.

Why treat risks?

A key outcome of the risk evaluation process is a list of those risks requiring further treatment, as determined by the overall level of the risk against the organisation's risk tolerance levels. However, not all risks will require treatment as some may be accepted by the organisation and may only require occasional monitoring throughout the period.

The risks that fall outside of the organisation's risk tolerance levels are those which may have a significant potential impact on the ability of the organisation to achieve its set objectives. The purpose of treating risks is to minimise or eliminate the potential threat the risk may pose to the achievement of the set objectives.

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 **Risk treatment**
3.6 Communication and reporting
3.7 Reviewing and learning

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

How to treat risks

Treating risks involves the following key steps, each of which is covered in detail in this section:

1. identify risk treatment options
2. select risk treatment options
3. assign risk ownership
4. prepare risk treatment plans.

1. Identify risk treatment options

Risk treatment design should be based on a comprehensive understanding of how risks arise. This means understanding not only the immediate causes of an event but also the underlying factors that influence whether the proposed treatment will be effective.

2. Select risk treatment options

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances.

Risk Treatment Options	
Tolerate	The exposure may be tolerable without any further action being taken. Even if it is not tolerable, the ability to do anything about certain risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained. In these cases, the response may be to tolerate the existing level of risk. This option, of course, may be supplemented by contingency planning to handle the impacts should the risk be realised.
Treat	By far the greater number of risks will be addressed in this way. The purpose of treatment is to take action (control) to constrain the risk to an acceptable level while continuing, within the organisation, with the activity giving rise to the risk. Such controls can be further sub-divided according to their particular purpose.
Transfer	For some risks, the best response may be to transfer them. This might be done by conventional insurance, or it might be done by paying a third party to take the risk in another way. This option is particularly useful for mitigating financial risks or risks to assets. The transfer of risks may be viable either because it is the best way of reducing the organisation's exposure or because another organisation (which may be another government organisation) is more capable of effectively managing the risk. It is important to note that some risks are not (fully) transferable – in particular it is generally not possible to transfer reputational risk even if the delivery of a service is contracted out. The relationship with the third party to which the risk is transferred needs to be carefully managed to ensure successful transfer of the risk.
Terminate	Some risks will only be treatable, or containable to acceptable levels, by terminating the activity. It should be noted that the option of termination of activities may be severely limited in government when compared to the private sector; a number of activities are conducted in the government sector because the associated risks are so great that there is no other way in which the output or outcome, which is required for the public benefit, can be achieved. This option can be particularly important in project management if it becomes clear that the projected cost /benefits relationship is in jeopardy.

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

Take the Opportunity	This option is not an alternative to those above; rather, it is an option which should be considered whenever tolerating, transferring or treating a risk. There are two aspects to this. The first is whether or not, at the same time that threats are being mitigated, an opportunity arises to exploit a positive impact. For example, if a large sum of capital funding is to be put at risk in a major project, are the relevant controls considered good enough to justify increasing the sum of money at stake to gain even greater advantages? The second is whether or not circumstances arise which, whilst not generating threats, offer positive opportunities. For example, a drop in the cost of goods or services frees up resources which can be redeployed.

It is recommended that consideration be given to the cost of the treatment as compared to the likely risk reduction that will result. For example, if the only available treatment option would cost in excess of $10M to implement and the cost impact of the risk is only $5M, it may not be advisable.

To understand the costs and benefits associated with each risk treatment option, it is necessary to conduct a cost-benefit analysis.

Basic cost-benefits analysis:

- Define or break down the risk into its elements by drawing up a flowchart or list of inputs, outputs, activities and events.
- Calculate, research or estimate the cost and benefit associated with each element (include if possible direct, indirect, financial and social costs and benefits).
- Compare the sum of the costs with the sum of the benefits.

Cost-Benefit Analysis Example:

An HR manager has a risk of "Ineffective records management leading to loss of employee data". As a treatment strategy, she is deciding whether to implement a new personnel management and payroll system. The HR department has only a few computers and staff are not highly computer literate. She is aware that computerised information will allow more accurate analysis of data and give a higher quality of reliability and service to internal customers.

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

Her financial cost-benefits analysis is shown below:

Costs:

Description	Quantity	$ Price	$ Total
PCs with supporting software	10	2450	24,500
Server	1	3500	3,500
Printers	3	1200	3,600
Cabling & Installation	1	4600	4,600
Payroll Software	1	15000	15,000
Computer introduction training	8 People	400	3,200
Keyboard skills	8 People	400	3,200
Payroll system training	4 People	700	2,800
Lost time	40 man days	200	8,000
Total cost			**68,400**

Benefits

Description	$ / Year
Doubling of payroll capacity: estimate:	40,000
Improved efficiency and reliability of client service: estimate:	50,000
Improved accuracy of customer information: estimate:	10,000
Reduction of payroll and processing effort:	30,000
Total benefits	**130,000**

3. Assign risk ownership

The CEO and/or the Executive Management Committee typically allocate responsibility for risk to an operational or functional area line manager.

Assigning Risk Ownership: Example	
Risk Type	**Risk Owner**
Strategic	CEO
Human Resources	HR Manager
Finance / Budgeting	Finance Manager / Chief Financial Officer
Health and Safety	Facilities manager or HR Manager
Business Continuity	Risk Officer or Facilities Manager
Reputational	CEO / Communication Manager
IT and Systems	IT Manager

Risk owners nominated by executive management should assume responsibility for developing effective risk treatment plans. The risk owner should be a senior staff member or manager with sufficient technical knowledge about the risk and/or risk area for which treatment is required.

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

The risk owner will often delegate responsibility (but not accountability) to his/her direct reports or consultants for detailed plan development and implementation.
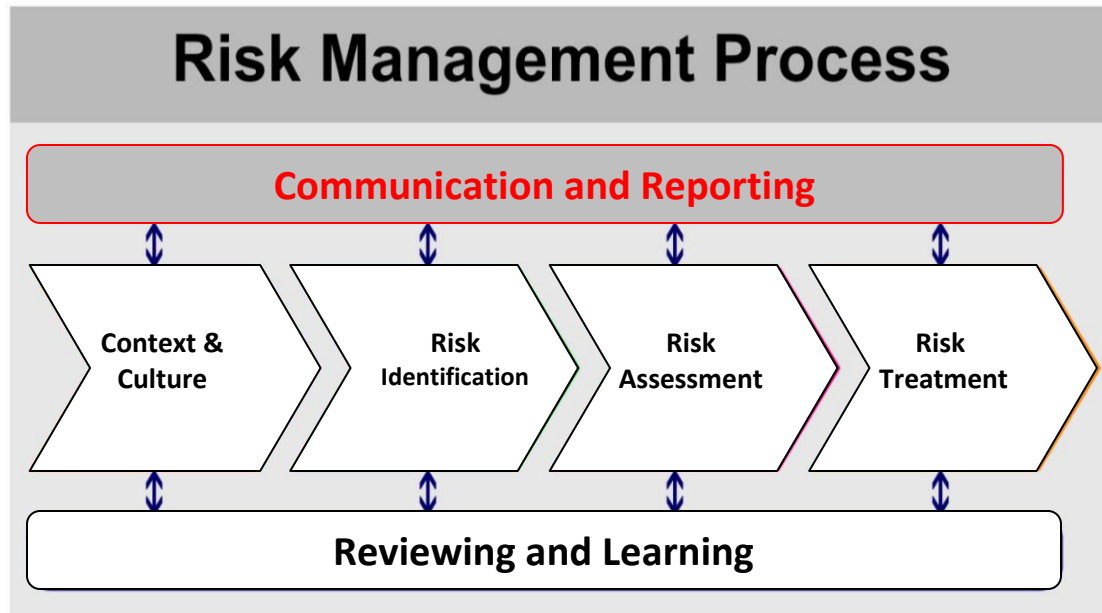
4. Prepare treatment plans

Once treatment options for individual risks have been selected, all treatment options should be consolidated into risk action plans and/or strategies. As one risk treatment may impact on multiple risks, treatment actions for different risks need to be combined and compared in order to identify and resolve conflicts between plans and to reduce duplication of effort.

Treatment plans should:

- identify responsibilities, schedules, the expected outcome of treatments, budgets, performance measures and the review process to be set in place.
- include mechanisms for assessing and monitoring treatment effectiveness, within the context of individual responsibilities and organisational objectives, and processes for monitoring treatment plan progress against critical implementation milestones. All this information should arise from the treatment design process.
- document how, practically, the chosen options will be implemented.

The successful implementation of the risk treatment plan requires an effective management system that specifies the methods chosen, assigns responsibilities and individual accountabilities for actions, and monitors them against specified criteria. Communication is a very important part of treatment plan implementation.

	3.1 Overview of the risk management process
	3.2 Context and culture
IMPLEMENTING A RISK	3.3 Risk identification
MANAGEMENT FRAMEWORK	3.4 Risk assessment
	3.5 Risk treatment
	3.6 Communication and reporting
	3.7 Reviewing and learning

3.6 Communication and Reporting

Risk Management Process

Communication and Reporting

Context & Culture → Risk Identification → Risk Assessment → Risk Treatment

Reviewing and Learning

Risk communication

Risk communication is generally defined as an interactive process of exchange of information and opinion, involving multiple messages about the nature of risk and risk management. This applies to internal communication in the organisation and to communication with external stakeholders.

Informed communication between an organisation and its stakeholders on an issue prior to making a decision or determining a direction on a particular issue is fundamental to effective risk management.

Informed communication is a process, not an outcome; it impacts decision-making through influence and learning rather than power, and it is about inputs to decision-making, not necessarily joint decision-making.

Why do it?

Communication with internal and external stakeholders is essential for effective risk management and should take place at each step of the risk management process as far as necessary.

Effective internal and external communication is important to ensure that those responsible for implementing risk management, and those with a vested interest, understand the basis on which decisions are made and why particular actions are required.

Stakeholders are likely to make judgements about risk based on their perceptions. These can vary due to differences in values, needs, assumptions, concepts and concerns as they relate to the risks or the issues under

IMPLEMENTING A RISK
MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

discussion. Since the views of stakeholders can have a significant impact on the decisions made, it is important that their perceptions of risk be identified, recorded and integrated into the decision-making process.

The key steps to communication are:

- establish communication and consultation objectives
- analyse stakeholders or recipients of the message
- develop key messages and purpose
- identify communication owners and senders
- identify appropriate channels
- determine timing of communication
- deliver key messages.

Objectives of communication may include:

- Building awareness and understanding about a particular issue
- Learning from stakeholders
- Influencing the target audience
- Obtaining a better understanding of the context, the risk criteria, the risk, or the effect of risk treatments
- Achieving an attitudinal or behavioural shift in relation to a particular matter
- Any combination of the above.

Developing a communication plan is essential to ensure that key messages are delivered effectively to the right people at the right time using the most appropriate channels at every step of the risk management process.

A stakeholder consultation plan helps to ensure that "all bases are covered" when it comes to understanding perceptions around risk and risk management, identifying and assessing risks, and developing treatment options. The plan is also useful for ensuring that the consultation is as inclusive as is appropriate.

When implemented effectively, a stakeholder consultation plan should:

- appropriately define an organisation's context
- ensure that the interests of stakeholders are understood and considered.

Ensure risks are adequately identified

- bring different areas of expertise together in analysing risks
- ensure that different views are appropriately considered in evaluating risks
- ensure appropriate change management techniques during the risk management process
- promote "ownership" of risk by managers
- engage stakeholders to allow them to appreciate the benefits of particular controls and the need to endorse and support a risk treatment plan.

IMPLEMENTING A RISK
MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

Risk and risk management reporting

Risk reporting is the regular provision of appropriate risk-related information to stakeholders and decision-makers within an organisation to support understanding of risk management issues and to assist stakeholders in performing their duties within the organisation.

The need for risk reporting

Successful risk management requires frequent and open communication with a broad group of internal and external stakeholders. This makes risk reporting and the definition of a risk communications and reporting plan a key component of an organisational risk management (or ERM) program.

Effective risk reporting also contributes to good corporate governance by providing reliable and current information to boards, senior managers and other stakeholders regarding the risks faced by the organisation as well as the treatment plans in place to manage these risks. The Board of a public entity is also required to inform the Minister and department head of known major risks.

The availability of this information can be used to support management decision-making during strategic planning and operational management processes.

Foundations of good reporting

The following principles should be remembered when developing a risk-reporting solution:

- The quality of risk reporting is dependent on a fully functioning risk management system. Incomplete or unreliable risk identification, assessment, prioritisation and treatment outputs will be reflected in poor reporting outputs.
- There is no single risk report that meets the needs of all stakeholders. Reports should be developed and customised to reflect the needs and preferences of the target audience and its purpose. Seek input from stakeholders before implementing a risk-reporting solution, as this should be part of existing reports and reporting frameworks.
- Although all organisations need to report on risk to various stakeholder groups, organisations with more mature and sophisticated risk management frameworks will typically produce a number of customised risk reports to meet the needs of different stakeholder groups throughout the year.
- Avoid providing too much or too little information in risk reports. Senior Management and the Board will typically prefer a summary of risks and risk trends, focusing on high risk and strategic issues across the organisation, while those involved in managing specific risks will require detailed information covering their areas of responsibility.

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

The audience for risk reporting

Risk reports should be delivered to a broad spectrum of organisational stakeholders. Typical recipients of regular formal risk reports should include:

- CEO and Board of Directors
- Business unit heads of all major business functions
- Compliance committees (notably Internal Audit and Risk Management)
- Staff directly responsible for designing and implementing risk management treatments
- Employees who need to assist in the identification of risk and the implementation of risk plans
- Government ministries and agencies
- The public (through access to Annual Reports and press releases).

A single person, typically the risk manager, should be responsible for coordinating and drafting risk reports to ensure consistency in standards and format.

Risk reporting can be automated using risk management software such as the Vigilant ERM's Vigilant Risk Manager. However, it is still important to ensure that reporting formats meet stakeholder requirements.

The risk process should ensure that risks are linked to strategic objectives. This helps to report on risk within a strategic organisational context.

Frequency of risk reporting

At a minimum, an organisation should update and report on its risk profile on an annual basis. While an annual reporting and update cycle may meet statutory requirements, effective risk management typically requires more frequent reporting on risk.

The frequency of risk reporting should reflect the cycle of the organisation's regular internal reporting. Where the Executive receives monthly or quarterly progress reports on Financial, Operational, Health and Safety or IT matters, they may wish to receive similar risk reports.

Types and content of risk reports

The information within risk reports is drawn from the risk register of the organisation. By filtering the information within the risk register, it is possible to draft a number of reports tailored to suit the needs of the various recipients.

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

The following table illustrates the different types of reporting:

Report Type	Comment
Annual Report Attestation	• Boards/CEOs and Secretaries who are accountable for the risks of their organisations are required to attest in the annual report that organisations have risk management processes in place and that: • These processes are effective in controlling risks to a satisfactory level • A responsible body or audit committee verifies that view.
Top Risks/Strategic Risks	• These reports contain a prioritised list of the top 10 to 20 risks based on consequence and likelihood scores. Typically they include details about the risk, information on key controls and their effectiveness and additional treatments needed, with timeframes.
Risk Trends	When risks are regularly reassessed, it is possible to: • Define target risk levels for key risks • Identify which risks are getting worse or where treatments are reducing risk exposures • Identify risk areas that need additional attention • Demonstrate the success of treatment plans.
New and/or Emerging Risks	• By sorting risks according to when they were identified, it is possible to report easily on new risks that may still need to be fully considered and understood. From an emerging-risk perspective, types or categories of risks that may begin to emerge over the next 2-3 years or longer should be identified and captured. Details at this stage may only include information regarding what research is being undertaken on the risk, and who is responsible.
Risk with Ineffective Controls	• By identifying significant / extreme risks with ineffective controls, the Board and Executive can identify potential points of business failure that need urgent interventions or resource support.
Risk Categories / Risk Types	• By grouping all risks that have not been allocated to a responsible person for follow-up and response, management can identify key risks that are not being effectively monitored and managed.
Risk Owner / Person Responsible	• By filtering the report by the risk owner, it allows those responsible to view risk treatments that they need to oversee or develop.
Risk Treatments Due or Overdue	• By sorting risks according to due dates for treatment plans / responses, Risk Managers, Project Managers and others can identify critical timeframes for responding to key risks as well as identify and manage potential delays and/or non-performance in responding to risk.

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

It should be noted that for all the risk report types outlined above, organisations may choose to report predominantly on an "exception" basis. This means to either:

- only report on the changes from the last report rather than producing risk reports that contain data that are largely unchanged from the last reporting cycle; or,
- only report on risks at the Executive/ Senior Manager level that fulfil predefined characteristics (e.g. significant risks with poor control effectiveness).

This approach prevents a situation where the same risk may justifiably appear on the report time after time as it is rated high, but no further action can be taken to mitigate the risk at that time (i.e. the risk has been accepted as high). In this instance, report recipients may fail to pay attention to the risk report as they become used to seeing the same risk information and, therefore, begin to regard the risk-reporting process as non-value-adding. It is important, however, to exercise complete oversight of all risks on at least an annual basis to ensure that there have been no changes to the overall risk profile and that the executives/senior managers are fulfilling their oversight duties.

Format of risk reports

The way in which risk information is presented can make a huge difference to the value it adds.
It is often useful to represent risk information graphically to make it easily understood and to show a large volume of information in a compact manner.

The following section provides examples of three types of risk reports:

1. Strategic risk reports
2. Operational risk reports
3. Key risk indicator reports.

1. Strategic risk report formats

Heat maps are commonly used to report on the top risks faced by the organisation and are well received by most boards. They are useful as they graphically illustrate the relative severity of risks in relation to one another.

Current Risk Heat Map

	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	11	16	20	23	25
Likely	7	12	17	21 1	24
Possible	4	8	13	18	22
Unlikely	2	5	9	14 1	19
Rare	1	3	6	10	15

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1   Overview of the risk management process
3.2   Context and culture
3.3   Risk identification
3.4   Risk assessment
3.5   Risk treatment
3.6   Communication and reporting
3.7   Reviewing and learning

The green areas represent the least severe risks, and as the risk moves upward and right towards the red shaded area the level of risk exposure increases.

Heat maps are less useful (difficult to read) when there is a need to illustrate a large number of risks, or where risk scores are very similar for all risks.

The ability to effectively link an organisation's key risks to its strategic objectives or business goals is an indicator of a maturing risk management framework. An example is illustrated in the value chain report below.

2. Operational risk report format

Table formats, of which there are many variations, are useful for reporting on a large number of risks or when a greater amount of detail about each risk is required. This approach is best suited to operational risk reporting where, for example, the risk owner or risk manager will want to review more detailed risk and control information such as:

•   control effectiveness levels
•   rating scores
•   treatment plans
•   treatment due dates.

These reports are used by risk committees, program managers and risk owners to monitor and manage the update, implementation and review of risk management activities/ plans. This level of detail can be provided as supporting information to summary executive reports, or provided where the board or executive wish to review a specific risk or cluster of risks.

A key advantage of table or spreadsheet reports is that they can easily be filtered or sorted to meet the reporting requirements of a specific target audience. It is also easy to add to or modify content following risk update processes.

3. Key Risk Indicators (KRIs)

Key risk indicators – which are used to measure risk levels – should be developed once an organisation is satisfied that the basic elements of its risk management framework are well established and operating effectively.

In addition to reports containing qualitative data, once an organisation has established an effective system of risk reporting, it may wish to consider the use of quantitative data in the form of KRIs. Indicators are a valuable tool to facilitate the monitoring of risks and controls over time against an organisation's risk appetite. Whilst risk and control data in many organisations are formally updated on a regular basis, key indicators enable an organisation to continuously and predicatively monitor changes to its risk profile or control framework and allow actions to be carried out in a more timely and effective manner.

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

It is important to note that the use of KRIs is considered to be at the "mature end" of the risk management spectrum; therefore, organisations should not attempt to develop and roll out such indicators until they have established a robust risk management framework that delivers clearly defined and understood risk and control data. In addition, as risk indicators can be costly to implement and maintain, it is recommended that such indicators be used only for significant risks.

For organisations that are keen to focus on more quantitative data but which do not have the necessary resources to identify and monitor the large volumes of data required for risk indicators, it is recommended that priority be given to the identification and monitoring of key control indicators instead (see definitions below), as they are easier to identify and capture and will reflect a weakening in the control environment that is likely to result in an increased level of risk.

Key indicators allow an organisation to:

• understand how the risk profile changes in different circumstances
• appreciate how risk moves and is affected by the business environment
• focus attention on risk drivers that are most volatile
• ensure that controls around the drivers are robust and effective
• gain a forward-looking perspective of the current risk profile
• understand the early warning signals for emerging risks.

For example, the motor insurance industry relies heavily on risk indicators when determining appropriate policy pricing. Factors such as the age of the applicant, neighbourhood and number of kilometres driven each year build a profile of the applicant and, hence, the 'risk' that the insurance firm will have to pay out on a claim. If an insurance company were to attempt to write new business without utilising indicators, underwriters would be forced to use their intuition to judge the likelihood of a new customer claiming in the future. While some may prove to have good insight, many would misjudge the risk and, consequently, business performance would be significantly (negatively) affected.

There are three types of key indicators commonly used: Key Performance Indicators, Key Risk Indicators and Key Control Indicators. There is often confusion surrounding the difference between them. Below is a brief definition of each:

i) Key Performance Indicators (KPIs) are used to monitor the change in overall business performance (e.g. budget) in relation to specific business objectives. KPIs can measure internal or external factors and can be seen as events that may raise warnings of potential risks.

ii) Key Risk Indicators (KRIs) are a specific measure relating to a particular risk that shows a change in the likelihood or consequence of that risk event occurring. KRIs that demonstrate increased exposure to potential risks (e.g. significant increases in business volumes combined with staff numbers) can show what level of stress or strain current control activities may experience.

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1   Overview of the risk management process
3.2   Context and culture
3.3   Risk identification
3.4   Risk assessment
3.5   Risk treatment
3.6   Communication and reporting
3.7   Reviewing and learning

iii) Key Control Indicators (KCIs) are metrics that can demonstrate a change in a specific control's effectiveness (e.g. a control's design and its actual performance). A deterioration in KCIs reflects a weakening in the control environment and is likely to result in an increase in a risk's likelihood or consequence.

The definition of an effective system of Key Risk Indicators (KRIs) can be broken down into five phases:

1.   identify and document the key risk and control indicators
2.   source and validate existing KRI data
3.   establish tolerance levels and escalation procedures
4.   analyse, report and revise the KRIs
5.   monitor KRIs.

The use of risk management software for reporting

The use of risk management software is useful in helping manage risk-related information. However, it is not essential to use risk software to achieve a robust and effective risk management framework.

Most specialised risk management software tools, such as Vigilant Risk Manager, include automated risk reporting capabilities. Software tools can simplify and reduce the time required to report on risk management initiatives.

While many generic reports can be drawn from such software, it is still important to ensure that the report format and content meets stakeholder requirements. In many cases, an organisation may commission consultants, software vendors or internal IT specialists to develop customised reports to meet specific reporting requirements.

The VRM Risk Register is designed to allow organisations to:

- Create a single risk register across the organisation
- Record pertinent risk information, including:
  1.   Risk descriptions, causes and impacts
  2.   Risk assessment outcomes (likelihood, consequence, control effectiveness etc.)
  3.   Categorisation of risks (risk categories)

- Link risks to specific business units

  1.   Linkage of risks to specific strategic and operational objectives
  2.   Current control information
  3.   Responsibility for risk
  4.   Risk treatment and response
  5.   Risk response status and due dates

- Select from a range of pre-defined summary and detailed risk reports in both graphical and text formats. The software can generate heat map reports.

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

Conclusion

The importance of an effective risk-reporting system should not be underestimated as it ultimately supports improved decision-making ability. The failure to effectively report on risk will also undermine executive and Board support for the organisation's risk management process.

Reports should be viewed as a business tool rather than a compliance requirement.

Remember that there is no 'right or wrong' approach to risk reporting, as long as the reports produced:

- meet the needs of your stakeholders
- are available when needed by the business
- contain current, updated quality information
- are easily understandable
- contain the right level of detail
- are supported by detailed underlying risk information, where appropriate
- support action and accountability for risk management across the organisation.

Consideration of these requirements when designing risk-reporting solutions should maximise the benefits obtained from risk management processes.

IMPLEMENTING A RISK
MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

3.7. Reviewing and Learning

Risk Management Process

Communication and Reporting

| Context & Culture | Risk Identification | Risk Assessment | Risk Treatment |

Reviewing and Learning
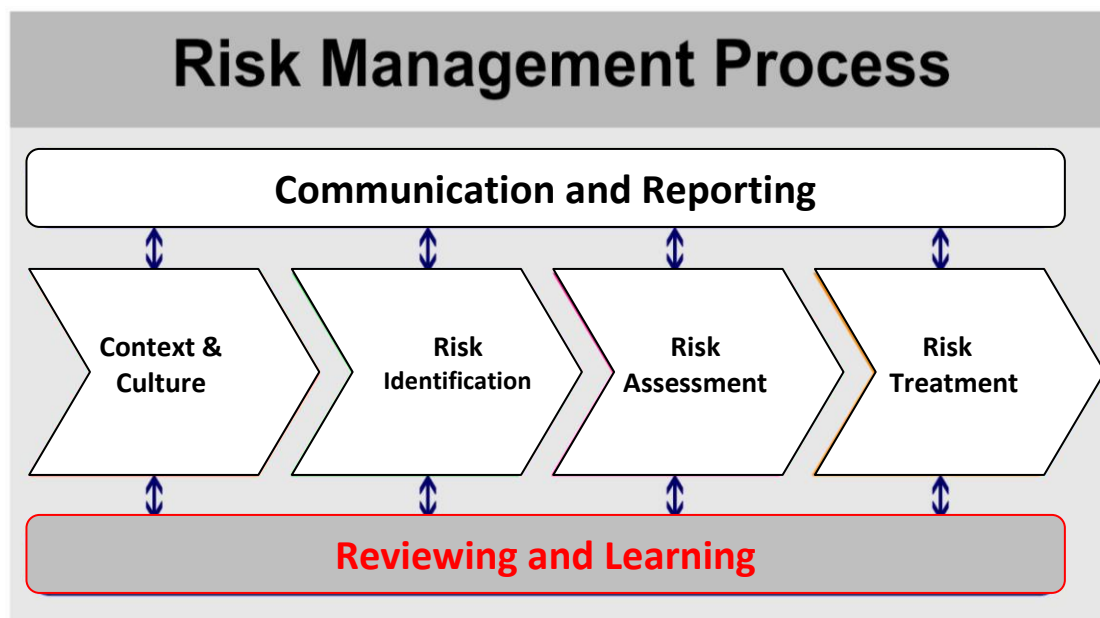
Reviewing and learning

It involves:

- analysing and learning lessons from events, changes and trends
- detecting changes in the external and internal contexts, including changes to the risk itself, which may require revision of risk treatments and priorities
- ensuring that the risk control and treatment measures are effective in both design and operation.

Reviewing and learning is an essential and integral part of managing risk and is one of the most important steps in the risk management process. It is necessary to review risks, the effectiveness and appropriateness of the strategies and management systems set up to implement risk treatments, and the risk management plan and system as a whole.

Why do it?

Regular review throughout the risk management process is necessary to:

- ensure accuracy of risk information - the environment in which the organisation is operating is constantly changing and so therefore are its risks. If risk information is inaccurate, it may cause the organisation to make poor decisions it might otherwise have avoided.
- ensure effectiveness and adequacy of risk management processes

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK	3.1 Overview of the risk management process
	3.2 Context and culture
	3.3 Risk identification
	3.4 Risk assessment
	3.5 Risk treatment
	3.6 Communication and reporting
	3.7 Reviewing and learning

- continuously evolve to desired levels of risk management maturity
- learn and continuously improve, adopting better practices and developments in risk management.

How to review

The key steps to review are:

1. understand the different types and levels of review
2. establish your review cycle
3. measure risk management performance.

1 Understand different levels and types of monitoring and review

Different types of review will be dependent on the type of decisions made around risks and risk management. This also implies varying levels of frequency and aggregation of risk information depending on the purpose of the review:

- At the task level, routine measurement or checking of particular parameters (for example, pollution levels or cash flows) is often required through continuous (or, at least, frequent) review.
- At the functional or operational level, line management reviews risks and their treatments on a regular basis. Risks are reviewed within a predefined scope and prioritised according to agreed criteria.
- At an organisational level, a risk function, manager or committee reviews enterprise-level risks. At this level of review, relevance and alignment with organisational strategies are reviewed. The risk management framework is also reviewed at this level.

Review of risk management framework

- The context of risk management needs to be reviewed at the enterprise level. This may include ensuring the accuracy of the organisation's risk criteria, risk tolerance, risk categories.
- The maturity of the risk management framework in terms of design and implementation could be monitored through tools such as surveys and benchmarking, comparing against the latest risk management better practices.
- The maturity of risk management can be reviewed by comparing the current level of maturity and the desired level of maturity at regular intervals (e.g. annually).

IMPLEMENTING A RISK MANAGEMENT FRAMEWORK

3.1 Overview of the risk management process
3.2 Context and culture
3.3 Risk identification
3.4 Risk assessment
3.5 Risk treatment
3.6 Communication and reporting
3.7 Reviewing and learning

2 Establish your review cycle

The review cycle will vary depending on the context of risk management and an organisation's risk management strategy. Typically,

- On an annual basis, the entire risk profile will be reviewed by the Risk & Compliance Committee (or equivalent); however this may be more frequent if major business changes are occurring.
- Every three years the risk management framework and associated documentation will be reviewed either as part of the internal audit process or by an independent third party.

3 Measuring risk management performance

Performance Indicators (PIs) are quantitative measures of the level of performance of a given item or activity. They need to be measurable and appropriate to individual business units and hold individuals accountable while forming the basis for continuing improvement.

Organisations should use their normal organisational planning processes to generate performance measures for the risk management system and processes. The performance indicators should reflect the range of key organisational objectives defined when the context was established at the start of the process. Performance indicators may monitor outcomes (for example, specific losses or gains) or processes (for example, consistent performance of risk treatment procedures).
Normally, a blend of indicators is used. However, outcome performance indicators usually lag significantly behind the changes that give rise to them; hence, in a dynamic environment operational process indicators are likely to be more useful.

Performance indicators should reflect the relative importance of risk management actions, with the greatest effort and focus applied to:

- the highest risks
- the most critical treatments or other processes
- treatments or processes with the greatest potential for improvements in efficiency.

Risk management performance indicators may be included in risk management reports to senior management and the Board.

4 Review and Enhance Risk Management Framework

4.1 Reviewing a risk management framework

What is it?

Reviewing a risk management framework is different to reviewing risks and their associated controls for effectiveness. The latter is a subset of the former as, by obtaining assurance on the effectiveness of the practices in place to manage specific risks, an organisation can be satisfied that at least part of its risk management framework is operating effectively. This review activity would then be coupled with a review of additional components of the risk management framework to ensure its overall effectiveness.

Why do it?

The aim of reviewing the risk management framework is to ensure that appropriate framework enhancements are occurring when and as needed. It is important to be confident in the effectiveness and efficiency of the risk management framework, as it provides the structure within which all risks are managed.

How to review the risk management framework

When reviewing the framework, particular attention should be paid to whether the framework has been appropriately customised and is operating in a manner that illustrates that:

- risks are being effectively identified and appropriately analysed
- this leads to adequate and appropriate risk management and control
- there is effective review by management and executives to detect changes in risks and controls.

There are several approaches available to help organisations effectively review their frameworks, including reviewing the framework against:

- Risk management process components
- Risk management maturity models.

The factors to consider when choosing the appropriate approach include:

- the maturity level of the risk management, as determined through any previous maturity assessments
- the number of planned risk management improvement initiatives currently being undertaken / recently having been undertaken
- the findings from previous risk management framework reviews
- the size and complexity of the organisation
- the number of major risks that have eventuated in that year
- whether the organisation has entered into providing any new services /products
- whether there have been significant organisational changes
- use of implementation partners.

For example, a medium-sized organisation that has been previously assessed as having mature risk management but which had numerous major risks eventuating in the last year would be most likely to undertake a more rigorous review of its risk management framework. The fact that the organisation scored highly in a previous maturity assessment does not outweigh the fact that it has seen many risks eventuate, as this would normally indicate some form of failure in its risk management practices.

It should also be noted that one may choose to use a combination of approaches at different times or alternate the approach used from year to year. For example, it may be appropriate to conduct an annual review of the framework against the process components; however, on a three-yearly basis, it may be useful to conduct a risk management maturity assessment, particularly if over that period a number of risk management improvement initiatives have occurred.

4.2 Enhancing a risk management framework

The framework clearly articulates the 'enhancing a risk management framework' loop that supports the on-going effectiveness of a risk management framework. Set out below is the diagram provided within that Standard to demonstrate this process.

Why do it?

Continuous improvement and change management is essential for ensuring the on-going relevancy and effectiveness of risk management activities within an organisation. To achieve the greatest benefits from continuous improvement, it must span all risk management framework elements including the process, capability, behaviours, tools and templates, reporting structures, and the practices used to manage actual risks.

How to achieve it?

There is a direct link between the outcomes of review activities and the continual enhancement of the framework. Continuous enhancement is supported and informed by both the review of risks and controls (as outlined in the 'Implementing the Risk Management Framework' section) and the review of the risk management framework.

As the continual enhancement of a risk framework includes discrete risk management improvement initiatives, there is understandably a clear link between an organisation's risk management strategy and the initiatives it wishes to undertake to improve its framework.

The initiatives that are identified during review activities should be prioritised and then included within the risk management strategy and risk plans to ensure that they are appropriately approved and supported in their implementation. Inclusion of these initiatives in the strategy will also increase accountability for their delivery and should drive a need to measure their value once implemented; this explains the importance of establishing linkages between the various elements of the process outlined in these guidelines.

By continuously improving its risk management framework, an organisation should obtain benefits including:

- Organisational resilience by being more proactive in managing risks as compared to reactive in managing issues
- Better governance through regular reporting which strengthens an organisation's ability to oversee its risks and direct changes in approach where necessary
- Increased accountability through well defined risk management responsibilities against which performance is measured
- Being able to leverage leading risk management practice in its risk management approach.

5 Appendices

5.1 Appendix A: Glossary of key terms

The glossary below provides definitions for commonly used risk management terminology.
The ISO 31000:2009 has been used as the primary source of definitions.
Where the Standard does not include a definition of a particular term, other sources have been used.

Communication and consultation
Continual and iterative processes that an organisation conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk

Consequence
Outcome of an event impacting objectives

Control
Measure that modifies risk

Control assessment
Systematic review to ensure that controls are still effective and appropriate

Enterprise-Wide Risk Management (ERM)
An integrated approach to assessing and addressing all risks that threaten the achievement of the organisation's strategic objectives; the purpose of ERM is to understand, prioritise, and develop action plans to maximise benefits and mitigate top risks.

Establishing the context
Defining the external and internal parameters to be taken into account when managing risk and setting scope and risk criteria for the risk management policy

Event
Occurrence or change of a particular set of circumstances

Exposure
Extent to which an organisation and/or stakeholder is subject to an event

External context
External environment in which the organisation seeks to achieve its objectives

Frequency
Number of events or outcomes per defined unit of time

Hazard
A source of potential harm

Internal audit
Independent, objective assurance and consulting activity designed to add value and improve an organisation's operations…accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of: (1) Risk management (2) Control, and (3) Governance processes. (IIA Professional Practices Framework)

Internal context
Internal environment in which the organisation seeks to achieve its objectives

Key control indicator (KCI)
Measures or metrics that demonstrate a change in a specific control's effectiveness

Key performance indicators (KPIs)
Metrics or measures used to monitor changes in business performance in relation to specific business objectives (e.g. volumes of business, revenue etc.)

Key risk Indicators (KRI)
Measures and metrics that relate to a specific risk and demonstrate a change in the likelihood or consequence of the risk occurring

Level of Risk
Magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood

Likelihood
Chance of something happening

Loss
Any negative consequence or adverse effect, financial or otherwise

Monitoring
Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected

Probability
Measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty

Residual risk
Risk remaining after risk treatment

Review
Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

Risk
Effect of uncertainty on objectives

Risk acceptance
Informed decision to take a particular risk

Risk aggregation
Combination of a number of risks into one risk to develop a more complete understanding of the overall risk

Risk analysis
Process to comprehend the nature of risk and to determine the level of risk

Risk appetite
Amount and type of risk that an organisation is willing to pursue or retain

Risk assessment
Overall process of risk identification, risk analysis and risk evaluation

Risk attitude
Organisation's approach to assess and eventually pursue, retain, take or turn away from risk

Risk aversion
Attitude to turn away from risk

Risk avoidance
Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk

Risk criteria
Terms of reference against which the significance of risk is evaluated

Risk description
Structured statement of risk usually containing four elements:
sources, events, causes and consequences

Risk evaluation
Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable

Risk financing

Form of risk treatment involving contingent arrangements for the provision of funds to meet or modify the financial consequences should they occur

Risk identification

Process of finding, recognising and describing risks

Risk management

Coordinated activities to direct and control an organisation with regard to risk

Risk management audit

Systematic, independent and documented process of obtaining evidence and evaluating it objectively in order to determine the extent to which the risk management framework or any selected part of it is adequate and effective

Risk management framework

Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

Risk management plan

Scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk

Risk management policy

Statement of the overall intentions and direction of an organisation related to risk management

Risk management process

Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk

Risk matrix (or heat map)

Tool for ranking and displaying risks by defining ranges for consequence and likelihood

Risk mitigation

Measures taken to reduce an undesired consequence

Risk owner

Person or entity with the accountability and authority to manage a risk

Risk perception

Stakeholder's view on risk

Risk profile

Description of any set of risks

Risk reduction

Actions taken to lessen the likelihood, negative consequences, or both, associated with a risk

Risk register
Record of Information about identified risks

Risk reporting
Form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management

Risk retention
Acceptance of the potential benefit of gain, or burden of loss, from a particular risk

Risk severity
A measure of the magnitude of a risk, based on a combination of the likelihood and consequence of a risk

Risk sharing
Form of risk treatment involving the agreed distribution of risk with other parties

Risk source
Element which alone or in combination has the intrinsic potential to give rise to risk

Risk tolerance
Organisation's or stakeholder's readiness to bear the risk, after treatment, in order to achieve its objectives

Risk treatment
Process to modify risk

Stakeholder
Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Investors in
Risk Management

Investors in Risk Management

3 Oswin Road
Leicester, LE3 1HR
United Kingdom

T: 00 (44) 116 3664 011
info@iirmglobal.com
www.iirmglobal.com

www.iirmglobal.com