UNIT-14

Developing a Risk Management Framework

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ Overview – Risk management framework
- ✓ Key considerations when developing a risk management framework
- ✓ Documenting a risk management framework
- ✓ Risk management governance
- ✓ Risk management information systems

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:

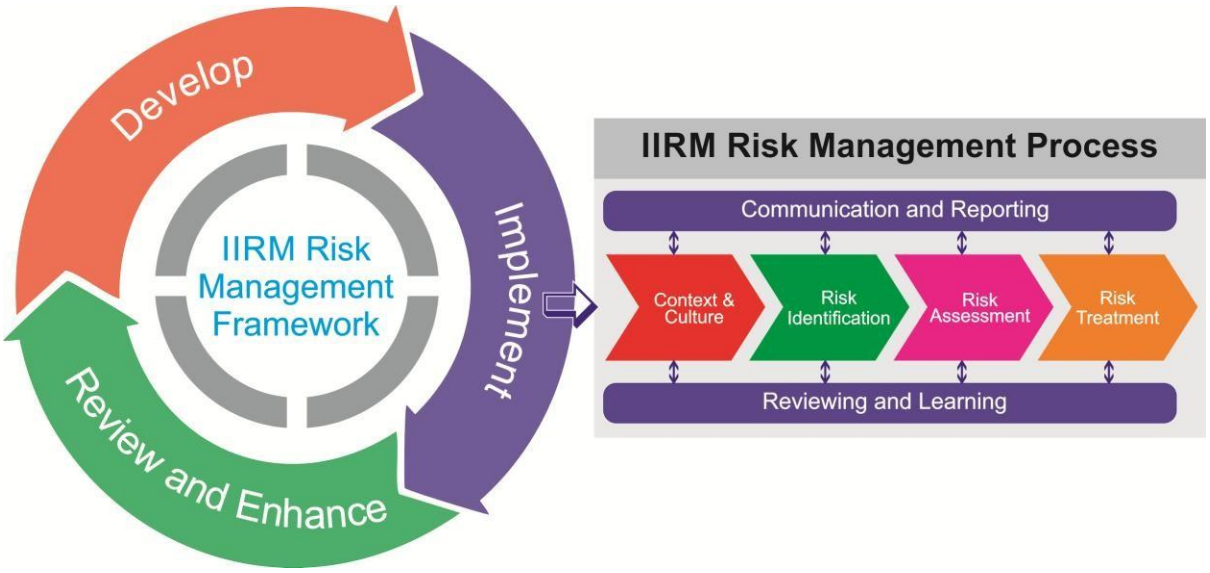
- the nature of the risks faced by the organisation
- the organisation's ability to accept and/or manage risk/s
- the resources available to manage risks within the organisation
- the organisation's culture

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).
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.

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.

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.

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

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

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.

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 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.

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

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.

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

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
- 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.
- 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

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?

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

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:

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.

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
- 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.

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.

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

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.

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?

Glossary of Key Terms

The glossary below provides definitions for commonly used risk management terminology.

- 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.

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